Freedom Security Justice
European Legal Studies

Collana diretta da Angela Di Stasi

CYBERVIOLENZA DI GENERE E NUOVE "FRONTIERE" NORMATIVE E GIURISPRUDENZIALI: LA DIRETTIVA UE 2024/1385

CIBERVIOLENCIA DE GÉNERO Y NUEVAS "FRONTERAS" NORMATIVAS Y JURISPRUDENCIALES: LA DIRECTIVA UE 2024/1385

a cura di

Angela Di Stasi
Rosario Espinosa Calabuig

EDITORIALE SCIENTIFICA
2025

Collana
Freedom, Security & Justice: European Legal Studies

14

CYBERVIOLENZA DI GENERE E NUOVE "FRONTIERE" NORMATIVE E GIURISPRUDENZIALI: LA DIRETTIVA UE 2024/1385

CIBERVIOLENCIA DE GÉNERO Y NUEVAS "FRONTERAS" NORMATIVAS Y JURISPRUDENCIALES: LA DIRECTIVA UE 2024/1385

a cura di

Angela Di Stasi
Rosario Espinosa Calabuig

EDITORIALE SCIENTIFICA
2025

Volume finanziato con fondi dell'Unità di ricerca dell'Università di Salerno – Progetto PRIN 2017 MIUR – "International Migrations, State, Sovereignty and Human Rights: open legal issues/Migrazioni internazionali, Stato, sovranità, diritti umani: questioni giuridiche aperte" e del Progetto (FARB) ex 60% – anno 2023 – e realizzato nell'ambito delle attività di ricerca dell'Osservatorio sullo spazio europeo di libertà, sicurezza e giustizia.

Via San Biagio dei Librai, 39
80138 Napoli

ISBN 979-12-235-0233-4

INDICE/*INDICE DE CONTENIDO*

PARTE II
LA DIRETTIVA (UE) 2024/1385 E LA SUA TRASPOSIZIONE NELL'ORDINAMENTO ITALIANO E SPAGNOLO/*LA DIRECTIVA (UE) 2024/1385 Y SU TRANSPOSICIÓN EN EL ORDENAMIENTO ITALIANO Y ESPAÑOL*

ORDINAMENTO ITALIANO/*ORDENAMENTO ITALIANO*

ORDINAMENTO SPAGNOLO/*ORDENAMIENTO ESPAÑOL*

Presentazione

Angela Di Stasi[*] *– Rosario Espinosa Calabuig*[**]

Il presente volume costituisce il risultato del lavoro svolto da una rete di ricerca multidisciplinare a cui hanno partecipato accademici dell'Università di Salerno e dell'Università di Valencia e che è stata integrata da accademici delle Università Autonoma di Barcellona, Ca' Foscari di Venezia, Campania "Luigi Vanvitelli", Foggia, Sapienza di Roma e Udine. Questa rete, di formazione teorico-pratica, ha utilizzato la lente di lettura del diritto internazionale pubblico, del diritto internazionale privato e del diritto dell'Unione europea (senza escludere profili di diritto costituzionale, criminologia, diritto penale e diritto processuale penale). Inoltre, è stata arricchita da una indispensabile lettura sociologica del fenomeno con la finalità di fornire una analisi esaustiva della direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica, da prospettive molto diverse, riservando un *focus* specifico alla cyberviolenza, sempre più spesso esercitata nei confronti delle donne.

L'analisi svolta presenta un carattere innovativo. Da un lato, perché è stata condotta con un approccio interdisciplinare, esaminando le fonti internazionali ed europee esistenti in materia a partire dalla Convenzione di Istanbul e dalla sua ratifica da parte dell'Unione europea. Dall'altro, perché è stato preso, come punto di riferimento, il quadro giuridico dell'ordinamento italiano e spagnolo, con l'obiettivo di fornire un contributo per una corretta trasposizione della menzionata direttiva negli ordinamenti giuridici degli Stati membri dell'Unione europea (ad eccezione della Danimarca).

La lettura integrata delle fonti internazionali, europee e nazionali,

[*] Professoressa ordinaria di Diritto internazionale e Diritto dell'Unione europea, Università degli Studi di Salerno. E-mail: adistasi@unisa.it.

[**] Professoressa ordinaria di Diritto internazionale privato, Università di Valencia. E-mail: rosario.espinosa@uv.es.

effettuata in questo lavoro, con riferimento agli sviluppi più recenti e anche a quelli passati, è stata completata dalla disamina della giurisprudenza della Corte europea dei diritti dell'uomo che non solo condiziona spesso le scelte del legislatore nazionale, ma arricchisce in modo evidente l'intera analisi.

Il risultato è un quadro di riferimento composito caratterizzato dall'esistenza di nuove "frontiere" normative e giurisprudenziali che riguardano la violenza contro le donne, realizzata con mezzi digitali, ovvero la cosiddetta cyberviolenza. La rapida evoluzione della tecnologia digitale, che ha inaugurato una nuova era con un *continuum* senza precedenti tra realtà fisica e digitale, ha dato origine a nuovi problemi comportando ulteriori sfide nella lotta alla violenza contro le donne.

La scelta di affiancare alla versione cartacea del volume quella in *open access* è dettata dall'obiettivo di rendere più facilmente accessibili i risultati di questa ricerca. Essa risulta contrassegnata anche da una precipua dimensione valoriale che si fonda sul fermo impegno, personale e professionale, rispetto alla lotta per la parità di diritti, per l'eliminazione della violenza contro le donne nonché per l'introduzione di una prospettiva di genere che è essenziale nella redazione, interpretazione e applicazione del diritto da parte di tutti gli operatori giuridici.

Salerno -Valencia, *Giornata Internazionale della Donna*, 8 marzo 2025

PRESENTACIÓN

*Angela Di Stasi** – *Rosario Espinosa Calabuig***

El presente volumen es fruto del trabajo realizado por una red de investigación multidisciplinar en la que han participado académicas/os de la Universidad de Salerno y de la Universidad de Valencia, y que se ha completado con académicas/os de la Universidad Autónoma de Barcelona, Ca' Foscari de Venecia, Campania "Luigi Vanvitelli", Foggia, Sapienza de Roma y Udine. Esta red de formación teórico-práctica ha sido realizada desde la óptica del derecho internacional público, el derecho internacional privado y el derecho de la Unión europea (sin excluir los perfiles de derecho constitucional, criminología, derecho penal y derecho procesal). Además, se ha visto enriquecida por una imprescindible lectura sociológica del fenómeno y por un análisis exhaustivo de la directiva (UE) 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica desde perspectivas muy diferentes, reservando un enfoque específico a la ciberviolencia que se ejerce cada vez más contra las mujeres.

El análisis realizado tiene un carácter innovador. Por un lado, porque se ha realizado con un perfil interdisciplinar, examinando las fuentes internacionales y europeas existentes sobre la materia, a partir del Convenio de Estambul y su ratificación por la Unión europea. Por otro lado, porque se ha tomado como punto de referencia el marco jurídico del ordenamiento italiano y español, con el fin de proporcionar indicaciones útiles para una correcta transposición de la citada directiva en los ordenamientos jurídicos de los Estados miembros de la Unión europea (a excepción de Dinamarca).

La lectura integrada de las fuentes internacionales, europeas y na-

* Catedrática de Derecho internacional y Derecho de la Union europea, Universidad de Salerno. E-mail: adistasi@unisa.it.

** Catedrática de Derecho internacional privado, Universitat de València. E-mail: rosario.espinosa@uv.es.

cionales realizada en este trabajo, con referencia a los desarrollos más recientes y también a los pasados, se ha completado con el examen de la jurisprudencia del Tribunal europeo de derechos humanos, que no sólo condiciona a menudo las opciones del legislador nacional, sino que enriquece claramente todo el análisis.

El resultado es un marco de referencia que se caracteriza por la existencia de nuevas "fronteras" normativas y jurisprudenciales de la violencia ejercida contra las mujeres, sobre todo cuando se lleva a cabo por medios digitales, esto es, la llamada ciberviolencia. La rápida evolución de la tecnología digital, que ha dado paso a una nueva era con un *continuum* sin precedentes entre la realidad física y la digital, ha originado paso a nuevos problemas y a desafíos adicionales en el combate de la violencia contra las mujeres.

La decisión de añadir una versión de acceso abierto a la versión impresa del libro obedece al objetivo de hacer más fácilmente accesibles los resultados de esta investigación. Ellos son además fruto de nuestro firme compromiso, personal y profesional, con la lucha por la igualdad de derechos, la eliminación de la violencia contra las mujeres y la introducción de una perspectiva de género, imprescindible en la elaboración, interpretación y aplicación del derecho por todos los operadores jurídicos.

Salerno - Valencia, *Día Internacional de la Mujer,* 8 de marzo de 2025

Saggio introduttivo/*Ensayo introductorio*

CYBERVIOLENZA DI GENERE E NUOVE "FRONTIERE" NORMATIVE E GIURISPRUDENZIALI: LA DIRETTIVA (UE) 2024/1385

Angela Di Stasi[*]

SOMMARIO: 1. La violenza digitale come *species* del più ampio *genus* della violenza contro le donne (e *lato sensu* di genere) e il suo articolato quadro di riferimento normativo. – 2. Dalla parziale insufficienza delle esistenti fonti "generaliste" all'adozione della direttiva (UE) 2024/1385. – 3. Il ricorso ad un (mero) atto di armonizzazione legislativa quale la direttiva. La sua trasposizione negli ordinamenti nazionali. – 4. Le direttrici di indagine della ricerca.

1. *La violenza digitale come* species *del più ampio* genus *della violenza contro le donne (e* lato sensu *di genere) e il suo articolato quadro di riferimento normativo*

Come è ben noto, nella recente attualità, alle "classiche" forme di violenza contro le donne (e, *lato sensu,* di genere), si aggiunge una diversa modalità di esplicazione della stessa: la violenza digitale[1]. Tale

[*] Professoressa ordinaria di Diritto internazionale e di Diritto dell'Unione europea, Delegata d'Ateneo alle Pari opportunità, Università degli Studi di Salerno. Email: adistasi@unisa.it.

[1] Già nel 2017 l'Istituto europeo per l'eguaglianza di genere aveva posto l'attenzione sul problema della violenza virtuale contro donne e ragazze, denunciando la difficoltà nel reperimento di dati disaggregati rispetto al genere ed evidenziando parimenti l'altissima percentuale di vittime nonché la significativa gravità dei danni che ne derivano. Lo stesso Istituto aveva, inoltre, sottolineato che la violenza in Rete debba essere intesa come un *continuum* rispetto a quella fisica, da cui non va dissociata, anche perché atta a provocare ripercussioni "reali" sulla vita delle persone coinvolte laddove appare tendenzialmente superata la distinzione tra mondo fisico e mondo virtuale, per effetto del c.d. "*on-life*" in cui siamo perennemente immersi. Anche il Parlamento europeo, pochi anni più tardi, con la Risoluzione del 14 dicembre 2021,

dimensione della violenza si traduce in una vasta gamma di atti, commessi online o tramite strumenti tecnologici, i quali realizzano un *continuum* nelle forme di violenza che donne e ragazze subiscono per motivi legati al loro genere[2].

Invero, se la rapida evoluzione della tecnologia digitale ha inaugurato una nuova era, caratterizzata da una sinergia senza precedenti tra realtà fisica e digitale, tale circostanza è suscettibile di affiancare alle più consuete forme di violenza contro le donne (sia quelle che vengono realizzate nelle relazioni endo-familiari che in quelle eso-familiari)[3] possibili, ulteriori fattori di criticità che non possono non comportare una accresciuta *due diligence* da parte degli Stati[4].

Quella stessa rete che, *inter alia*[5], è potenzialmente in grado di of-

aveva espresso raccomandazioni alla Commissione europea sulla lotta alla violenza di genere soffermandosi in maniera particolare sulla violenza online.

[2] Per una prima definizione di cyberviolenza contro le donne si veda la nozione fornita dalla Commissione europea (cfr. Commissione europea, *Comitato consultivo sulle pari opportunità per donne e uomini*, 2020) che ha chiarito che si tratta di "un atto di violenza di genere commesso, direttamente o indirettamente, attraverso le tecnologie dell'informazione della comunicazione che dà origine, o è probabile che dia origine, a violenza fisica, sessuale, psicologica o economica e che comprende le minacce di compiere tali atti … la cyberviolenza fa parte del continuum della violenza contro le donne: non è un fenomeno isolato, piuttosto si origina da forme multiple di violenza offline e le alimenta". V. *infra* nella nota 25 la definizione datane nella Raccomandazione generale n. 1 adottata dal GREVIO.

[3] La violenza contro le donne è definita dalla Convenzione di Istanbul (ai sensi dell'art. 3, lett. b) come "una violazione dei diritti umani e una forma di discriminazione contro le donne, comprendente tutti gli atti di violenza fondati sul genere che provocano o sono suscettibili di provocare danni o sofferenze di natura fisica, sessuale, psicologica o economica, comprese le minacce di compiere tali atti, la coercizione o la privazione arbitraria della libertà, sia nella vita pubblica, che nella vita privata".

[4] Si rinvia a E. MARTÍNEZ GARCÍA, *Ciberviolencia machista en el marco de la directiva (UE) 2024/1385 y Convenio de Estambul: perspectiva de género y obligationes del Estado/La cyberviolenza di genere nel quadro della direttiva (UE) 2024/1385 e della Convenzione di Istanbul: prospettiva di genere e obblighi dello Stato*, in questo Volume, pp. 215-255. Si veda in particolare l'art. 5 della Convenzione di Istanbul che prevede che "le parti adottano le misure legislative e di altro tipo necessarie per esercitare la debita diligenza nel prevenire, indagare, punire i responsabili e risarcire le vittime di atti di violenza commessi da soggetti non statali che rientrano nel campo di applicazione della presente Convenzione" e …

[5] Nel Rapporto *E.Government Survey 2024* delle Nazioni Unite si evidenziano i

frire inediti spazi di libertà per le donne, idonei a ridurre il divario di genere (si pensi all'opportunità di utilizzare il web in termini di *community building* e dunque di *empowerment*), può divenire l'ambiente in cui la violenza contro le donne si manifesta con caratteristiche nuove, rispetto alle quali gli strumenti tradizionali di contrasto (e anche di prevenzione) rischiano di palesare la loro parziale inadeguatezza anche in ragione della strutturale aterritorialità dello spazio cibernetico[6].

Proprio le peculiari caratteristiche dello spazio digitale e degli spazi digitali rendono più complessa la predisposizione di forme efficaci di tutela nei confronti di tali forme di violenza contro le donne. Una complessità che implica anche il ricorso a nuovi criteri di localizzazione, atti a declinare i metodi e i criteri propri del diritto internazionale privato in maniera tale da assicurare la tutela dei diritti in uno spazio digitale in cui i rapporti tra privati non sono più connessi a territori statuali ma a spazi digitali per i quali è controversa l'appartenenza all'uno o all'altro Stato[7].

Il ricorso ai vari strumenti di diritto internazionale (pubblico e privato) non esclude ovviamente la tutela, di tipo costituzionale, con riferimento a "vecchi" e "nuovi" diritti suscettibili di essere violati da atti di cyberviolenza[8].

Orbene, se la violenza digitale costituisce una *species* del più am-

progressi nel governo digitale globale con una riduzione del divario tecnologico dal 45% al 22%.

[6] Si rinvia a G.M. RUOTOLO e A.M. GALLO, *Le norme sulla lotta alla violenza di genere online nel contesto della regolamentazione internazionale ed europea di Internet: alcune questioni generali e di metodo/Normas para combatir la violencia de género en línea en el contexto de la regulación internacional y europea de Internet: algunas cuestiones generales y metodológicas*, in questo Volume, pp. 61-82.

[7] Si rinvia a S. TONOLO, *La cyberviolenza di genere: alcuni spunti di riflessione relativi al possibile contributo del diritto internazionale privato al contrasto della violazione dei diritti fondamentali di genere/La ciberviolencia de género: algunas reflexiones sobre la posible contribución del derecho internacional privado en la lucha contra la violación de los derechos fundamentales de género,* in questo Volume, pp. 83-122.

[8] Si rinvia a M. MARTÍNEZ LÓPEZ-SÁEZ, *Una (re)visión constitucional de los derechos clásicos y emergentes ante nuevas formas de ciberviolencia contra la mujer/Una (re)visione costituzionale dei diritti classici ed emergenti di fronte alle nuove forme di cyberviolenza contro le donne,* in questo Volume, pp. 161-184.

pio *genus* della violenza contro le donne (e, *lato sensu*, di genere)[9] la sua prevenzione e repressione risultano sicuramente riconducibili all'applicazione – anche integrata – dell'insieme delle fonti di diritto internazionale, di diritto dell'Unione europea e di diritto interno previste per quest'ultima, nel quadro di una più generale azione internazionale finalizzata a realizzare misure di *cybersecurity* per garantire un cyberspazio sicuro.

Al tempo stesso il contrasto (e la prevenzione) della violenza digitale richiede l'adozione di strumenti specifici, comportandone una consacrazione normativa in vari atti giuridici[10]. Essi sono il frutto dell'azione di un'Unione europea, sempre più alle prese con il consolidamento di una "sovranità tecnologica o digitale"[11] ma anche del crescente interesse di altre organizzazioni internazionali[12]: il tutto in linea

[9] Secondo un recentissimo studio condotto in maniera congiunta dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA), dall'Istituto europeo per l'uguaglianza di genere (EIGE) e dall'Ufficio statistico dell'Unione europea (EUROSTAT) sulla base di dati raccolti tra il 2020 e il 2024, a livello UE, una donna su tre è colpita da violenza fisica, sessuale o minacce in età adulta; una su cinque ha avuto esperienza di violenza fisica da parte del proprio partner o da parte di conoscenti stretti; una su tre è stata vittima di molestie sessuali sul luogo di lavoro. Cfr. FRA, EIGE, EUROSTAT, *EU gender-based violence survey – Key results. Experiences of women in the EU-27*, Publications Office of the European Union, Luxembourg, 2024.

[10] Si pensi alla normativa relativa ai servizi di media audiovisivi o a quella in tema di IA che cerca di mitigare i rischi legati alle tecnologie *deepfakes*.

[11] La Commissione europea, presieduta da Ursula Von Der Leyen, ha parlato di "sovranità tecnologica dell'Europa", nel 2020. V. Comunicazione della Commissione, del 10 marzo 2020, al Parlamento, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una nuova strategia industriale per l'Europa*, COM (2020) 102, p. 4, 15.

[12] Dall'Organizzazione delle Nazioni Unite a organizzazioni regionali quali, ad esempio, il Consiglio di Europa. V. il richiamo alla "*Intensification of efforts to prevent and eliminate all forms of violence against women and girls: the digital environment*" dell'11 novembre 2024 operato da parte dell'Assemblea generale delle Nazioni Unite (A/C.3/79/L17 Rev.1). Il 24 dicembre 2024, l'Assemblea generale delle Nazioni Unite ha adottato la Convenzione sulla criminalità informatica (*Cybercrime Convention*), dopo cinque anni di negoziati da parte di un Comitato *ad hoc* istituito nel 2019 (*Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*; vedi Risoluzione 74/247 dell'Assemblea generale delle N.U., del 27 dicembre 2019, *sul contrasto all'uso di tecnologie dell'informazione e della comunicazione a scopi criminali*).

con una crescente attenzione – che riguarda, per la verità, tutte le questioni giuridiche in tema di violenza di genere e anche questioni relative a categorie specifiche di donne[13] – all'interno di un percorso evolutivo il quale, prima di essere giuridico, è di tipo socio-culturale.

Come è ben noto, a fronte della sottovalutazione, per lungo tempo, della radice culturale del fenomeno della violenza contro le donne, tollerata in quanto ritenuta espressione di costumi sociali consolidati[14], solo negli ultimi decenni se ne è registrata una più incisiva presa di coscienza a livello, oltre che nazionale, internazionale ed europeo, con la sua riconduzione nell'alveo della tutela dei diritti umani[15]. Tale presa di coscienza si è tradotta nell'adozione di un insieme di fonti internazionali ed europee: in particolar modo convenzioni sia a carattere universale che regionale ma anche atti normativi di diritto dell'Unione europea che si fondano sull'utilizzo di una o più basi normative contenute nel diritto primario.

Con riferimento alle convenzioni internazionali basti ricordare la Convenzione onusiana per l'eliminazione di tutte le forme di discriminazione nei confronti delle donne del 18 dicembre 1979 e la Convenzione di Istanbul del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica dell'11 maggio 2011, entrambe ratificate dall'Italia senza riserve[16].

Quanto al diritto primario dell'UE ci si limita, in questa sede, a ri-

[13] Si rinvia a C. MORINI, *Dimensione cibernetica della violenza e delle molestie di genere in ambito lavorativo: il contesto internazionale ed europeo/Dimensión cibernética de la violencia de género y del acoso en el lugar de trabajo: el contexto internacional y europeo,* in questo Volume, pp. 291-326

[14] Si rinvia a G. CERSOSIMO, *La violenza di genere nelle relazioni online. Una riflessione sociologica/Violencia de género en las relaciones online. Una reflexión sociológica*, in questo Volume, pp. 39-60.

[15] Si rinvia a D. MARRANI, *La dimensione digitale della violenza contro le donne tra diritti umani e cybercriminalità/La dimensión digital de la violencia contra las mujeres entre los derechos humanos y la ciberdelincuencia,* in questo Volume, pp. 273-290.

[16] La Convenzione CEDAW è stata adottata dall'Assemblea generale delle Nazioni Unite ed è entrata in vigore il 10 luglio 1985. La Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, adottata dal Comitato dei Ministri del Consiglio d'Europa il 7 aprile 2011, aperta alla firma l'11 maggio 2011 in occasione della 121a Sessione del Comitato dei Ministri a Istanbul, è entrata in vigore il 1° agosto 2014.

chiamare le norme del Trattato di Lisbona (artt. 2, 3 par. 3 del TUE e artt. 10, 153, 157 par. 4 del TFUE)[17] nonché la Carta dei diritti fondamentali dell'Unione europea che all'art. 21 contempla il divieto di ogni forma di discriminazione fondata *sul sesso*, l'origine etnica o la razza, le convinzioni particolari e le opinioni politiche, mentre all'art. 23 sancisce il principio di parità tra donne e uomini in tutti i campi della vita sociale[18].

L'applicazione di questo complesso di fonti, di varia natura – cui si affiancano anche diversificate fonti di *soft law*[19] – all'interno della stessa regione internazionale (l'Europa intesa in senso lato e l'Unione europea in senso stretto) se, da un lato, non esclude distonie e asimmetrie, nondimeno può beneficiare della predisposizione di forme di "collegamento intersistemico", come testimonia, ad esempio, la recente adesione dell'Unione europea alla Convenzione di Istambul[20].

È appena il caso di rilevare che le già menzionate specificità legate alla violenza online rendono, in ogni caso, (almeno parzialmente) insufficienti le attuali fonti esistenti, pensate per le forme "classiche" di violenza contro le donne facendo emergere una esigenza di "adattamento/specificazione" del quadro normativo esistente.

[17] Tali basi normative non esauriscono le norme di diritto primario richiamabili. Si pensi al ricorso agli artt. 82 e 83 del TFUE per l'adozione della direttiva (UE) 2024/1385, di cui *infra.*

[18] Si rinvia a A. FESTA, *Dalla strategia per la parità di genere all'inserimento della violenza digitale tra gli "eurocrimini": l'approccio olistico dell'Unione europea al fenomeno della violenza contro le donne e di genere/De la estrategia de igualdad de género a la inclusión de la violencia digital entre los "eurocrímenes": el enfoque holístico de la Unión europea ante el fenómeno de la violencia contra las mujeres y de género*, in questo Volume, pp. 357-383.

[19] Si pensi, *inter alia*, alla Strategia per la parità di genere presentata dalla Commissione europea il 5 marzo del 2020, per il periodo 2020-2025, quale programma d'azione volto a fissare gli obiettivi strategici e le azioni da compiere per dare nuovo slancio all'uguaglianza tra donne e uomini e costruire un'Europa garante della parità di genere

[20] L'adesione perfezionata il 1° giugno 2023, dopo un articolato *iter* che ha contemperato anche un parere reso dalla Corte di Giustizia su richiesta del Parlamento europeo, oltre all'indubbio valore politico, comporta una serie di conseguenze sul piano giuridico.

2. *Dalla parziale insufficienza delle esistenti fonti "generaliste" all'adozione della direttiva (UE) 2024/1385*

Siffatta esigenza di "adattamento/specificazione" del citato complesso delle fonti di diritto internazionale e di diritto dell'Unione europea è astrattamente suscettibile di essere soddisfatta con il ricorso ad un ventaglio di opzioni normative ed eventualmente, in via residuale, anche mediante soluzioni giurisprudenziali.

Una prima opzione riposa nell'adozione di atti c.d. "di nuova generazione" quale costituisce, in particolare, la direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio sulla lotta alla violenza contro le donne e alla violenza domestica, pubblicata il 14 maggio 2024 ed entrata in vigore il 13 giugno 2024 che, all'interno di un contesto più ampio, contempla espressamente un set di norme sulla cyberviolenza[21].

Altra ipotesi percorribile è quella dell'adozione di protocolli *ad hoc,* atti ad ampliare i confini delle fattispecie normative previste in convenzioni esistenti. Si pensi, ad esempio, a come la mancanza nella Convenzione di Budapest del 2001 sulla criminalità informatica[22] di una disciplina specifica sulla cyberviolenza di genere[23] potrebbe rendere auspicabile l'adozione di un Protocollo *ad hoc* in considerazione delle gravi conseguenze che tali violazioni possono comportare rispetto alle vittime di siffatti crimini.

Restano, in ogni, caso prefigurabili forme di "integrazione dinamica" di alcune previsioni normative della Convenzione di Budapest

[21] V. in GUUE 24/5/2024. Essa si applica nei confronti di tutti i paesi membri, fatta eccezione per la Danimarca, a norma del Protocollo 22 al Trattato di Lisbona.

[22] Convenzione sulla criminalità informatica, STE, n. 185, aperta alla firma il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004.

[23] Essa definisce alcune condotte criminose rispetto alle quali gli Stati devono adottare misure sanzionatorie ma si tratta di condotte che solo indirettamente rilevano nel quadro della violenza di genere. In particolare l'accesso illegale ad un sistema informatico è contemplato dall'art. 2 quale azione volta a ottenere informazioni all'interno di un computer con intento illegale, ma senza alcun riferimento specifico alla violenza di genere; così pure l'art. 4 sanziona l'attentato all'integrità dei dati, l'art. 5 disciplina l'attentato all'integrità di un sistema mentre l'art. 9 prevede una disposizione specifica in merito ai reati relativi alla pornografia infantile senza che in esso compaia una caratterizzazione specifica in termini di violenza di genere.

(e, in particolare, del suo secondo Protocollo addizionale del 2022 che intende fornire norme comuni a livello internazionale e rafforzare la cooperazione in materia di criminalità informatica e raccolta delle prove in formato elettronico per le indagini o i procedimenti penali) con alcune disposizioni della Convenzione di Istanbul[24].

Un'ulteriore soluzione percorribile, ai fini della specificazione dei contenuti "generalisti" degli atti internazionali esistenti, risiede nell'adozione di strumenti di *soft law*. Lo testimonia, ad esempio, la Raccomandazione generale numero 1 sulla dimensione digitale della violenza sulle donne, adottata dal Gruppo di esperti sulla lotta contro la violenza nei confronti delle donne e la violenza domestica (GREVIO) nella sua attività di monitoraggio dell'applicazione della Convenzione di Istanbul ancorché la sua adozione non escluda questioni legate al rapporto tra la fonte convenzionale di *hard law* (che non contempla espressamente la violenza digitale) e la fonte di *soft law* che, attraverso lo strumento (debole) dell'atto raccomandatorio, la specifica[25].

[24] Il Protocollo, aperto alla firma il 12 maggio 2022, è stato firmato da 46 Stati ma ancora non è entrato in vigiore. Si rinvia a A. IERMANO, *Convenzione di Istanbul e Convenzione di Budapest: una risposta coordinata alla cyberviolenza contro le donne/ Convenio de Estambul y Convenio de Budapest: una respuesta coordinada al fenómeno de la ciberviolencia contra las mujeres*, in questo Volume, pp. 185-213.

[25] Cfr. GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women*, adottata il 20 ottobre 2021. Il GREVIO, rispetto alla circostanza che frequentemente la dimensione digitale della violenza contro le donne viene trascurata dalle leggi e non adeguatamente contemperata nelle politiche nazionali, introduce nella Raccomandazione la definizione di "dimensione digitale della violenza sulle donne", che comprende sia gli atti di violenza perpetrati online – come la condivisione di immagini umilianti, insulti, minacce di morte e di stupro – sia atti di violenza compiuti utilizzando tecnologie esistenti e non ancora inventate quali tecnologie di tracciamento riportate dalle società di sicurezza informatica. La Raccomandazione invita anche ad agire per evitare che possano essere controllate le risorse economiche di una donna senza il suo consenso attraverso l'*Internet banking*. Inoltre, essa promuove l'alfabetizzazione digitale e la sicurezza online nei curricula formali e a tutti i livelli di educazione, e la formazione sulle forme digitali di violenza contro le donne per gli attori interessati (forze dell'ordine, magistratura e operatori sanitari). Infine essa contiene un riferimento a un capitolo dedicato agli abusi sessisti online a cui si riferiva la Raccomandazione del 2019 del Comitato dei Ministri del Consiglio d'Europa a tutti gli Stati membri sulla prevenzione e la lotta al sessismo e profila potenziali opportunità di sinergia tra la Convenzione di Istanbul e la Convenzione di Budapest.

Infine, ancorché in via residuale, è prefigurabile un'interpretazione evolutiva di fonti normative "generalistiche" non solo mediante il ricorso ad una generale interpretazione *gender sensitive* delle stesse[26] ma anche attraverso una specifica interpretazione di basi normative esistenti, atta a ricomprendere l'ampliamento delle forme di violenza contro le donne nella moderna società del *tech*.

Come corollario della diversità – in termini di loro collocazione nella gerarchia delle fonti di diritto internazionale e di diritto dell'Unione europea e di *vis* sua giuridica (atto di *hard* o di *soft law*) – delle soluzioni normative adottate ma anche del loro diverso ambito di applicazione in senso soggettivo (più o meno lato), ne deriva la diversità delle ricadute all'interno degli ordinamenti dei vari Stati membri dell'Unione europea (e della Paneuropa).

Orbene, nel ventaglio di soluzioni percorribili già ricordate, si segnala l'adozione della menzionata direttiva (UE) 2024/1385 dell'Unione europea che, *inter alia*, – come si diceva – disciplina espressamente anche la violenza digitale.

Essa appare chiaramente riconducibile al più ampio quadro di riferimento normativo citato[27] e, rispetto alla variabilità, negli ordinamenti dei paesi membri dell'Unione europea, dei livelli di conformazione alle fonti internazionali e di diritto dell'Unione europea in materia, è suscettibile di dischiudere un nuovo capitolo nelle azioni di prevenzione e di contrasto di tale forma grave di violazione dei diritti umani.

Se, dunque, la direttiva si colloca nel menzionato ampio *framework* di fonti normative, sia di diritto internazionale che di diritto dell'Unione europea, sostenendo gli impegni internazionali degli Stati membri dell'UE[28], essa non può non ricollegarsi anche, in senso lato,

[26] V. A. IERMANO, *Donne migranti vittime di violenza domestica: l'interpretazione "gender-sensitive" dei giudici nazionali in conformità alla Convenzione di Istanbul*, in *Ordine internazionale e diritti umani*, 2021, p. 731 ss., in part. pp. 744-753.

[27] Si rinvia a E. BERGAMINI, S. DE VIDO, *La cyberviolenza di genere nel rapporto fra la direttiva 2024/1385 e gli altri strumenti di diritto dell'Unione europea/La ciberviolencia de género en la relación entre la directiva 2024/1385 y otros instrumentos del derecho comunitario*, in questo Volume, pp. 329-355.

[28] Come recita il suo Preambolo al 4° Considerando: "La presente direttiva sostiene gli impegni internazionali assunti dagli Stati membri per combattere e prevenire

ad una casistica giurisprudenziale che, in molti casi, anche con interventi di tipo "creativo", ha condizionato o accelerato l'avvio di riforme nazionali[29].

Senza dimenticare gli effetti che potranno rinvenirsi nella giurisprudenza della Corte di giustizia dell'Unione europea, a seguito della sua adesione alla Convenzione di Istanbul. Al riguardo va ricordata, in particolare, una giurisprudenza della Corte europea dei diritti dell'uomo particolarmente sensibile al tema della violenza contro le donne[30] e, in misura ancora residuale, a quella della violenza online[31]: una giurisprudenza che contribuisce a stimolare processi, in parte ancora *in fieri*, di "adattamento/specificazione" del quadro normativo esistente, talora "anticipando", l'adozione di successivi atti internazionali e/o di strumenti di diritto interno.

Ora è ben noto che la Convenzione europea dei diritti dell'uomo e delle libertà fondamentali (CEDU) non contiene un espresso riferi-

la violenza contro le donne e la violenza domestica, in particolare la convenzione delle Nazioni Unite sull'eliminazione di ogni forma di discriminazione nei confronti della donna e la convenzione onusiana sui diritti delle persone con disabilità e, ove pertinente, la convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica e la convenzione dell'Organizzazione internazionale del lavoro sull'eliminazione della violenza e delle molestie nel mondo del lavoro, firmata a Ginevra il 21 giugno 2019".

[29] Si pensi all'adozione in Italia della legge 19 luglio 2019, n. 69 recante "Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere" che possono considerarsi una sorta di *follow-up* dopo la pronuncia della Corte europea resa nel caso *Talpis c. Italia,* sentenza del 2 marzo 2017, ricorso n. 41237/14. V. su quest'ultima A. DI STASI, *Il diritto alla vita e all'integrità della persona con particolare riferimento alla violenza domestica (artt. 2 e 3 CEDU)*, in A. DI STASI (a cura di), *CEDU e ordinamento italiano*, II ed., Milano, 2020, pp. 1-32 cui si rinvia anche per i riferimenti dottrinali in materia. Per un commento alla legge n. 168/2023 e ad una più ampia ricostruzione del sistema normativo-giurisprudenziale v. P. DI NICOLA TRAVAGLINI e F. MENDITTO, *Il nuovo Codice rosso. Il contrasto alla violenza di genere e ai danni delle donne nel diritto sovranazionale e interno,* Milano, 2024.

[30] Cfr. ancora A. DI STASI, *Il diritto alla vita e all'integrità della persona*, cit., p. 1 ss.

[31] Si rinvia a V. TEVERE, *La giurisprudenza della Corte di Strasburgo in materia di violenza digitale/La jurisprudencia del tribunal de Estrasburgo sobre violencia digital*, in questo Volume, pp. 257-272.

mento ai diritti delle donne e alla violenza di genere né tantomeno alla violenza online. Nondimeno, in maniera analoga a quanto si è verificato per la tutela di altri diritti sprovvisti di una base normativa nel testo convenzionale, la Corte di Strasburgo, con un'interpretazione estensiva delle disposizioni convenzionali e con ampi riferimenti nel suo ragionamento giuridico alla ricostruzione del quadro di riferimento delle fonti di diritto internazionale e di diritto dell'Unione europea, ha ricondotto, in base ai livelli di gravità della violazione, la stessa sotto l' "ombrello" dell'art. 8 CEDU (diritto al rispetto della vita privata e familiare) e/o degli artt. 2 (diritto alla vita) e 3 (in tema di proibizione della tortura e divieto di trattamenti inumani e degradanti) e talvolta, anche se in via progressivamente residuale, dell'art. 14 (divieto di discriminazione)[32]. Quanto poi alla violenza digitale la stessa Corte ha prodotto una casistica allo stato ancora piuttosto limitata che, nelle tre sentenze rilevanti sul tema, ha individuato la violazione dell'art. 3 della CEDU (talora in collegamento con quella dell'art. 8)[33].

[32] Guardando, in una prospettiva diacronica, alla curva evolutiva che ha interessato la giurisprudenza della Corte di Strasburgo constatiamo, nell'ultimo ventennio, un più ampio ricorso al richiamo alla violazione degli artt.2 e 3 della CEDU (in sostituzione o in aggiunta a quello all'art.8) costituisce sicuramente un barometro di come la violenza contro le donne sia esercitata mediante azioni sempre più gravi. Si vedano le pronunce tese nei casi *Landi c. Italia* (sentenza del 7 aprile 2022, ricorso n. 10929/19), *De Giorgi c. Italia* (sentenza del 16 giugno 2022, ricorso n. 23735/19) e *M.S. c. Italia* (sentenza del 7 luglio 2022, ricorso n. 32715/19) con le quali la Corte di Strasburgo ha accertato la violazione della CEDU con riguardo agli artt. 2 (diritto alla vita) e 3 (divieto di trattamenti inumani e degradanti). Più di recente l'Italia è stata condannata in un nuovo caso di violenza domestica (caso *P.P. c. Italia*, sentenza del 13 febbraio 2025, ricorso n. 64066/19) per violazione dell'art. 3 CEDU a causa dei ritardi procedurali nelle indagini. La ricorrente aveva denunciato le Autorità nazionali per non aver preso in considerazione nei tempi le sue denunce nei confronti dell'ex partner per fatti di *stalking* e molestie. Sebbene la denuncia formalmente fosse stata presentata nel dicembre 2009, essa fu registrata dopo tre mesi. Il compagno fu rinviato a giudizio solo quattro anni dopo e la sentenza di primo grado fu pronunciata più di sei anni dopo. La Corte, condividendo le preoccupazioni sui ritardi del sistema procedurale italiano già segnalate dal GREVIO, ha evidenziato come grava sullo Stato la responsabilità di un elevato numero di casi di violenza domestica andati in prescrizione a causa delle lungaggini processuali, in spregio degli obiettivi della Convenzione e in maniera non compatibile con gli obblighi derivanti dall'art. 3 CEDU.

[33] Il riconoscimento della violazione di entrambe le norme si rinviene nel caso *Vo-*

È appena il caso di precisare che l'intercorsa adesione dell'Unione europea alla Convenzione di Istanbul non vanifichi l'importanza dell'adozione della direttiva né tantomeno l'adozione della direttiva svuoti di significato l'adesione alla Convenzione, giacché i due atti operano su piani diversi[34]: mentre la Convenzione promuove l'operato dell'Unione sul fronte della lotta alla violenza di genere e alla violenza domestica, la direttiva si indirizza agli Stati membri dell'UE con la conseguenza che quelli che non hanno ratificato la Convenzione – sebbene non tenuti a rispettarne gli obblighi di criminalizzazione – sono invece chiamati a dare attuazione alle previsioni contenute nella direttiva. Non va dimenticato, inoltre, che ai sensi dell'art. 73 della Convenzione di Istanbul, quest'ultima non escluda una più ampia tutela in tema di violenza contro le donne e di genere che eventualmente possa essere garantita dal diritto interno o dagli strumenti internazionali[35].

3. *Il ricorso ad un (mero) atto di armonizzazione legislativa quale la direttiva. La sua trasposizione negli ordinamenti nazionali*

Come si è detto il "legislatore" dell'Unione europea, in ragione della crescente rilevanza anche sul piano fenomenologico della violenza online e della diversità delle legislazioni in materia all'interno degli Stati membri dell'Unione europea, ha scelto di ricorrere ad un atto di (mero) ravvicinamento e armonizzazione delle suddette legislazioni quale la direttiva (UE) 2024/1385.

Essa – che origina dall'invito formulato dal Parlamento europeo[36],

lodina n. 2 in tema di *revenge porn* (Corte EDU, sentenza del 9 luglio 2021, ricorso n. 41261/17). La prima sentenza in materia è quella resa nel caso *Buturugă c. Romania* (Corte EDU, sentenza 11 febbraio 2020, ricorso n. 56867/1).

[34] Cfr. S. DE VIDO, *L'adesione dell'Unione europea alla Convenzione di Istanbul del Consiglio d'Europa: il ruolo delle organizzazioni della società civile a tutela delle donne*, in *Sistema Penale*, 2023, disponibile online.

[35] Cfr. A.A. DAVID, *Article 73. Effects of this Convention*, in S. DE VIDO e M. FRULLI (eds.), *Preventing and combating violence against women and domestic violence,* Cheltenham, 2024, p. 789 ss.

[36] Già con una Risoluzione del 26 novembre 2009, il PE aveva raccomandato agli Stati membri di migliorare la propria legislazione e le politiche nazionali per combat-

nel settembre 2021, alla Commissione ad annoverare la violenza di genere tra gli "eurocrimini", ai sensi dell'art. 83 TFUE[37], per equipararla a reati particolarmente gravi come il terrorismo, la tratta degli esseri umani, la criminalità informatica, lo sfruttamento sessuale e il riciclaggio di denaro – riflette un approccio normativo teso a considerare la violenza contro le donne quale fenomeno criminale grave che si pone in contrasto con i valori ed i diritti fondamentali dell'Unione europea, rilevando non già come prodotto di convinzioni etnico-culturali, ma in quanto crimine legato al genere.

Il testo di tale strumento di diritto derivato dell'Unione europea, sebbene risulti il frutto di un sensibile ridimensionamento rispetto ad alcuni contenuti della proposta originaria[38] – presentata nel 2022 dal

tere ogni forma di violenza contro le donne mentre in una relazione del 2013 del Servizio di ricerca del Segretariato Generale del Parlamento europeo veniva proposta l'adozione di quattro direttive: una sullo stupro, una contro le mutilazioni genitali femminili, una contro la violenza domestica ed una, in alternativa alle precedenti, più ampia sulla violenza di genere contro le donne in generale, con base giuridica individuata nell'art. 83 TFUE. Sul tema cfr. V. TEVERE, *Il difficile cammino verso una tutela integrata delle donne vittime di violenza nello spazio di libertà, sicurezza e giustizia: sviluppi normativi e perduranti profili di criticità*, in *Freedom Security & Justice: European Legal Studies*, 2019, fasc. 2, pp. 184-207.

[37] L'art. 83, par. 1, TFUE costituisce la disposizione che consente l'adozione di atti normativi volti ad armonizzare le legislazioni penali sostanziali degli Stati membri. Tale norma si presenta strutturata in diversi commi. Il primo, nel delineare un ambito di intervento dell'Unione mediante l'adozione di direttive adottate da Parlamento europeo e Consiglio con il ricorso alla procedura legislativa ordinaria, lo limita alle sole norme minime relative alla definizione di reati e sanzioni, in sfere di criminalità che siano considerate particolarmente gravi e manifestino una natura transnazionale "derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni". Il successivo, par. 1, co. 2, della stessa norma definisce, in maniera tassativa, le specifiche aree delittuose per cui l'intervento normativo è configurabile. Esso tuttavia contempla la possibilità, in ragione della mutevolezza e della variabilità delle attività criminali, per il Consiglio di adottare – all'unanimità e previa approvazione del Parlamento europeo – una decisione mediante la quale siffatta elencazione possa ricomprendere ulteriori settori (art. 83, par. 1, co. 3, TFUE).

[38] Si pensi al fatto che per il delitto di violenza online e diffusione di immagini intime la vittima debba dimostrare di aver subito un danno grave (art.6). Cfr. in dottrina E. BERGAMINI, *Combating Violence against Women and Domestic Violence from the Istanbul Convention to the EU Framework: The Proposal for an EU Directive*, in *Freedom Security & Justice: European Legal Studies*, 2023, n. 2, pp. 21-41.

Parlamento europeo e dal Consiglio ad esito di un'ampia consultazione pubblica realizzata mediante il portale «Dì la tua» – testimonia una compiuta consapevolezza, da parte delle istituzioni dell'Unione europea, della crescente diffusione della violenza online. Tale consapevolezza si traduce nella conseguente esigenza (che è sottesa all'adozione della citata direttiva) di armonizzazione delle legislazioni nazionali – ancorché in ragione di "norme minime" – in ordine alla "definizione dei reati e delle pene nei settori dello sfruttamento sessuale di donne e bambini e (con particolare riguardo all'oggetto di questo lavoro) dei reati informatici".

I *consideranda* da 17 a 27 della stessa definiscono il perimetro della violenza online laddove viene sottolineato che "l'uso delle TIC (Tecnologie dell'Informazione e della Comunicazione) comporta il rischio di un'amplificazione facile, rapida e diffusa di alcune forme di violenza online, con l'evidente rischio di provocare o aggravare danni profondi e a lungo termine per la vittima" (considerando 18).

Come si anticipava *supra* la nuova direttiva, a differenza della Convenzione di Istanbul che non la contemplava, assume la violenza online quale corollario della violenza subita dalle vittime nella vita reale riservando uno spazio significativo, all'interno del suo articolato, alla delineazione di tale modalità di esplicazione della violenza nello spazio digitale che può configurare apposite ipotesi di reato (artt. da 5 a 8 della stessa)[39]: una modalità suscettibile di implicare "un maggior rischio di vittimizzazione ripetuta, prolungata o addirittura continua" (v. considerando 51), che potrebbe trovare nella reiterazione del reato

[39] Con riferimento alle specificità dell'ordinamento italiano si rinvia ai contributi di M. TELESCA, E. LO MONTE, *La "risposta penalistica" alla violenza contro le donne e alla violenza domestica prevista dalla direttiva 2024/1385: verso l'emanazione di nuove fattispecie incriminatrici?/La "respuesta penal" a la violencia contra las mujeres y a la violencia doméstica en la directiva 2024/1385:¿hacia nuevas figuras penales?,* in questoVolume, pp. 387-426; L. KALB, *Il quadro giuridico generale auspicato nella fonte sovranazionale: dalla protezione delle vittime all'accesso alla giustizia/El marco jurídico general propuesto en la fuente supranacional: de la protección de las víctimas al acceso a la justicia ?,* in questo Volume, pp. 427-453; R. ALFANO, *Le scelte del legislatore italiano: attività investigativa e procedimento cautelare "speciale"/Las opciones del legislador italiano: actividad de investigación y procedimientos cautelares "especiales"*, in questo Volume, pp. 455-473.

il verificarsi di una circostanza aggravante (art. 11 lett. a). Nella misura in cui la direttiva è destinata a stabilire soltanto "norme minime" per le forme più gravi di violenza online, i pertinenti reati definiti nella stessa dovrebbero essere limitati a condotte che possono provocare danni gravi o un grave danno psicologico alla vittima, oppure a condotte atte a indurre la vittima a temere seriamente per la propria incolumità o per quella delle persone a suo carico[40].

Se le "norme minime" segnano il limite al di sotto del quale non è consentito scendere, la direttiva contiene parimenti, all'art. 48, una clausola di non regressione: il che si traduce nel fatto che, qualora gli Stati membri dispongano di norme più avanzate di quelle contenute nella direttiva, essi sono tenuti a mantenere il quadro normativo esistente più garantista essendo liberi di adottare o mantenere norme penali più rigorose (v. considerando 18).

Con riferimento ai suoi destinatari, per quanto l'intitolazione della direttiva sembrerebbe circoscrivere il suo campo di applicazione soggettivo alla tutela esclusiva delle donne, la previsione del considerando 12 – nella misura in cui sottolinea che altre persone sono oggetto di queste forme di violenza – consente potenzialmente di ampliarne la sua portata soggettiva. Inoltre essa testimonia una forte attenzione alla tutela dei minori, sottolineando, tra l'altro, quanto "può essere devastante" per questi ultimi assistere ad atti di violenza domestica "in ragione della loro vulnerabilità" (considerando 13)[41].

La direttiva coniuga l'esistenza di contenuti piuttosto dettagliati, relativi alle sanzioni minime da applicare, alle circostanze aggravanti,

[40] In ciascun caso, nel valutare se la condotta è suscettibile di causare un danno grave, si dovrebbe tener conto delle circostanze specifiche del caso, fatta salva l'indipendenza della magistratura. La probabilità di causare un danno grave può essere dedotta da circostanze materiali oggettive.

[41] Si rinvia, per differenti aspetti, a R. BORGES BLÁZQUEZ, *Ciberviolencia de género en menores de edad: vulnerabilidad, prueba, supernacionalidad y huida del proceso/Violenza informatica di genere contro i minori: vulnerabilità, aspetti probatori, dimensioni sovranazionali e fuga dall'azione penale*, in questo Volume, pp. 595-630 e a R. ESPINOSA CALABUIG, *Ciberviolencia contra las mujeres y cooperación judicial digitalizada en procesos de sustracción internacional de menores/Cyberviolenza contro le donne e cooperazione giudiziaria digitalizzata nei procedimenti sottrazione internazionale di minori*, in questo Volume, pp. 113-159.

alla giurisdizione e ai termini di prescrizione al riconoscimento (come è tipico di un atto di armonizzazione quale essa costituisce) di un certo margine di discrezionalità in capo agli Stati membri[42].

Divisa in 7 capi[43], si richiama alla "filosofia" ispiratrice della Convenzione di Istanbul fondata sull'insieme di prevenzione, protezione, azione penale e politiche coordinate. In particolare i capi 3 e 4 della stessa direttiva sono relativi alla protezione e al sostegno alle vittime, a cui deve essere garantito l'accesso alla giustizia, a cure mediche complete e a servizi di salute sessuale e riproduttiva. Gli Stati membri sono tenuti a fornire una formazione adeguata ai professionisti che potrebbero interagire con le vittime, comprese le forze dell'ordine, i pubblici ministeri e la magistratura. Viene sottolineata l'importanza di prevedere o rafforzare i "percorsi di formazione specifica e permanente rivolti a tutte le autorità e agli organismi competenti affinché svolgano celermente e adeguatamente la valutazione individuale del rischio, necessaria per preservare l'incolumità della vittima e fornire un'assistenza su misura, ed evitino il perpetuarsi di stereotipi sessisti che portano ad una vittimizzazione secondaria o ripetuta in tutte le fasi del procedimento"[44]. Per quanto riguarda l'assistenza alle vittime, la direttiva predispone l'istituzione di centri antistupro e di case rifugio e introduce una linea di assistenza telefonica rosa attiva 24/24[45]. Il capo 5 è, invece, relativo alla prevenzione, legata alle campagne e ai programmi di sensibilizzazione che devono essere svolti nelle scuole e nelle Università

[42] Ad esempio, il termine di prescrizione dei reati non è stato deciso a livello UE ma è disposto dai singoli Stati in relazione alla gravità del reato in questione.

[43] Denominati rispettivamente: Disposizioni generali; Reati concernenti lo sfruttamento sessuale delle donne e dei minori e crimini informatici; Tutela delle vittime e accesso alla giustizia; Supporto alle vittime; Prevenzione ed intervento precoce; Coordinamento e cooperazione; Disposizioni finali.

[44] Il legislatore italiano all'atto di recepimento sarà chiamato a rafforzare e integrare gli strumenti con cui l'autorità giudiziaria dispone misure urgenti di allontanamento, ordinanze restrittive e/o ordini di protezione al fine di tutelare efficacemente le vittime e le persone a loro carico. Si veda a questo proposito il citato caso *Talpis c. Italia* in cui la Corte europea dei diritti dell'uomo ha condannato l'Italia per non aver assicurato una tutela effettiva alla ricorrente, vittima di ripetute violenze da parte del marito, a causa dei ritardi nella procedura e della mancata adozione di misure idonee a prevenire il ripetersi delle aggressioni denunciate dalla donna.

[45] Si tratta del numero 116 016.

per contrastare gli stereotipi di genere, promuovere l'uguaglianza di genere, il rispetto reciproco e il diritto all'integrità personale e a incoraggiare tutte le persone, in particolare gli uomini e i ragazzi, a fungere da modelli di riferimento positivi per agevolare cambiamenti comportamentali in tutta la società[46].

In ogni caso, si richiede agli Stati membri di adottare politiche globali e coordinate (art. 38) e di introdurre piani d'azione nazionali (art. 39) che dovrebbero essere attuati con la cooperazione a livello sindacale (art. 43) laddove questi sforzi sono suscettibili di essere rafforzati dalla collaborazione con organizzazioni non governative.

La direttiva, come prevede il suo art. 49, dovrà essere trasposta negli ordinamenti degli Stati membri dell'Unione europea entro il 14 giugno 2027[47] comportando negli stessi effetti variabili in ragione del quadro normativo preesistente. In attesa dello spirare di tale termine i principi che la ispirano, come da giurisprudenza consolidata, costituiscono un limite rispetto alla sopravveniente normazione interna degli Stati che dovesse recare contenuti confliggenti con essi: un corollario dell'obbligo di leale cooperazione incombente sugli Stati membri dell'UE che, nel comportare la produzione di effetti giuridici sin dalla sua entrata in vigore delle direttiva, si traduce nel divieto di adottare, da parte degli Stati, misure che rendano più difficile la sua attuazione.

4. *Le direttrici di indagine della ricerca*

In questo volume le nuove "frontiere "(ovviamente intese in senso "metafisico") normative e giurisprudenziali della cyberviolenza contro le donne (e *lato sensu* di genere) sono delineate alla luce di tre direttrici di indagine.

[46] A tale proposito può segnalarsi che l'Unione europea già da tempo riserva dei fondi specifici a tali obiettivi: si pensi al Programma europeo *Daphne*, varato nel maggio 1997, e volto a prevenire e combattere la violenza contro i bambini, i giovani e le donne e per proteggere le vittime e i gruppi a rischio.

[47] V. la ricerca dell'EIGE (Istituto europeo per l'uguaglianza di genere) del 2022 che ha fatto una classificazione dettagliata delle forme di cyberviolenza di genere comparando i diversi ordinamenti degli Stati membri (EIGE, *Combatting Cyber Violence against Women and Girls*, 2022, in eige.europa.eu).

Da un lato, sulla base della consapevolezza dell'impossibilità di analizzare il tema separando l'approccio giuridico da quello non giuridico o metagiuridico, con la possibilità di riflettere su possibili cambi di paradigmi, nella messa in discussione anche del baricentro del sistema (solo la vittima o anche l'autore del reato?). Si tratta, in fondo, del richiamo alla menzionata "filosofia" ispiratrice della Convenzione di Istanbul fondata, come si diceva, su di una architettura garantistica con riferimento alle classiche tre "p", *Prevention, Protection and Prosecution,* corredate e rafforzate da una serie di altri impegni, di carattere politico e sociale, intesi alla realizzazione di strategie integrate per il contrasto e l'eliminazione della violenza contro le donne e della violenza domestica.

Dall'altro, l'analisi è finalizzata a delineare le nuove "frontiere" normative e giurisprudenziali della cyberviolenza contro le donne attraverso una lettura il più possibile integrata delle fonti internazionali, europee e nazionali *inter se* con riferimento ai più recenti sviluppi in atto e anche agli sviluppi mancati: il tutto laddove, come è noto, sovente i legislatori nazionali si muovono in esecuzione di obblighi di derivazione internazionale o europea o in risposta a sentenze di condanna ad opera di giurisdizioni internazionali.

Questo volume assume l'Italia e la Spagna come ordinamenti giuridici di riferimento[48].

Orbene, ancorché la legislazione italiana e quella spagnola (sovente in ragione dell'adattamento alle disposizioni contenute negli "atti derivati" dalla Convenzione di Istanbul nonché della giurisprudenza

[48] Quanto all'ordinamento spagnolo si tratta del primo Stato dell'Unione europea ad aver adottato una legislazione sulla cyberviolenza si rinvia a N. IGAREDA GONZÁLEZ, *La ciberviolencia de género en España: límites y oportunidades de la respuesta legal a un fenómeno global/La cyberviolenza di genere in Spagna: limiti e opportunità della risposta legale a un fenomeno globale*, in questo Volume, pp. 477-499; A. JAREÑO LEAL, *La protección penal del derecho a la imagen íntima. Especial referencia a los casos de* deepfake *sexual/La tutela penale del diritto all'immagine intima. Riferimento speciale ai casi di* deepfake *sesuali*, in questo Volume, pp. 501-518; J.C. VEGAS AGUILAR, *Medidas cautelares nacionales y transnacionales de interés para la protección de víctimas de ciberviolencia de gébero/Misure cautelari nazionali e transnazionalii relative alla protezione delle vittime di violenza informatica di genere*, in questo Volume, pp. 519-550; M.J. JORDÁN DÍAZ-RONCERO, *La prueba en los procesos por violencia digital de género/La prova nei processi per violenza digitale di genere*, in questo Volume, pp. 551-593.

della Corte di Strasburgo[49]), contengano un *corpus* di norme piuttosto avanzato, in ogni caso, all'interno dei suddetti ordinamenti, le soluzioni normative adottate, anche laddove appaiono piuttosto convincenti con riferimento alla prevenzione e al contrasto della violenza contro le donne e di genere, non mancano di evidenziare l'esistenza di alcune lacune normative proprio rispetto alle specificità della cyberviolenza.

Infine, rileva la terza direttrice di indagine che registra lo sforzo di saldare il sistema delle fonti con la prassi giudiziaria e la casistica, alla luce di un approccio ricostruttivo atto a coniugare teoria e prassi. Rispetto a questioni giuridiche ancora aperte possono essere, infatti, preziose le interazioni tra dato normativo e prassi giurisprudenziale, sovente foriera di soluzioni ancorate al richiamo alla contemporanea sussistenza di vari obblighi internazionali con l'obiettivo di apportare una tutela accresciuta e più effettiva.

In conclusione, la corretta trasposizione della direttiva (UE) 2024/1385, alla luce dell'ampio quadro di riferimento normativo-giurisprudenziale delineato e che sarà oggetto di disamina nei contributi che seguiranno, non potrà non muoversi in adesione a quanto sottolineato in un passaggio della sentenza adottata dalla Corte di Strasburgo (par. 49 della pronuncia resa nel caso *Volodina* 2): "la violenza online o cyberviolenza è correlata alla violenza offline e rappresenta una delle facce del fenomeno più complesso della violenza domestica. Gli Stati hanno gli obblighi positivi di istituire ed applicare un sistema effettivo di punizione delle forme di violenza domestica e di prevedere misure di salvaguardia sufficiente per le vittime".

[49] In argomento si veda B. NASCIMBENE, *Tutela dei diritti fondamentali e "violenza domestica". Gli obblighi dello Stato secondo la Corte EDU*, in *La legislazione penale*, 12 giugno 2018, p. 4 ss.; A. DI STASI, *Il diritto alla vita e all'integrità della persona*, cit., p. 1 ss.; A.G. LANA, *Le violazioni della Convenzione europea dei diritti umani riscontrate nella più recente giurisprudenza della Corte EDU in casi di violenza domestica*, in A. DI STASI, R. CADIN, A. IERMANO, V. ZAMBRANO (a cura di), *Donne migranti e violenza di genere nel contesto giuridico internazionale ed europeo*, p. 635 ss.; A. SANGIORGI, *Le vulnerabilità delle donne migranti nella giurisprudenza della Corte Edu tra profili di tutela e problematiche irrisolte*, in A. DI STASI, R. CADIN, A. IERMANO, V. ZAMBRANO (a cura di), *op. cit.*, p. 743 ss.

Abstract

Il presente saggio contiene una introduzione al volume destinata a individuare il "perimetro" delle nuove "frontiere" normative e giurisprudenziali della cyberviolenza contro le donne (e *lato sensu* di genere) con riferimento ai più recenti sviluppi in atto e anche agli sviluppi mancati. La direttiva (UE) 2024/1385 viene collocata nel più ampio quadro di riferimento costituito dalle fonti internazionali ed europee che la disciplinano, senza trascurare gli effetti della giurisprudenza (in particolare quella della Corte europea dei diritti dell'uomo) che risulta particolarmente sensibile al tema della violenza contro le donne e, in misura ancora residuale, a quella della violenza online. Le specificità legate alla violenza online rendono, in ogni caso, (e almeno parzialmente) insufficienti le attuali soluzioni normative esistenti, pensate per le forme "classiche" di violenza contro le donne facendo emergere una esigenza di "adattamento/specificazione" del quadro normativo esistente.

KEYWORDS: "Frontiere" normative e giurisprudenziali – violenza online – direttiva (UE) 2024/1385 – fonti internazionali – fonti europee

CIBERVIOLENCIA DE GÉNERO Y NUEVAS "FRONTERAS" NORMATIVAS Y JURISPRUDENCIALES: LA DIRECTIVA (UE) 2024/1385

Este ensayo contiene una introducción al volumen destinada a describir el "perímetro" de las nuevas "fronteras" normativas y jurisprudenciales de la ciberviolencia contra las mujeres (y *lato sensu* de género) con referencia a los desarrollos más recientes y también a los avances que se han pasado por alto. La directiva (UE) 2024/1385 se sitúa en el marco de referencia más amplio constituido por las fuentes internacionales y europeas que la regulan sin descuidar los efectos de la jurisprudencia (en particular la del Tribunal Europeo de Derechos Humanos) particularmente sensible a la cuestión de la violencia contra las mujeres y, en una medida aún residual, a la de la violencia online. Las especificidades relacionadas con la violencia online hacen, en cualquier caso, (y al menos parcialmente) inadecuadas las soluciones jurídicas existentes diseñadas para las formas "clásicas" de violencia contra las mujeres, poniendo de manifiesto la necesidad de "adaptación/especificación" del marco jurídico existente.

PALABRAS CLAVE: "Fronteras" legales y jurisprudenciales – violencia online – directiva (UE) 2024/1385 – fuentes internacionales – fuentes europeas

PARTE I

QUADRO DI RIFERIMENTO EUROPEO ED INTERNAZIONALE

MARCO DE REFERENCIA EUROPEO Y INTERNACIONAL

LA VIOLENZA DI GENERE NELLE RELAZIONI ONLINE. UNA RIFLESSIONE SOCIOLOGICA

Giuseppina Cersosimo[*]

1. *Breve premessa*

Facebook nata nel 2004 è stata la più grande comunità di incontro tra persone in uno spazio virtuale, così anche i social venuti dopo, i quali da un lato hanno costituito un luogo di condivisione di immagine, foto *travel*, *food*, *fashion* (Instagram - Twitter) e, dall'altro hanno fatto nascere nuove relazioni sociali, figure come gli influencer e nuove forme di attivismo specie per i più giovani per la generazione Z e anche alcuni millennial (TikTok). Oltre ad essere luoghi di intrattenimento sono divenuti luoghi di attivismo politico, spazio democratico di interazione tra i giovani per ragionare di pace e conflitti, ma anche di discriminazione di genere, aborto, cambiamento climatico, sostenibilità ambientale e sviluppi di altri temi sociali importanti. Tuttavia, questi stessi social sono stati anche il luogo nel quale hanno fatto ingresso l'invidia sociale, l'*hate speech*, la cyberviolenza. In Italia da una rilevazione, relativa al periodo gennaio-ottobre del 2021, realizzata da VOX, Osservatorio Italiano sui Diritti, emerge che su 797.326 tweet, dei quali 550.277 critici, ad essere colpite maggiormente per il 47,30% sono le donne. Più nello specifico VOX ha rivelato che su un totale di 340.280 tweet che parlavano di donne, 240.460 (71%) erano messaggi misogini e colmi di odio[1]. In particolare, le donne maggiormente espo-

[*] Professoressa ordinaria di Istituzioni di sociologia e di sociologia del web e degli impatti sociali, Università degli Studi di Salerno. Email: gcersosi@unisa.it.

[1] VOX – OSSERVATORIO ITALIANO SUI DIRITTI, *La nuova mappa dell'intolleranza* 6, 2021, disponibile su http://www.voxdiritti.it/la-nuova-mappa-dellintolleranza-6/.

ste sono quelle che hanno un ruolo pubblico, come giornaliste e politiche prese di mira da insulti e minacce e regolarmente mortificate per il loro aspetto fisico.

La cyberviolenza di genere è problema sociale, culturale, giuridico nonché politico interno alle diverse forme di violenza di genere oggi prodotte sempre più nello spazio digitale diventando emergenza sociale, politica e culturale prioritaria da affrontare con urgenza a tutela di milioni di donne, in particolare di giovani che rappresentano il target più colpito, date le conseguenze e i costi che il fenomeno ha sia a livello individuale che sociale. La definizione e la dimensione digitale della violenza di genere riguardano una vasta gamma di atti commessi online o tramite strumenti tecnologici, tutti parte del *continuum* di violenza che donne e ragazze subiscono anche nella sfera domestica. Si tratta di un fenomeno così vasto che non esiste una definizione unica per spiegarne e comprenderne le diverse caratteristiche. La crescita delle Tecnologie dell'Informazione e della Comunicazione (TIC) e dei siti di social network (SNS) ha generato nuove opportunità di violenza, in particolare rivolta a donne, ragazze e minoranze sessuali e di genere. Gli abusi che si verificano su e attraverso le TIC e gli SNS rappresentano il fenomeno della violenza informatica, tra cui, ma non solo, cyberbullismo, molestie online, abuso di appuntamenti online, *revenge porn*, *cyberstalking*, *shallowfake*, *sextortion*, *deepfake* e così via.

Pertanto, lo spazio online è divenuto un luogo di relazione non sicuro, colmo di odio e di pratiche aggressive e discriminatorie[2], nel quale proliferano commenti violenti dall'uso di giudizi sessuali espliciti alla diffusione di minacce, all'adozione di un linguaggio scurrile, all'esercizio ricorrente di rabbia e odio, che divengono routine nelle interazioni online quotidiane contro donne e ragazze, ma anche verso gruppi sociali emarginati o membri della comunità LGBTQ+.

Per il Consiglio d'Europa la cyberviolenza comporta atti di aggressione e danno perpetrati per via digitale, con l'intento di causare, facilitare o minacciare danni o sofferenze a persone[3]. Questo fenome-

[2] S. TIROCCHI M. SCOCCO, I. CRESPI, *Generation Z and Cyberviolence: between Digital Platforms Use and Risk Awareness*, in *International Review of Sociology*, 2022, n. 3, pp. 443-462.

[3] Council of Europe, Cybercrime Convention Committee, Working group on

no, noto con l'acronimo cyber-VAWG, è stimato avere ripercussioni molto concrete sul benessere di chi lo subisce[4]; tuttavia, alcuni studiosi di cyberviolenza hanno tenuto separati le violazioni online dalle forme più tradizionali di violenza perpetrata contro le donne poiché, secondo loro, la cyber-VAWG non ha la stessa gravità attribuibile ai danni fisici, pertanto deve essere trattata distintamente. Sebbene questi studi abbiano una loro traiettoria di ricerca in questo *paper* la cyber-VAWG è considerata una violenza che, al pari di quella agita offline, lascia cicatrici, tanto più se consideriamo che oggi la nuova specificità della nostra vita quotidiana è agita, vissuta, in modalità *on-life.*

2. *Tradizione e mutamento nelle relazioni online: il ruolo del digitale*

La cyberviolence è parte del *continuum* della violenza ed enfatizza come le sue varie manifestazioni derivino da una comune radice culturale e siano intrinsecamente connesse tra loro. Non a caso la violenza di genere contro donne e ragazze, cyber-VAWG è un fenomeno che esacerba le dinamiche di discriminazione, emarginazione ed esclusione delle donne dalla società. Non si tratta di un fenomeno isolato, ma nasce e si alimenta nelle istituzioni improntate a profonde disuguaglianze e discriminazione strutturali. Pertanto, come sostenuto da molte femministe[5] la violenza nelle relazioni online dovrebbe essere intesa come il "*continuum* della violenza tradizionale", meglio, una sua estensione

cyberbullying and other forms of online violence, especially against women and children, *Mapping Study on Cyberviolence with Recommendations adopted by the T-CY on 9 July 2018*, (T-CY (2017)10), 9 July 2018.

[4] L. GIUNGI, A. YAKOVLEVA, N. GREENFIELD, I. GALIZIA, C. TAYLOR, M. PLAZA, S. RHODES, L. ROSENGARD, J. KUMAR, S. AWAN, *Digital Gender-Base Violence: the State of the Art*, in GEN POL – GENDER & POLICY INSIGHTS, *When Technology Meets Misogyny, Multi-level Intersectional Solutions to Digital Gender-Based Violence*, 2019, pp. 13-25, disponibile su https://gen-pol.org/wp-content/uploads/2019/11/When-Technology-Meets-Misogyny-GenPol-Policy-Paper-2.pdf.

[5] Tra le altre si vedano C. COCKBURN, *The Continuum of Violence: A Gender Perspective on War and Peace*, W. GILES, J. HYNDAN (eds.), *Sites of Violence: Gender and Conflict Zones*, Berkeley, 2004, pp. 24-44 e S. E. DAVIES, J. TRUE, *Reframing Conflict-related Sexual and Genderbased Violence: Bringing Gender Analysis Back*, in *Security Dialogue*, 2015, vol. 4, n. 6, pp. 495–512.

che si propaga grazie all'uso di tecnologie informatiche per perpetrare atti violenti contro le donne in un comune sistema di oppressione[6]. In altri termini, siamo di fronte a un persistente retaggio culturale di genere a sostegno dello *status quo* del dominio maschile che le interazioni offline riflettono nell'online[7]. La violenza contro le donne è ancora una manifestazione di rapporti di forza ineguali tra uomini e donne che generano disuguaglianze nell'accesso al potere.

Come già detto, la violenza digitale è un *continuum* della violenza di genere tradizionale. Pertanto, la violenza da partner intimo, attuale o precedente, è comunemente definita come comprendente abusi fisici, sessuali, psicologici ed emotivi, nonché *stalking* e comportamenti di controllo. Si tratta di una delle forme più comuni di violenza contro le donne, e i dati dell'Organizzazione Mondiale della Sanità riportano che circa un terzo delle donne nel mondo ha subito questo tipo di violenza nel corso della propria vita. I rapidi sviluppi delle tecnologie di comunicazione e sorveglianza sono stati, senza sorpresa e per alcuni forse anche senza idea di quello che potevano divenire, sempre più utilizzati dagli autori di violenza nelle relazioni intime, ampliando i mezzi e la portata delle tattiche di abuso[8]. Questo ragionamento trae ulteriore evidenza dall'osservazione che, nell'era digitale, i confini tra le dimensioni online e offline sono sempre più sfumati.

Ciò detto, però, bisogna capire che cos'è questa violenza che si determina oggi negli ambienti informatici, digitali e perché le relazioni di genere si sono spostate all'interno dello spazio digitale. Sicuramente una cosa molto interessante è stata avanzata già da molto tempo da alcuni sociologi come Innis[9], McLuhan[10] che suggerirono che l'introdu-

[6] Human Rights Council, Report of the Special Rapporteur on Violence against women, its causes and consequences, MS. DUBRAVKA ŠIMONOVIĆ, *On online violence against women and girls from a human rights perspective*, A/HRC/38/47, 18 June 2018.

[7] P. BOURDIEU, *La domination masculine*, Paris, 1998 (trad. it. *La dominazione maschile*, Milano, 1999).

[8] A. POWELL, *Intimate Intrusions': Technology Facilitated Dating and Intimate Partner Violence*, in A. FLYNN, A. POWELL, L. SUGIURA (eds.), *The Palgrave Handbook of Gendered Violence and Technology*, Berlino, 2021, pp. 157-179.

[9] H.A. INNIS, *The bias of communication, Introduction by Marshall McLuhan*, Toronto, 1964.

[10] M. MCLUHAN, *Understanding media: The extensions of man*, Toronto, 1964.

zione di nuove tecnologie comunicative in una società modifica sostanzialmente il modo nel quale i suoi membri percepiscono, pensano ed interagiscono. Questo vuol dire che i processi comunicativi tecnologicamente strutturati attraverso i nuovi *device* hanno colonizzato tutti gli ambiti della vita quotidiana in modo più o meno rapido e più di quanto si possa pensare: in effetti hanno ricodificato il modo nel quale pensiamo e agiamo anche la violenza contro le donne.

Jan van Dijk definisce la società delle reti come: "Una forma di società che organizza sempre di più le sue relazioni a partire da reti di media destinate gradualmente a integrare le reti sociali della comunicazione faccia a faccia"[11].

L'apparato digitale, attraverso il quale interagiamo con gli altri, ci trasforma sul piano cognitivo, percettivo, psicologico, sociale, psichico e perfino neurologico. Rispetto a un regime industriale oppressivo, pesante, pressante, ripetitivo, ristretto, solido, stabile, è evidente l'apparato digitale "viene usato come un buon amico" ed è casuale, silenzioso, pervasivo, in mutamento simbolico e sistemico. Non di meno i suoi effetti sono costanti e sempre presenti. Esso ricodifica le esperienze online e offline, quelle pubbliche e private, locali e globali, e il rapporto tra intelligenza umana e artificiale. E rispetto alla standardizzazione dei lavoratori e dei consumatori, da parte di una logica industriale monolitica, l'apparato digitale opera rendendo anzitutto personale ma anche consuetudinario il suo uso. Non distorce il corpo quanto ristruttura la mente. Non contrappone le persone quanto ridefinisce le regole dell'interazione reciproca. Non scinde il sé, ma promuove nuove forme di individualità. Soprattutto invita ognuno a scegliere le proprie evasioni, reti, fantasie, ontologie private, mentre fornisce a ogni utente conferme personalizzate[12]. Oggi siamo di fronte non solo alla *network society* ma anche alla *information society*, nella quale gli individui utilizzano i *new media* principalmente per informarsi, mentre

[11] J. VAN DIJK, *Sociologia dei nuovi media,* Bologna, 2002, p. 273 (ed. or. *The Network Society. An Introduction to the Social Aspects of New Media*, NewYork, 1999).

[12] S. GOTTSCHALK, *L'interface work nell'era digitale*. (trad. it. e cura di G. CERSOSIMO), Lecce, 2015.

iniziano a prendere forma anche le interazioni online nelle dimensioni più intime e emotive.

I nostri adattamenti all'interazione online stanno avvenendo in un momento storico che un certo numero di studiosi definisce "ipermoderno". Interdisciplinare e ispirato all'umanesimo critico, il progetto ipermoderno cerca di comprendere il momento contemporaneo analizzando quattro aree interrelate della vita quotidiana: (1) l'impatto delle tecnologie digitali sui comportamenti e sugli stili di vita degli individui; (2) le manifestazioni e le conseguenze individuali di una nuova relazione con il tempo, con gli altri e con se stessi; (3) le conseguenze della società dell'iperconsumo e l'integrazione della mentalità commerciale nella vita quotidiana degli individui e (4) gli effetti delle nuove tecnologie sugli stili di lavoro e le loro conseguenze sulla vita individuale e collettiva[13]. Due forze sociali interrelate sono particolarmente importanti nell'approccio ipermoderno: eccesso e accelerazione. Per Nicole Aubert, la società ipermoderna è quella nella quale consumo, competizione, profitto, ricerca del piacere, violenza, terrorismo, capitalismo, in una parola tutto, è esagerato, spinto al limite e a un livello oltraggioso. È il risultato della globalizzazione dell'economia, della flessibilità generalizzata che produce, dei livelli sempre crescenti di performance, adattabilità e reattività che richiede la profonda modificazione dei nostri comportamenti, che induce anche una società catturata dalla logica mercantile trionfante e frantumata dall'esplosione di tutti i limiti che avevano finora strutturato la costruzione delle identità individuali[14].

Qual è divenuta allora la natura dei rapporti umani nella società dei consumi? Secondo la Illouz tutte le divisioni e distinzioni su cui si basano le nostre società si fondano sulle culture emozionali. Le emozioni sono un fenomeno culturale e sociale, e le distinzioni su cui si basano le nostre società si fondano sulle culture emozionali come, ad esempio, quella tra uomini e donne.

Le divisioni di genere, infatti, si basano sulle distinzioni emotive,

[13] S. GOTTSCHALK, *The Terminal Self: Everyday Life in Hypermodern Times*, London, 2018, pp. 23-31.

[14] N. AUBERT (cur.), *@ La Recherche du Temps: Individus Hyperconnectés, Société Accélérée*, Toulouse, 2018.

senza le quali i ruoli di uomini e donne non potrebbero venire riprodotti. Si parla non più solo di capitalismo digitale[15], ma anche di "capitalismo emotivo", ovvero di una cultura nella quale le pratiche emozionali e quelle economiche interagiscono, creando un movimento nel quale la vita emotiva degli individui segue le logiche dei rapporti economici e dello scambio. Partendo da questo concetto, Illouz ha avanzato la classificazione di nuove forme emozionali, si tratta delle "emozioni in rete", sottolineando come i siti di incontri siano una delle maggiori fonti di lucro nell'economia di Internet.

I siti web di incontri trasformano l'identità private in qualcosa da esibire pubblicamente e l'io viene oggettivizzato attraverso i mezzi di rappresentazione visiva e del linguaggio. Una delle conseguenze di questo fenomeno è che l'ordine tradizionale delle interazioni sentimentali viene sovvertito, in quanto sul sito di incontri prima viene la conoscenza approfondita, mediata dal virtuale per lo più come finzione, e poi l'attrazione. Inoltre, gli individui in Internet vengono posti in un mercato in cui tutti sono in competizione con tutti: "Ciascuna delle persone che è alla ricerca di un partner viene messa da Internet su un libero mercato di libera concorrenza con altri. Nel momento in cui ci registriamo in un sito veniamo istantaneamente collocati in una posizione in cui siamo in concorrenza con altri che di fatto sono tutti spiattellati sotto i nostri occhi"[16].

Il paradosso che si crea è che in un ambiente in cui si è esposti a così tanti sguardi si è portati a concentrarsi molto di più su di sé, al fine di comunicare al meglio la propria unica soggettività. Sfugge così l'altro che oltre ad essere una finzione può essere violento, può intraprendere azioni che non sono di corteggiamento ma di condivisione di immagini private, fino a poter divenire un ricattatore pericoloso o un *cyberstalker*. L'importanza dell'esteriorizzazione dell'aspetto fisico nei siti d'incontri acquisisce un grande valore sociale ed economico e diventa l'oggetto attraverso cui le persone vengono messe in competizione le une con le altre, fino alle manifestazioni di *hate speech*, *body-*

[15] S. GOTTSCHALK, *op. cit.*

[16] E. ILLOUZ, *Intimità fredde: le emozioni nella società dei consumi*, Milano, 2007, p. 121.

shaming, richieste di prostituzione online con prestazioni sessuali online con ricatti e minacce.

Le relazioni online hanno comportato un modo di vivere i rapporti sentimentali dettato dal consumismo e dall'ottimizzazione delle proprie scelte. Online si è portati a mostrare le proprie posture sentendosi liberi, ma non sempre quella libertà preserva la dignità e la possibilità per le donne di subire violazione, attacchi, stupri mediatici e anche violenze domestiche che sono figlie delle app.

Questo mercato diviene violento spesso per le più giovani che, in assenza di filtri e/o consapevolezza, non comprendono che la Rete "organizza la ricerca del partner letteralmente come un mercato, o, meglio, struttura la ricerca del partner nella forma di una transazione economica: trasforma l'io in un prodotto confezionato in concorrenza con altri su un mercato flessibile regolato dalla legge della domanda e dell'offerta"[17].

Ritrovandosi spesso dopo essersi fotografate con amiche, o da sole in posizioni che ne ritraggano il proprio look accattivante, la propria postura, finiscono in *dépliant* "a rischio", i cui maltrattanti sono autori al pari di coloro che violano nel reale le donne. Lo scambio non autorizzato di proprie immagini è un mercato che, come tutti i mercati, può sottrarsi all'etica e divenire feroci.

Una situazione sicuramente allarmante è che le preadolescenti, spesso le più esposte ad alcuni rischi, a volte si riprendono o fotografano in posizioni, ipotizzate spesso come sensuali, che poi condividono con amiche. La produzione fatta da loro stesse diviene poi oggetto diffamatorio per la diffusione che ne viene fatta da altri, agita contro di loro. Alle più giovani quasi viene sottratta la libertà di esprimere la propria autonomia nello spazio virtuale; pertanto, l'alfabetizzazione degli strumenti digitali e la gestione delle interazioni nelle chat deve essere oggetto di riflessione comune e ove possibile di norme giuridiche a tutela dei e delle meno consapevoli di alcune azioni che possono essere agite nello spazio virtuale.

[17] *Ibidem*, p. 132.

3. *Forme e impatti sociali della violenza nelle relazioni online*

La cyber-VAWG si manifesta in molti modi e forme, include, ma non si limita a, atti di incitamento all'odio – *hate speech*, *body-shaming*, *slut-shaming*, *doxing*, *cyberstalking*, *sextortion*, *gendertrolling*, *shallowfake*, violenza sessuale facilitata dalla tecnologia e distribuzione non consensuale di immagini intime altrimenti detta *revenge porn*. Queste pratiche mirano a controllare le donne e impedire loro di partecipare e prendere parte alle opportunità online, influendo negativamente sulla parità di genere. Le molestie online delle donne sono così sistemiche che colpiscono anche donne e ragazze che non hanno subito direttamente violenza[18].

Dal 2014 abbiamo numeri in crescita esponenziale di questo fenomeno. In Europa, già nel 2014, una donna su dieci prima di aver compiuto 15 anni aveva subito *cyberviolence* e il 5% *stalking* online. Sette donne su dieci, vittime di violenza online, hanno anche subito almeno una forma di violenza fisica/sessuale da parte del partner o dell'ex partner[19]. Negli Stati Uniti la situazione appare ancora peggiore: già nel 2014 una giovane su quattro subiva *stalking* o molestie sessuali mentre solo in tempi recenti, l'Istituto europeo per l'uguaglianza di genere (EIGE)[20] ha sollevato il problema della violenza cosiddetta virtuale contro donne e ragazze, denunciando la difficoltà nel reperimento di dati disaggregati rispetto al genere, nella difficoltà di classificare un fenomeno che è in realtà ibrido, complesso e parzialmente opaco.

Nel 2019 l'azienda di sicurezza informatica Kaspersky ha rilevato un aumento del 67% su base annua dell'utilizzo di *stalkerware* sui propri dispositivi mobili degli utenti a livello globale. I paesi europei

[18] M. ElSherif, E. Belding, D. Nguyen, *#notokay: Understanding Gender-Based Violence in Social Media*, in Y. Lin, Y. Mejova, M. Cha (eds.), *Eleventh International AAAI Conference on Web and Social Media*, Washington, 2017, vol. 11 n. 1, pp. 52-61.

[19] Women's Aid, *Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking*, 2014, disponible su https://www.womensaid.org.uk/virtual-world-real-fear/.

[20] European Institute for Gender Equality, *Cyber Violence against Women and Girls*, 2017, disponible su https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf.

più colpiti sono Germania, Italia e Francia. Più nel dettaglio, la Germania ha il maggior numero di vittime di *stalkerware*, raggiungendo la decima posizione su scala mondiale, mentre l'Italia è il secondo paese europeo per numero di vittime di *stalkerware* con 405 casi[21].

Per quanto riguarda l'uso di *stalkerware* nel mondo, Kaspersky ha analizzato 185 paesi, affermando che nel 2021 le vittime di *stalkerware* nel mondo sono state 32.694, classificando Russia, Brasile, Stati Uniti e India come i primi quattro paesi colpiti da tale fenomeno anche se per la *Coalition against stalkerware* il numero di vittime annualmente è stimato intorno a un milione[22].

Lo *stalkerware* è un fenomeno allarmante che si riferisce all'installazione di app, software e dispositivi che consentono di monitorare il computer o il telefono della vittima. Ciò che è allarmante è che gli *stalkerware* sono in grado di controllare ogni attività eseguita sul dispositivo preso di mira, come messaggi ricevuti e inviati, cronologia delle chiamate, cronologia web, foto e video e posizione. Inoltre, consentono all'autore di accedere al microfono e alla webcam per spiare, registrare o fare screenshot della vittima e manipolare tutti gli elettrodomestici per causare disagio. La maggior parte degli *stalkerware* richiede l'accesso fisico al telefono o al computer per essere installati; quindi, è strettamente collegato alla violenza perpetrata da un ex o attuale partner nella vita reale – offline. Infatti, la Rete europea per il lavoro con gli autori di violenza domestica ha rivelato che in Europa il 70% delle donne che ha subito *stalking* digitale è anche vittima di violenza sessuale o fisica perpetrata da un partner attuale o ex. Inoltre, il 71% degli autori di violenza domestica sorveglia le attività informatiche delle donne mentre il 54% utilizza uno *stalkerware* per monitorare il cellulare della vittima[23]. In Italia l'11% delle intervistate

[21] KASPERSKY, *Lo stato dello* stalkerware *nel 2022. Coalition Against* stalkerware, 2022, disponibile su https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/03/07152747/EN_The-State-of-Stalkerware_2022.pdf .

[22] KASPERSKY, *Lo stato dello* stalkerware *nel 2021*, *Coalition Against* stalkerware, 2021, disponibile su https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2022/04/12080239/IT_Lo-stato-dello-stalkerware_2021-1.pdf.

[23] European Network for the work with the Perpetrators of Domestic violence, *Destalk, detect and stop stalkerware and cyberviolence against women*, 2022, disponible su https://www.work-with-perpetrators.eu/destalk.

ha affermato di aver subito *stalking* digitale, mentre il 13% ha dichiarato di essere vittima di violenza domestica perpetrata da un partner.

La violenza online agisce come *trend amplifiers* perpetua e rafforza quei processi di discriminazione ed esclusione[24] delle donne dalla società; gli abusi e le aggressioni nelle relazioni online sono pratiche di violenza di genere già presenti nella società, amplificazione, dunque, di relazioni sociali che già esistono. Internet, i *new media* dialogano con gli elementi offline che costituiscono le nostre società, dando vita ad una struttura *onlife* dalla quale non è possibile sottrarsi o isolarsi, in quanto essa regola e pervade tutti gli ambienti in cui siamo immersi. La vita offline e quella online coesistono, rendendo possibili nuovi scenari di violenza di genere.

Così la non neutralità del digitale replica le dinamiche di potere esistenti nelle relazioni offline, basti pensare anche al *bias* di genere nell'architettura degli algoritmi[25]. Un esempio ne è DeepNude.now che ostenta esplicitamente la sua capacità di spogliare liberamente il corpo delle donne e non quello degli uomini. Come vedremo più avanti, questa app diffonde notizie false o anche una iperfalsicifazione iperrealistica di contenuti audio e visivi generati dalla Intelligenza Artificiale. Il *deepfake* è un fenomeno recente, ma in crescita, che consiste nell'utilizzare algoritmi e Intelligenza Artificiale per creare immagini o video altamente realistici. Il *deepfake* comprende la ricreazione facciale, lo scambio di volti, clip audio e la sincronizzazione labiale. La manipolazione è così accurata e veritiera che il contenuto sembra reale, causando gravi ripercussioni, come rivelato da un rapporto condotto da Deeptrace su un'azienda con sede ad Amsterdam: il 96% dei video *deepfake* consiste in pornografia *deepfake* non consensuale e le donne, in particolare attrici e musiciste, sono il bersaglio principale[26]. Di conseguenza, le donne si ritrovano vittime di *revenge porn* senza nemmeno aver scattato una foto di nudo. Tale tecnologia è stata definita come l'ultima arma anti-donne poiché danneggia e prende di mira le donne

[24] J. VAN DIJK, *op. cit*.

[25] C. LUTZ, *Digital inequalities in the age of artificial intelligence and big data*, in *Human Behavior and Emerging Technologies*, 2019, vol. 1, n. 2, pp. 141–148.

[26] H. AJDER, F. CAVALLI, L. CULLEN L., G. PATRINI, *Deepfakes: Landscape, Threats, and Impact*, 2019, disponible su https://sensity.ai/reports/.

in modo sproporzionato, causando loro disagio psicologico, danni economici e stigma sociale[27].

Anche il *Panel for the Future of Science and Technology* (STOA) dell'Unione europea ha riferito che il *deepfake* non prende più di mira le celebrità femminili, ma la sua accessibilità ha reso possibile la creazione di *deepfake* utilizzando persone non famose, sollevando preoccupazioni sull'uso di questa tecnologia per la realizzazione di *revenge porn*, *sextortion* e altre forme di violenza contro le donne[28].

Una delle app per computer di *deepfake* più diffuse è DeepNude. Quest'ultima è stata creata nel giugno 2019 e ha consentito agli utenti di manipolare le foto delle donne sostituendo i loro vestiti con genitali femminili. Ciò che colpisce di più è il fatto che questa app è stata programmata per funzionare solo sul corpo delle donne, risultando impossibile manipolare anche le foto degli uomini. La creazione di DeepNude ha causato un effetto a cascata che ha permesso la diffusione e la mutazione in app più precise e sofisticate, rendendone impossibile la rimozione. Secondo una classifica delle prime dieci del giugno 2022 le app di "spogliarello" più influenti e diffuse in base alla loro influenza globale e locale sono: Deepfake e DeepNudenow.com. Anche in Italia il caso del *deepfakesex* accaduto presso una scuola media superiore di Roma, con l'app Bikini-Off con la quale adolescenti hanno spogliato le proprie compagne di scuola con una applicazione di ChatbotGPT e poi hanno fatto circolare le immagini e umiliato le loro compagne, come non annoverarlo come una *cyberviolence* di genere a danno delle giovani vittime.

Altro fenomeno associato al *deepfake* è lo *shallowfake*. Quest'ultimo consiste nel manipolare video già esistenti. I tre modi principali di manipolare un video sono estrapolare scene dal contesto, aggiungere o omettere contenuti dalla versione originale e trasformare

[27] GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women. Council of Europe's Violence Against Women Division*, 2021, disponibile su https://www.coe.int/en/web/istanbul-convention/-/grevio-publishes-its-general-recommendation-no-1.

[28] European Parliamentary Research Service, *Panel for the Future of Science and Technology*, *Tackling deepfakes in European policy*, 2021 disponibile su https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf.

o falsificare il contenuto originale alterando il linguaggio del corpo o il discorso. Di solito, i bersagli dello *shallowfake* sono personaggi pubblici come politici e giornalisti. Su tutti valga l'esempio di Nancy Pelosi che è stata vittima di troll che hanno manipolato il suo video rallentando il suo discorso e facendola borbottare per farla sembrare ubriaca[29].

Le donne e le ragazze cybernaute sono più a rischio di molestie e umiliazioni degli uomini o di altri gruppi sociali[30]. Un rapporto del 2018 commissionato dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA)[31] stima che la donna europea su 10 (11%) abbia subito qualche forma di molestia informatica o *cyberstalking* dall'età di 15 anni. In particolare, le giovani donne e le ragazze sembrano essere particolarmente vulnerabili alla violenza online[32].

Sebbene la cyber-VAWG rappresenti un problema sociale relativamente nuovo, questa forma di violenza ha ricevuto un crescente riconoscimento nel dibattito pubblico italiano, in particolare in rapporto agli episodi di distribuzione non consensuale di immagini intime.

In Italia, la violenza online ha iniziato a essere discussa nel 2016, dopo il suicidio di Tiziana Cantone, nota anche come Tiziana Giglio, una donna che il 13 settembre 2016, all'età di trentatré anni, si suicidò dopo la diffusione in Rete, senza il suo consenso, di alcuni suoi video pornografici amatoriali. La sua storia ha avuto un profondo impatto sull'opinione pubblica, come la "pornografia di vendetta", diventata una questione di preoccupazione significativa nel dibattito pubblico

[29] R. BARNETT, C. RIVERS, *Deepfake: The Latest Anti-Woman Weapon. Women's e-news*, 2022, disponibile su https://womensenews.org/2022/05/deep-fakes-the-latest-anti-woman-weapon.

[30] A. K. FANSHER, R. RANDA, *Risky Social Media Behaviors and the Potential for Victimization: A Descriptive Look at College Students Victimized by Someone Met Online*, in *Violence and Gender*, 2019, n. 6, pp. 115–123.

[31] European Union Agency for Fundamental Rights, *Fundamental Rights Report 2018*, 2018, disponibile su https://fra.europa.eu/en/publication/2018/fundamental-rights-report-2018.

[32] European Institute for Gender Euqality, *Understanding Intimate Partner Violence in the EU: the Role of Data*, 2019, disponible du https://eige.europa.eu/publications/understanding-intimate-partner-violence-eu-role-data.

italiano sulla violenza di genere[33]. I recenti cambiamenti nel quadro legislativo italiano riflettono l'attenzione rivolta a questa specifica forma di cyber-VAWG. Nel 2019 l'Italia ha approvato il noto "Codice Rosso" (Legge 69/2019), per soddisfare gli standard stabiliti dalla Convenzione di Istanbul 2011, trattato proposto dal Consiglio d'Europa per prevenire e contrastare la violenza contro le donne e la violenza domestica, che il governo italiano ha ratificato solo nel 2014. Il "Codice Rosso" non solo inasprisce le pene per i maltrattanti ma ha introdotto un nuovo reato che criminalizza la divulgazione non autorizzata e non consensuale di immagini e video sessualmente espliciti di altri, riconoscendo pene anche per i partner intimi che perpetrano questo tipo di violenza.

Gli studiosi criticano sempre più l'uso popolare del termine *revenge porn* per descrivere il comportamento che consiste nella distribuzione, in genere online, di immagini intime di natura sessuale, acquisite con o senza il consenso della persona raffigurata nell'immagine o anche ottenute consensualmente e poi distribuite senza consenso, nonché manipolate senza consenso[34].

Infatti, tale termine è stato considerato fuorviante poiché la parola "vendetta" attribuisce alla vittima una connotazione negativa come se la condotta fosse una conseguenza delle azioni della vittima perciò accettabile o da giustificare. Sembrerebbe sfuggire che il fenomeno può essere innescato da vari motivi come vendetta, estorsione, notorietà o noia e può essere perpetrato in diverse forme come *sextortion*, *upskirting*, *doxing* e *deepfake*. Così come il termine *revenge* anche quello di porno deve essere tradotto e interpretato come abuso sessuale non consensuale. Infatti, il termine "abuso sessuale basato sulle immagini" racchiude i tre comportamenti principali che caratterizzano tale condotta: la diffusione non consensuale di immagini di nudo o sessuali, la creazione non consensuale di immagini di sesso o di nudo, comprese quelle alterate digitalmente come i *deepfake*; e le minacce di diffusione

[33] C. GIUS, *(Re)thinking gender in cyber-violence. Insights from awareness-raising campaigns on online violence against women and girls in Italy*, in *MEDIA EDUCATION – Studi, ricerche e buone pratiche*, 2023, vol. 14, n. 2, pp. 95-106.

[34] European Institute for Gender Equality, *Combating Cyber violence against women and girls*, 2022, disponibile su https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls.

di immagini di sesso o di nudo immagini[35]. Le relazioni online mostrano come la violenza digitale contro le donne è duplice nello spazio digitale: da una parte si pongono il *revenge porn* e la sua questione, il *cyberstalking*, l'*upskirting*, lo *stalkerware* e, dall'altro, il fenomeno che ha avuto inizio con Facebook, Instagram, Twitter, TikTok: l'*hate speech*.

Il discorso d'odio basato sul genere contro le donne è profondamente radicato in una cultura patriarcale e misogina che legittima, fomenta e giustifica. È perpetrato principalmente online, con pericolose ricadute offline, mettendo a tacere le sue vittime. È pervasivo poiché si propaga rapidamente e con forza, è difficile da contenere ed è molto pericoloso poiché inarrestabile, riproducibile. Non ha bisogno di essere innescato, al contrario è latente e pronto a manifestarsi senza alcun incitamento[36].

Pertanto, questo fenomeno viene affrontato in vari modi, come "discorso d'odio sessista", "discorso d'odio basato sul genere/sesso", e "discorso d'odio basato sul genere online"[37].

Il barometro dell'odio di Amnesty International ha rivelato che un attacco su tre rivolto a una donna è sessista, soprattutto quando il contenuto riguarda "donne e diritti di genere"[38]. Adrine Van der Wilk ha sostenuto che il 3,1% dei contenuti segnalati alle piattaforme di social media nell'UE riguardava incitamento all'odio illecito contro identità di genere o sesso. Gli attacchi sessisti contro le donne assumono molte forme come ri-vittimizzazione, *revenge porn*, *slutshaming*, minacce sessualizzate e brutali di stupro, violenza e morte; commenti offensivi sulla sessualità, sull'orientamento sessuale, sull'aspetto o i ruoli di genere. Tale attacco può essere perpetrato implicitamente attraverso l'uso di presunte battute, falsi complimenti, nascondendosi dietro l'umorismo

[35] Australian Institute of Criminology, A. FLYNN, N. HENRY, N., A. POWELL (eds.), *Image-based sexual abuse: victims and perpetrators*, 2019, n. 572, pp. 1-182, disponibile su https://www.aic.gov.au/sites/default/files/2020-05/imagebased_sexual_abuse_victims_and_perpetrators.pdf.

[36] AMNESTY INTERNATIONAL, *Barometro dell'odio. Sessismo da tastiera*, 2020, p. 14, disponibile su https://d21zrvtkxtd6ae.cloudfront.net/public/uploads/2020/03/15212126/Amnesty-Barometro-odio-aprile-2020.pdf.

[37] E. ABBATECOLA, *Revenge Porn o D.I.V.I.S.E? Proposta per cambiare un'etichetta sessista*, in *AG About gender*, 2021, vol. 10, n. 19, pp. 401-413.

[38] *Ibidem.*

per ridicolizzare e umiliare la vittima[39]. Questa forma di violenza è indissolubilmente legata con l'intersezionalità, agita spesso contro donne con identità intersecanti come le donne in politica, nere, giornaliste, blogger, difensori dei diritti umani. Sono prese di mira online con minacce di stupro, di discorsi di odio, in particolare quelle dedicate ai diritti delle donne, le donne parte di comunità minoritarie, le comunità LGBTQ+.

Nonostante l'incitamento all'odio basato sul genere online possa essere perpetrato anche offline, la dimensione online ha alcune caratteristiche peculiari: amplificazione, durata, riproducibilità "ricercabilità del contenuto", l'uso di meme, neologismi, hashtag, emoticon, errori di ortografia, formazione di un nuovo odio creativo[40].

Inoltre, rispetto agli effetti dell'incitamento all'odio online a causa della suddetta durabilità, ricercabilità e rapida diffusione di contenuti d'odio, questi ultimi sono indelebili, permanenti, amplificando gli effetti dannosi che possono essere psicologici, fisici, economici e sociali e contribuendo alla ri-vittimizzazione, fino a causare l'abbandono delle piattaforme dei social media da parte delle donne, ampliando il divario digitale di genere preesistente. Pertanto, l'incitamento all'odio, insieme ad altre forme di violenza di genere contro le donne, non deve essere visto come un fenomeno isolato che prende di mira un singolo individuo, ma come un fenomeno sociale emergente in grado di mettere a repentaglio l'uguaglianza e i diritti delle donne. In altri termini, come ricorda Van Dijk[41], la struttura a rete pervade tutti gli aspetti della società, ma vi è ancora spazio per una scelta consapevole: gli effetti di questa struttura non sono unidirezionali, ma duali e ciò può creare opposizioni. Infatti, i *new media* portano alla connessione, così come alla disconnessione, poiché ci sarà sempre chi trae vantaggio, partecipa e decide all'interno di questi meccanismi e chi invece rimane escluso, nel nostro caso le donne.

[39] European Parliament, Directorate-General for Internal Policies of the Union, A. WILK, *Cyber violence and hate speech online against women*, European Parliament, 2018, p. 28, disponibile su https://data.europa.eu/doi/10.2861/738618.

[40] F. FALOPPA, *#Odio. Manuale di resistenza alla violenza delle parole*, Milano, 2020.

[41] J. VAN DIJK, *op.cit.*

4. *Considerazioni e azioni future*

La violenza online prende di mira le donne in modo sproporzionato per il solo fatto che sono donne. Questo, come già accennato, è la conseguenza di una società patriarcale, sessista. Ciò che fa la dimensione online è solo amplificare ed esporre una struttura sociale disfunzionale già esistente. Dall'inizio della pandemia di Covid-19, la violenza online contro le donne, insieme ad altre forme di violenza di genere, ha subito un aumento drammatico. Uno dei motivi principali è l'aumento dell'utilizzo di Internet, che in alcuni paesi è raddoppiato durante il lockdown, esponendo le donne in modo esponenziale. Tutte le donne e le ragazze sono a rischio in una società digitale piena di odio e misogina, e alcune categorie di donne lo sono ancora di più. Come affermato in precedenza, le donne con identità intersecanti, ovvero donne nere, asiatiche e appartenenti a minoranze etniche, donne disabili, lesbiche, transgender, bisessuali, donne non binarie e donne appartenenti a minoranze religiose sono tra quelle maggiormente oggetto di abusi e molestie online. Inoltre, anche le giornaliste, le donne difensori dei diritti umani, le donne femministe, le donne politiche sono altamente esposte alla violenza nel mondo digitale. Come già ricordato nel digitale il binomio tradizione-mutamento, sfera pubblica e sfera privata delle donne ritorna prepotentemente, cioè quello che attiene alla tradizionale esclusione delle donne dalla sfera pubblica, e dunque, anche dalla partecipazione ai dibattiti politici. Alcuni studiosi hanno spiegato questo fenomeno facendo riferimento a temi come l'accessibilità, i mezzi, l'etnia e la classe socioeconomica d'appartenenza. Questi sono tutti concetti riferibili all'intersezionalità, caratteristica tipica del femminismo della quarta ondata e dunque anche dell'attivismo digitale femminista[42]. Un'altra leva particolarmente significativa nell'analisi della partecipazione femminile al dibattito politico è rappresentata dall'età. Infatti, vari studi hanno dimostrato che

[42] E. MUNRO, *Feminism: A fourth wave?*, in *Political Insight*, 2013, vol. 4, n. 2, pp. 22–25 e European Parliamentary Research Service, *Panel for the Future of Science and Technology. Tackling deepfakes in European policy*, 2021, disponibile su https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf.

l'età rappresenta in generale un aspetto critico quando si parla di avere una voce politica. In questo, molte donne che prendevano parte a queste ricerche, hanno trovato in Twitter un'opportunità non solo per imparare ma anche e soprattutto, per dialogare e così farsi ascoltare. Tra le partecipanti, le più giovani hanno anche evidenziato la possibilità di sfruttare le informazioni acquisite attraverso i social media per informare a loro volta i compagni di scuola e gli amici[43]. Dall'altro lato però gli studiosi si stanno preoccupando di studiare anche l'aumento di (nuove) forme di misoginia nei confronti del femminismo e di alcune femministe in particolare, anche alla luce dello sviluppo tecnologico e dunque della diffusione di piattaforme come i social. La maggior parte delle femministe che hanno preso parte alle ricerche ha dichiarato di aver avuto esperienza di *trolling*, negatività e ostilità nei loro confronti e in generale di aver dovuto fronteggiare varie forme di abusi online[44]. Un esempio di questa misoginia è il caso della vincitrice del premio Nobel americano-filippino Maria Ressa, che secondo il documento di discussione di ricerca pubblicato dall'UNESCO rappresenta uno degli attacchi più feroci orchestrati contro una giornalista con valori improntati al femminismo e ai diritti delle minoranze. In effetti, gli attacchi a Maria Ressa, attualmente incarcerata, le sono diretti principalmente perché è una donna autonoma, libera e femminista. Inoltre, gli abusi prendono di mira anche la sua sessualità, il suo colore della pelle e la sua doppia cittadinanza, definendola una traditrice.

Gli esempi e classificazioni di *cyberviolence* presentati ripropongono il quesito se siamo veramente sicuri che minacce quali *deepfake* e *cyberstalking* – in altri termini la *cyberviolence* – non lasciano segni fisici. Credo che i segni, meglio le tracce, siano indelebili e non rimovibili.

Bisogna scegliere di mettere al centro dell'attenzione i più e le più giovani in una prevenzione anche *peer to peer* circa le relazioni online, poiché bisogna andare oltre il giusto e consapevole intervento del diritto con norme che, come ricordava Habermas in *Morale diritto e po-*

[43] K. MENDES, J. RINGROSE, J. KELLER, *#MeToo and the promise and pitfalls of challenging rape culture through digital feminist activism*, in *European Journal of Women's Studies*, 2018, vol. 25, n. 2, pp. 236-246.

[44] *Ibidem.*

litica, non possono regolare le relazioni sociali da sole. Infatti, la legalità può attingere legittimità solo da una razionalità procedurale ricca di contenuti morali, culturali e sociali. In altri termini una norma giuridica da sola non può risolvere i problemi di una società complessa nella quale le relazioni sociali possono comprendersi interpretarsi e spiegarsi, considerando i valori le norme e le sanzioni di contesto nelle quali le azioni si compiono. In questo scenario raggiungere e informare i e le più giovani è molto importante perché costituiscono una parte fondamentale di quello che può essere un mondo che, se alfabetizzato consapevolmente, può fare la differenza lungo l'affermazione della parità uomo donna. Occorre intraprendere un percorso di prevenzione di queste forme di violenza online che non siano solo il contrasto o il contenimento di natura giuridica: la questione più importante è come la violenza informatica, tecnologica, digitale non sia altro che un *continuum* della violenza di natura tradizionale. Da quasi trent'anni la conferenza di Pechino, 4 settembre 1995, ha stabilito un programma rivoluzionario per i diritti delle donne. I rappresentanti di 189 nazioni hanno adottato all'unanimità la Dichiarazione e la Piattaforma d'azione di Pechino. Questo progetto storico articolava una visione di pari diritti, libertà e opportunità per le donne – ovunque, indipendentemente dalle circostanze – che continua a dare forma all'uguaglianza di genere e ai movimenti delle donne in tutto il mondo. La suddetta Dichiarazione ha definito la violenza di genere una disparità di accesso a uomo e donna giocata su una dis-equità e disuguaglianza dell'accesso alle risorse e al potere, il che dunque scatena un binomio, quello ormai noto come dominio-violenza. Tuttavia, ancora questa parità non è presente e le forme di violenza agite nei luoghi reali oggi trovano spazio consistente e dis-equità anche online. Così nel 2023 il fenomeno della violenza digitale di genere è entrato in una raccomandazione di UN Women[45] per migliorare la costruzione di percorsi di parità di egua-

[45] Cfr. UN Women Regional Office for Europe and Central Asia, *The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia, Office for Europe and Central Asia*, 2023, disponibile su https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia .

glianza e giustizia e contenimento di qualsiasi forma di violenza contro le donne, anche quella digitale.

È necessario più che mai pianificare e intensificare campagne di sensibilizzazione incentrate sulla *cyberviolence* contro donne e ragazze, evidenziando l'urgenza di un approccio educativo che integri una prospettiva di genere nella creazione di percorsi di alfabetizzazione specificamente rivolti agli ambienti digitali "non neutri" dove si sviluppano nuove relazioni improntate anche all'odio e al conflitto, per promuovere *safety Word Wide Web* (WEB) e trasmettere conoscenze sui diritti e le responsabilità digitali. Questo vuol dire riconoscere che anche la cyber-VAWG è una forma distinta di violenza online di genere, e pertanto deve essere considerata nelle declinazioni normative del diritto, senza però trascurarne la sua dimensione quale pratica sociale. Tale prospettiva è fondamentale per garantire, tra le altre cose, che gli sforzi di educazione ai media non perpetuino gli stereotipi di genere[46] e promuovere strategie di benessere di genere che non si concentrino solo sullo sviluppo di competenze, ma considerino anche il contesto sociale e culturale in cui le pratiche digitali prendono forma. Inoltre, non bisogna dimenticare che l'Unione europea ha lanciato il progetto DeStalk con l'obiettivo di formare professionisti che lavorano con le vittime o in programmi per autori, ufficiali di polizia, enti locali e stakeholder in modo da combattere la violenza informatica contro le donne. Tuttavia, il programma deve ancora essere attivato[47].

Le cicatrici non si vedono, ma ci sono: "la rete non dimentica mai" oggi si vive *on-life* e c'è chi dice come Rushkoff[48] che nel digitale non è sparita la separazione tra offline e online, tra l'attività pubblica e quella privata, ma la distanza tra ora e allora, il passato si è precipitato nel presente e non è più su una scala appropriata o perfino prevedibile, è fuori dalla portata. Un incidente dimenticato, una violenza dimenticata, un *hate speech* può ricomparire nel presente come un'esplosione

[46] J. RINGROSE, L. HARVEY, R. GILL, S. LIVINGSTONE, *Teen Girls, Sexual Double Standards and 'Sexting: Gendered Value in Digital Image Exchange*, in *Feminist Theory*, 2013, vol. 14, n. 3, pp. 305-323.

[47] European Network for the work with the Perpetrators of Domestic violence, *op. cit.*

[48] D. RUSHKOFF, *Present Shock: Where Everything Happens Now*, New York, 2013.

minacciando la reputazione, il lavoro, la faccia, il matrimonio, la vita quotidiana di una donna. Tutto questo ci porta a dire alle più giovani di utilizzare certo tutto ciò che la tecnologia gli consente, perché abbiamo detto all'inizio TikTok e anche per i giovani una forma di attivismo politico, su cui ragionare di alcuni temi: loro ne sanno molto; ma sono tante e innumerevoli le memorie digitali che non vengono poi eliminate. Anche le foto, i video, le parole di un contesto specifico usate possono essere decontestualizzate, riprodotte all'infinito e persino ricontestualizzate, e relazioni e interazioni private, che si pensa di comunicare a pochi selezionati, possono poi divenire pubbliche in modo addirittura imbarazzante. Questo è quello a cui le ragazze possono, in particolare, andare incontro. Questa è stata la vergogna di alcune donne che hanno subito cyberviolenza e hanno anche compiuto gesti estremi: i confini nell'ambiente digitali sono labili e non tracciabili e lasciano idea di maggiore impunità, irresponsabilità e non consapevolezza a chi le compie.

Abstract

Le relazioni online come l'amore, le emozioni non sono solo una questione privata della manifestazione della violenza di genere ma diventano una pratica pubblica con le conseguenti azioni e reazioni che ne scaturiscono quando questa arriva ad essere presentata, postata e pubblicata in Rete. La cultura emotiva e i diversi *habitus* emotivi che si esprimono nelle relazioni sentimentali, perpetuando forme di controllo sociale, in forme talvolta meno evidenti rispetto al passato, ma altrettanto pericolose poiché senza limiti e né confine. Ciò che finisce online lascia tracce permanenti, riproducibili e policroniche e indelebili anche nella vita offline delle donne.

KEYWORDS: cyber-VAWG – genere – emozioni – disuguaglianza – impatto delle tecnologie digitali

VIOLENCIA DE GÉNERO EN LAS RELACIONES ONLINE. UNA REFLEXIÓN SOCIOLÓGICA

Las relaciones en línea, como el amor y las emociones, no son solo un asunto privado de manifestación de la violencia de género, sino que se convierten en una práctica pública con las consecuentes acciones y reacciones que surgen cuando se presentan, publican o comparten en la red. La cultura emocional y los diferentes hábitos emocionales que se expresan en las relaciones de pareja perpetúan formas de control social que, aunque menos evidentes que en el pasado, siguen siendo peligrosas porque no tienen límites ni fronteras. Lo que se sube a Internet deja huellas permanentes, reproducibles, policrónicas e indelebles en la vida fuera de línea de las mujeres.

PALABRAS CLAVE: cyber-VAWG – emociones – género – desigualdad – impactos de la tecnología digital

LE NORME SULLA LOTTA ALLA VIOLENZA DI GENERE ONLINE NEL CONTESTO DELLA REGOLAMENTAZIONE INTERNAZIONALE ED EUROPEA DI INTERNET: ALCUNE QUESTIONI GENERALI E DI METODO

Gianpaolo Maria Ruotolo[*] *- Angela Maria Gallo*[**]

SOMMARIO: 1. La regolamentazione di Internet e il diritto internazionale. Il loro rapporto biunivoco e l'utilizzabilità di norme pregresse. – 2. Internet come bene globale e patrimonio comune dell'umanità: le conseguenze di questa qualificazione sul relativo regime giuridico. – 3. Neutralità tecnologica ed equivalenza normativa come strumenti ermeneutici. – 4. Alcuni caratteri generali della disciplina UE del contesto digitale. – 5. La direttiva 2024/1385 e gli obblighi di penalizzazione: la necessità di esplicita previsione della "equivalenza normativa" in materia penale e un caso di sua violazione.

1. *La regolamentazione di Internet e il diritto internazionale. Il loro rapporto biunivoco e l'utilizzabilità di norme pregresse*

Il termine Internet, di cui attualmente web, Rete e cyberspazio sono generalmente considerati sinonimi, rappresenta la contrazione della locuzione "*interconnected networks*", "Reti interconnesse": Internet è infatti proprio un sistema di apparecchiature connesse tra loro da sottoreti che comunicano attraverso una serie di protocolli che hanno il compito di dettare le "regole" per il trasferimento dei dati[1]. Con le

[*] Professore ordinario di Diritto internazionale, Università di Foggia. Email: gianpaolo.ruotolo@unifg.it. È autore dei parr. 1-4.

[**]Dottoranda di ricerca in Ordine internazionale e diritti umani, Università di Roma "La Sapienza". Email angelamaria.gallo@uniroma.it. È autrice del par. 5.

[1] La struttura di Internet, con una buona approssimazione, può essere descritta come un sistema con una miriade di ramificazioni, in cui ogni nodo è collegato a molti altri: una sua rappresentazione grafica, una sorta di mappa geografica del cyberspazio, detta *Peacock Map* per la sua somiglianza alla coda di un pavone, è stata elaborata tempo fa da H. BURCH e B. CHESWICH ed è consultabile all'indirizzo www.cheswick.com. Per un'analisi generale dei connessi profili giuridici di diritto in-

medesime espressioni si fa pure riferimento, a volte e atecnicamente, all'insieme dei dati conservati sulle macchine connesse.

In questa sede faremo riferimento ad Internet come allo strumento attraverso il quale viaggiano dati che assumono forme e contenuti differenti, alcuni dei quali, per quanto qui ci interessa, sono alla base di alcune delle condotte oggetto della direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio del 14 maggio 2024 sulla lotta alla violenza contro le donne e alla violenza domestica, di cui si occupa questo Volume.

Sin dalla sua diffusione a livello globale, è il caso di ricordarlo, si è discusso delle modalità di disciplina giuridica della Rete, operazione che appariva non scontata anche in ragione della sua architettura, costituita, come dicevamo, da un insieme di sottoreti connesse tra loro in numerosi punti: in conseguenza della difficoltà di localizzare le informazioni e i comportamenti che vi hanno luogo, quindi, si affermavano in dottrina diverse teorie circa le modalità e gli strumenti più idonei alla sua regolamentazione, alcune delle quali tra loro antitetiche[2].

Un primo orientamento muoveva dal presupposto che l'inesistenza di frontiere fisiche avrebbe caratterizzato Internet come uno spazio senza frontiere; quindi, difficile da regolare ("*a legal void*"[3]), nel quale era ardua la localizzazione dei comportamenti che vi hanno luogo, con conseguente difficoltà dell'individuazione del diritto (statale) applicabile a una determinata fattispecie, nonché del giudice competente a dirimere eventuali controversie.

Inoltre, la dottrina in parola evidenziava pure i problemi derivanti da una diversa, e quindi frammentaria, regolamentazione statale dei fenomeni e sui rischi di sovrapposizione di varie regole, alcune peral-

ternazionale, anche per ulteriori riferimenti, ci permettiamo di rinviare a G.M. RUOTOLO, *Internet (Diritto internazionale)*, in *Enciclopedia del diritto*, Milano, 2014, p. 548 ss.

[2] J. GOLDSMITH, T. WU, *Who Controls the Internet? Illusions of a Borderless World,* Oxford, 2006; J. KULESZA, *International Internet Law*, New York, 2012. Per una interessante ricostruzione si veda, da ultimo, G. DELLA MORTE, *Limiti e prospettive del diritto internazionale del cyberspazio*, in *Rivista di diritto internazionale*, 2023, n. 1, p. 6 ss.

[3] A. GIGANTE, *Blackhole in Cyberspace: The Legal Void in the Internet*, in *J. Marshall Journal of Computer & Information Law*, n. 3, 1997, p. 413 ss.

tro suscettibili di applicazione extraterritoriale ("*spillover*"[4]). I sostenitori di questa teoria ritenevano quindi che fosse necessario concepire un *corpus* di norme prodotte *ex novo e autonomamente* dagli utenti della Rete, il quale avrebbe dato origine ad un *tertium genus* (né statale né internazionale) di diritto, il c.d. *cyber-law*.

Si tratta di un orientamento che è ormai sostanzialmente tramontato.

Altra parte della dottrina evidenziava come Internet fosse essenzialmente un nuovo mezzo di comunicazione, la cui natura transnazionale imponeva un'operazione di armonizzazione degli ordinamenti statali, da realizzarsi attraverso l'individuazione di principi di diritto internazionale di varia natura (consuetudinaria, pattizia, di *soft law* e anche "informale"[5]) per mezzo dei quali costruire un quadro giuridico generale comune a tutti gli Stati[6].

Altri ancora, evidenziavano come la Rete – che presenta una struttura mutevole, in quanto determinata dall'insieme delle apparecchiature che la compongono (*hardware*), ma, soprattutto, dal *software* (il "codice" informatico) che ne consente e disciplina l'uso – sarebbe da regolare attraverso il suo codice informatico, appunto, il quale, a sua volta, dovrebbe essere informato da norme giuridiche uniformi, volte essenzialmente a decidere quali siano i valori che devono essere assunti come parametro di riferimento dal primo[7].

[4] Per un'esposizione dell'orientamento brevemente illustrato si vedano, fra gli altri, D.J. POST, *Law and Borders. The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, n. 48, p. 1367; D.J. POST, *In Search for Jefferson's Moose*, Oxford, 2009, *passim*.

[5] Per un'analisi e altri riferimenti ci permettiamo di rinviare a G.M. RUOTOLO, *Fragments of Fragments. The Domain Name System Regulation: "Global" Law or Informalization Of The International Legal Order?*, in *Computer Law & Security Review*, 2017, n. 2, p. 159 ss.

[6] J.L. GOLDSMITH, *Against Cyberanarchy*, in *University of Chicago Law Review*, 1998, p. 1240 ss.; J.P. TRACHTMAN, *Cyberspace, Sovereignity, Jurisdiction and Modernism*, in *Indiana Journal of Global Legal Studies*, 1998, p. 568 ss.; S.S. MODY, *National Cyberspace Regulation: Unbounding the Concept of Jurisdiction*, in *Stanford Journal Int'l Law*, 2001, n. 2, p. 382 ss.

[7] L. LESSING, *Code - Version 2.0*, Cambridge, 2006, sostiene che Internet può essere controllata mediante forze "*in large part exercised by technologies [...], backed by the rule of law (or at least what's left of the rule of law). The challenge for our generation is to reconcile these two forces*".

Orbene, in siffatto contesto appariva comunque chiara l'impossibilità di regolare Internet *esclusivamente* attraverso mezzi giuridici di diritto interno, che nella prassi dimostravano da subito di essere non pienamente efficaci[8].

Evidente, quindi, come quello internazionale rappresenti l'ordinamento elettivo per una sorta di disciplina "generale" di Internet, quanto meno attraverso la fissazione di alcuni principi in grado di delimitare la *domestic jurisdiction* degli Stati in materia[9], e ciò non solo attraverso norme specifiche ma anche (e forse soprattutto) mediante norme e categorie giuridiche preesistenti, cioè attraverso l'applicazione *analogica* di norme di diritto internazionale generale e pattizio, nonché di *soft law*, preesistenti, originariamente nate per disciplinare situazioni "reali"[10].

In questo senso depone ormai da tempo la prassi, dalla quale emerge in più casi e nei contesti più disparati la volontà degli Stati (e non solo: si pensi al fatto che l'organo di soluzione delle controversie approntato da Meta, l'*Oversight Board*, applica esplicitamente il diritto internazionale[11]) di applicare il diritto internazionale ad Internet e alle fattispecie online.

Peraltro, è il caso di evidenziare l'esistenza di un rapporto biunivoco intercorrente tra ordinamento internazionale ed Internet, inteso come la capacità del primo di regolamentare il secondo, e del secondo di influenzare il primo in conseguenza della diffusione di informazioni per il suo tramite. Ora, sebbene questo fenomeno di mutua influenza non sia di nuovo conio, in quanto già riscontrato in altri ambiti a se-

[8] Per una ricostruzione della prassi in materia si rimanda a G.M. RUOTOLO, *Fragments of Fragments. The Domain Name System Regulation: Global Law or Informalization of the International Legal Order?* cit., p. 159 ss.

[9] G.M. RUOTOLO, *Abolish the Rules Made of Stone? Contemporary International Law and the Models of Internet Regulations,* in *The Italian Review of International and Comparative Law*, 2021, p. 252.

[10] Su questo orientamento, criticamente, v. J. D'ASPREMONT, *Cyber Operations and International Law: An Interventionist Legal Thought* in J*ournal of Conflict & Security Law,* 2016, p. 575 ss.

[11] J. ODERMATT, *International and European Law before the Meta Oversight Board*, in *Völkerrechtsblog.org*, 2024.

guito del progresso tecnologico[12], l'influenza che Internet esercita sugli ordinamenti giuridici, e in particolare su quello internazionale, differisce dai precedenti casi, in quanto essa appare in grado di influenzare non solo il *contenuto materiale* delle norme ma anche alcuni loro *procedimenti* di formazione e applicazione[13].

2. *Internet come bene globale e patrimonio comune dell'umanità: le conseguenze di questa qualificazione sul relativo regime giuridico*

Le caratteristiche intrinseche della Rete (esauribilità di alcune delle sue risorse[14], indivisibilità[15], natura *multistakeholder*[16]), che implica-

[12] Da sempre il progresso tecnologico informa di sé gli ordinamenti giuridici, compreso quello internazionale: si pensi alle numerose norme adottate per disciplinare i comportamenti degli Stati nello spazio extra-atmosferico, una per tutte la Convenzione sulla responsabilità internazionale per danni causati da oggetti spaziali, aperta alla firma il 29 marzo 1972 ed entrata in vigore l'1 settembre dello stesso anno, o ancora, a proposito dell'uso dell'orbita geostazionaria, l'Accordo sull'Organizzazione internazionale per i satelliti per telecomunicazioni, c.d. Convenzione Intelsat, oppure, per quanto concerne la ricerca scientifica nell'alto mare, la Convenzione delle Nazioni Unite sul diritto del mare. Tutti questi accordi sono stati conclusi solo quando il progresso tecnologico li ha resi necessari.

[13] In questa sede ci è impossibile analizzare compiutamente questo aspetto, per il quale ci permettiamo per brevità di rinviare, anche per ulteriori rimandi, a G.M. RUOTOLO, *The Impact of the Internet on International Law: Nomos without Earth?*, in *Informatica e diritto*, 2013, p. 7 ss.

[14] Si pensi al problema della c.d. *IPcalypse*, ossia dell'impossibilità di assegnare nuovi indirizzi IPv4 in quanto esauriti, che ha comportato la creazione di un nuovo protocollo, denominato IPv6, il quale consente di assegnare un numero maggiore di indirizzi IP rispetto alla precedente versione. Per approfondimenti, J. MALCOLM, *The Space Law Analogy to Internet Governance*, in *Journal of Law, Information and Science*, 2007, p. 57 ss.

[15] La Rete rappresenta una risorsa indivisibile, dal momento che mantiene la sua capacità di mezzo di comunicazione di incommensurabile potenza solo se non viene frammentata in una serie di sottoreti, ad esempio di portata nazionale, tra loro non comunicanti.

[16] Nella risoluzione del Consiglio economico e sociale delle Nazioni Unite (ECOSOC) del 28 luglio 2006, n. 2006/46, *Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development*, disponibile sul sito www.un.org., si legge: "*ensure the meaningful and effective*

no la necessità di una gestione condivisa di Internet da parte degli Stati, conducono a qualificarla quale bene pubblico globale e patrimonio comune dell'umanità. I due concetti, spesso utilizzati in modo intercambiabile per il fatto di fare riferimento a risorse o beni che, trascendono i confini nazionali, sono considerati essenziali per la sopravvivenza e il benessere dell'umanità nel suo complesso, si distinguono, sotto il profilo oggettivo, per il fatto che il primo si concentra più sulle risorse naturali e sulla loro gestione sostenibile, mentre il secondo enfatizza la protezione e la valorizzazione del patrimonio culturale e storico. Nel caso di Internet, in particolare, crediamo che la distinzione possa essere, per le sue caratteristiche, piuttosto sfumata.

Al patrimonio comune dell'umanità appartengono, come noto, beni di disparata natura, quali, ad esempio, i fondi marini e oceanici che si trovano oltre i limiti delle giurisdizioni nazionali[17], o il genoma umano, così come previsto dalla Dichiarazione UNESCO del 1997 sul genoma umano[18], tutti accomunati dalle predette caratteristiche, possedute, come abbiamo detto, anche da Internet, che, peraltro, è pure strumento attraverso il quale è possibile esercitare alcuni diritti fondamentali[19].

participation, including by providing assistance on a voluntary basis, of all stakeholders from developing countries, including nongovernmental organizations, small and medium-sized enterprises, industry associations and development actors".

[17] T. SCOVAZZI, *Fondi marini e patrimonio comune dell'umanità*, in *Rivista di diritto internazionale*, 1984, p. 249 ss.; A.G.O. ELFERINK, E. J. MOLENAAr (eds.), *The International Legal Regime of Areas Beyond National Jurisdiction*, Leiden, 2010.

[18] C. KUPPUSWAMY, *The International Legal Governance of the Human Genome*, London, 2012; S. MARCHISIO, *Patrimonio comune dell'umanità (dir. internaz.)*, in *Enciclopedia Il Sole 24 Ore*, Milano, 2007, p. 728 ss; ID., *L'ONU – Il diritto delle Nazioni Unite*, Bologna, 2012, p. 83 ss.; J.M. SPECTAR, *The fruit of the human genome tree: cautionary tales about technology, investment, and the heritage of humankind*, in *Loyola of Los Angeles*, 2001, p. 1 ss.

[19] Esiste un altro orientamento che concepisce Internet, invece, come bene globale "autonomo", l'accesso al quale rappresenterebbe un diritto fondamentale. Ci è impossibile, in questa sede, ricostruire la relativa prassi; per una visione d'insieme dei due approcci, rimandiamo a J.H. SY, *Global Communications for a More Equitable World*, in I. KAUL, I. GRUNDBERG, M.A. STERND (eds.), *Global Public Goods. International Cooperation in The 21st Century*, New York/Oxford, 1999, p. 326 ss. e D.L. SPAR, *The Public Face of Cyberspace*, *ivi*, p. 344 ss.

In conseguenza di questa qualificazione, quindi, è necessario applicare alla Rete il regime giuridico di diritto internazionale previsto per il patrimonio comune dell'umanità[20], che ne limita la libertà di sfruttamento da parte degli Stati, prevedendo: a) il divieto di esclusività della sovranità statale ai beni patrimonio comune e, in particolare, il divieto di appropriazione unilaterale; b) l'obbligo di assoggettamento dei beni in questione ad un regime internazionale di cooperazione in ordine alla loro gestione; c) il divieto di una loro utilizzazione, anche per interessi generali, tale da arrecare pregiudizio all'ambiente; d) l'obbligo di utilizzare tali beni esclusivamente per fini pacifici e, quindi, il divieto di porre in essere attività che siano irrispettose del diritto internazionale e, in particolare, dei principi di diritto internazionale generale e di quelli contenuti nella Carta delle Nazioni Unite relativi al mantenimento della pace e della sicurezza internazionale.

Interpretando tali obblighi e divieti alla luce dell'approccio che abbiamo descritto nel paragrafo precedente e adattandoli quindi alle caratteristiche dello specifico bene regolato, il principio di non appropriazione è qui da intendersi come il divieto, posto in capo a tutti gli Stati, di porre in essere unilateralmente comportamenti idonei a mettere in pericolo il funzionamento globale e condiviso di Internet (si pensi, ad es., a una manomissione del sistema dei nomi di dominio); l'obbligo di assoggettamento a un regime di cooperazione si traduce qui in un obbligo *di natura procedurale, de negotiando,* in merito alle misure di gestione dei meccanismi di base della Rete; il terzo e il quarto divieto, quelli di arrecare pregiudizio all'ambiente e di utilizzare il bene regolato per fini che non siano pacifici, comportano qui l'obbligo di non diffondere nell'ambiente virtuale strumenti che lo possano "inquinare" massivamente, come ad esempio *software* malevoli che ne

[20] Per una più esaustiva trattazione, si vedano A.C. KISS, *La notion de patrimoine commun de l'humanité,* in *Recueil des Cours de l'Académie de droit international de la Haye*, 1982, CLXXV, p. 99 ss., nonché K. BASLAR, *The Concept of the Common Heritage of Mankind in International Law*, Leiden, 1998; R. WOLFRUM, *The Principle of Common Heritage of Mankind*, in *Zeitschrift für ausländisches öffentlisches Recht und Völkerrecht*, 1983, p. 312 ss.; A. SEGURA SERRANO, *The Cyberspace and the Common Heritage of Mankind*, in M. IOVANE, F.M. PALOMBINO, D. AMOROSO, G. ZARRA (eds.) *The Protection of General Interests in Contemporary International Law: A Theoretical and Empirical Inquiry*, Oxford, 2021, p. 191 ss.

minino le strutture di base, o che costituiscano mezzi di violazione del divieto generalizzato di minaccia o uso della forza (*cyberwarfare* illegittima).

In particolar modo, per quanto concerne il terzo divieto, è utile ricordare che esistono analogie tra le norme che si impongono agli Stati in materia di inquinamento "reale" e l'inquinamento di Internet: se per inquinamento si intende, difatti, l'alterazione peggiorativa dell'ambiente per mezzo di fattori patogeni di origine umana, allora il divieto "tradizionale" di inquinamento transfrontaliero, e il connesso obbligo di adottare misure preventive e repressive dell'inquinamento ambientale, si traduce nell'obbligo di non inquinare l'ambiente virtuale, che deve essere preservato non solo attraverso misure volte ad evitare la diffusione *diretta* da parte degli Stati di *software* malevoli in grado di porre in pericolo il funzionamento della Rete, ma anche attraverso l'adozione di misure preventive e repressive che impediscano ai privati di diffondere *malware* massivi.

Quanto poi ad Internet come bene globale "strumentale", attraverso il quale, cioè, si esercitano anche diritti fondamentali, ricordiamo che il diritto internazionale prevede che questi ultimi debbano essere garantiti non solo nello spazio reale ma anche in quello virtuale, dal momento che "*the same rights people have offline must be protected online*"[21].

A tal proposito l'Assemblea generale delle Nazioni Unite ha affermato l'importanza di tutelare online i diritti fondamentali e ha chiesto agli Stati di rivedere le proprie norme interne alla luce del principio di *neutralità tecnologica*, su cui torneremo nel prossimo paragrafo[22].

[21] Human Rights Council*, 20th regular session*, Risoluzione del 5 luglio 2012, A/HRC/20/L.13, reperibile all'indirizzo www.ohchr.org. Nel medesimo senso l'Assemblea generale nella risoluzione sull'Intelligenza Artificiale dell'11 marzo 2024, A/78/L.49: "*The same rights that people have offline must also be protected online, including throughout the life cycle of artificial intelligence systems*"; in letteratura, da ultimo, v. A. STIANO, *Alcune considerazioni in tema di regolamentazione dell'intelligenza artificiale alla luce della recente prassi*, in *DPCE online*, 2025, reperibile online.

[22] Assemblea generale delle Nazioni Unite, Risoluzione 69/166, *The right to privacy in digital age*, *on the report of the Third Committee (A/69/488/Add.2 and Corr.1)*, A/RES/69/166 del 18 dicembre 2014; Assemblea generale delle Nazioni Unite, Risol-

Ancor più di recente, poi, l'Assemblea generale ha adottato una risoluzione in cui riconosce l'importanza della lotta a tutte le forme di violenza nel contesto delle tecnologie digitali, ivi compresi, con particolare riguardo al tema affrontato in questo Volume, lo sfruttamento e gli abusi sessuali, le molestie, lo *stalking*, il bullismo, la condivisione non consensuale di contenuti personali sessualmente espliciti, le minacce e gli atti di violenza sessuale e di genere, le minacce di morte, la sorveglianza e il tracciamento arbitrari o illegali, la tratta di persone, l'estorsione, la censura, l'accesso illegale a conti digitali, telefoni cellulari e altri dispositivi elettronici [23].

3. *Neutralità tecnologica ed equivalenza normativa come strumenti ermeneutici*

Evidentemente, quindi, le norme di tutela dei diritti umani incontrano la necessità di essere correttamente applicate nel contesto digitale[24].

Una parte della dottrina, muovendo dalla considerazione che alla diffusione di Internet su larga scala conseguano implicazioni giuridiche di varia natura, ritiene necessario trattare i diritti umani digitali quali diritti di nuova generazione, in particolare per il fatto che le caratteristiche intrinseche dell'ecosistema digitale non permetterebbero l'individuazione di soggetti pubblici in grado di garantirne efficacemente l'esercizio e il rispetto[25]. Questa dottrina, partendo dal presup-

uzione 71/199, *The right to privacy in the ditigal age*, *on the report of the Third Committee (A/71/484/Add.2)*, A/RES/71/199 del 19 dicembre 2016. Cfr. D. DROR-SHPOLIANSKY, Y. SHANY, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology*, in *European Journal of International Law*, 2021, p. 125 ss.

[23] Assemblea generale delle Nazioni Unite, Risoluzione 78/213, *Promotion and protection of human rights in the context of digital technologies*, *on the report of the Third Committee (A/78/481/Add.2, para. 139)*, A/RES/78/213 del 19 dicembre 2023.

[24] Per un approfondimento sul tema, si veda: L. PANELLA, *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, Napoli, 2018.

[25] A. ZIMMERMANN, *International Law and "Cyber Space"*, disponibile su www.esil-sedi.eu; K. MAČÁK, *From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers*, in *Leiden Journal of International Law*, 2017, p. 877 ss; M.N. SCHMITT, *Grey Zones in the International Law of Cyberspace*, in *Yale Journal of International*

posto che il cyberspazio è dominato da attori privati, i quali svolgono le loro attività anche al di fuori dell'ordinamento nazionale di origine e contribuiscono così alla "transnazionalizzazione" di Internet, e sottolineando come gli Stati ricoprano un ruolo piuttosto marginale nella regolamentazione di Internet, evidenzia le difficoltà di assicurare una tutela dei diritti fondamentali attraverso le norme, anche internazionali, preesistenti e, quindi, la necessità di aggiornarle o prevederne di specifiche.

In realtà, sebbene sia incontestabile che la natura *multistakeholder* di Internet renda più arduo il compito degli Stati di garantire i diritti fondamentali online, a noi pare che quest'ultimi, come abbiamo visto, possono essere ricondotti ai diritti umani già esistenti offline.

Per fare ciò è, essenzialmente, necessario interpretare le norme preesistenti alla luce del contesto tecnologico in cui devono essere applicate.

In questo senso un ruolo centrale è svolto dai *principi di neutralità tecnologica* e *di equivalenza normativa*: il primo, essenzialmente, si riferisce all'idea che le norme giuridiche dovrebbero applicarsi in modo uniforme a tutte le tecnologie, senza favorirne o discriminarne una rispetto a un'altra, e ciò anche al fine di evitare la loro obsolescenza a causa dell'evoluzione tecnologica; il secondo mira a che le normative garantiscano risultati equivalenti, indipendentemente dalla tecnologia utilizzata, nel senso che se due tecnologie diverse possono raggiungere il medesimo obiettivo, entrambe dovrebbero essere considerate "valide" e trattate in modo equivalente. Una loro combinazione si converte nell'obbligo per gli Stati di non differenziare la disciplina giuridica di una fattispecie sulla scorta del mezzo utilizzato per la sua realizzazione[26].

Ora, ricordando che la Convenzione di Vienna del 1969 sul diritto dei trattati non chiarisce se questi vadano interpretati tenendo conto

Law Online, 2017, p. 1; U. KOHL, *Jurisdiction in Cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, 2015, p. 30; W. HEINTSCHEL VON HEINEGG, *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013, p. 17.

[26] G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, p. 66 ss. Sul principio di neutralità tecnologica si v. anche V. SHADIKHODJAEV, *Technological Neutrality and Regulation of Digital Trade: How Far Can We Go?*, in *European Journal of International Law*, 2021, n. 4, p. 1221 ss.

del significato che le espressioni utilizzate avevano al momento della loro conclusione o al momento della loro applicazione, tutto quanto appena detto potrebbe contribuire al consolidamento del metodo evolutivo di interpretazione[27], nel senso di consentire e, anzi, imporre che il contenuto di una previsione normativa vada adattato ad una situazione o circostanza tecnicamente evolutasi *a posteriori* rispetto al momento conclusivo del trattato[28].

Un'operazione interpretativa siffatta dovrà, per un verso, evitare di spingersi fino all'imposizione agli Stati di obblighi del tutto nuovi rispetto a quelli originariamente concordati e, per altro, tenere comunque conto di altri interessi, eventualmente contrapposti.

A tal proposito, giova ricordare che la Corte internazionale di giustizia, in merito all'interpretazione dei trattati, ha chiarito che laddove le parti abbiano utilizzato, nel testo concordato, termini generici, si può presumere che le stesse fossero consapevoli che il significato dei medesimi era suscettibile di evolversi nel tempo e quindi, qualora il trattato sia stato stipulato per un periodo molto lungo o sia di "*continuing duration*", che le stesse abbiano inteso che "*those terms to have an evolving meaning*"[29].

Anche l'Organo d'appello dell'Organizzazione mondiale del commercio, con riguardo all'interpretazione delle liste di impegni specifici in materia di scambi di servizi, ha specificato come essa debba avvenire in considerazione del fatto che ritenere automaticamente che il significato ordinario da attribuire a tali termini debba necessariamente essere quello che avevano al momento della conclusione dell'allegato, significherebbe che ad impegni molto simili o formulati in modo identico potrebbero essere attribuiti significati, contenuti e portata, diversi a seconda della data della loro adozione, ciò minereb-

[27] Si v. M. ANDENAS, E. BJORGE (eds), *The Evolutionary Interpretation of Treaties*, Cambridge, 2014.

[28] G.M. RUOTOLO, *Non-fungible tokens e diritto internazionale*, in *Rivista di diritto internazionale*, 2024, n. 2, p. 393 ss.

[29] Corte internazionale di giustizia, *Costa Rica c. Nicaragua*, sentenza del 13 luglio 2009, nell'affare concernente la controversia relativa a diritti di navigazione e a diritti connessi, cfr. *I.C.J. Reports*, 2009, p. 13.

be prevedibilità, sicurezza e chiarezza degli impegni specifici del GATS[30].

Quanto poi ai termini tecnici *specifici* utilizzati all'interno di un trattato, l'approccio interpretativo che suggeriamo ci pare consenta di individuarne in maniera più chiara il significato, in questo caso in quanto fattore di interpretazione teleologica[31].

Dunque, è (anche) grazie a tale approccio che l'ordinamento internazionale riesce ad adattare le sue norme alle esigenze dettate dall'insorgenza delle nuove tecnologie dell'informazione, così da disciplinare il contesto digitale nel quale si vanno affermando.

4. *Alcuni caratteri generali della disciplina UE del contesto digitale*

Alla luce del quadro appena tracciato in materia digitale analizzeremo ora, seppur brevemente, la corrispondente normativa adottata dall'Unione europea, al fine di tracciare il contesto giuridico *complessivo* in cui la direttiva 1385/2024 si inserisce.

Ricordiamo che, come del tutto noto, l'Unione europea ha tra i suoi obiettivi quello di creare un mercato interno: ai sensi dell'art. 3 TUE essa "si adopera per lo sviluppo sostenibile dell'Europa, basato

[30] Organo di appello dell'Organizzazione mondiale del commercio, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, del 19 gennaio 2010, WT/DS363/AB/R, par. 397. Va detto che già venticinque anni or sono il Consiglio per gli scambi di servizi affermava che i Membri erano d'accordo sul fatto che il GATS si applica a tutti i servizi indipendentemente dal mezzo tecnologico con cui vengono forniti e osservava che il principio della neutralità tecnologica si applica agli impegni concordati, salvo diversa indicazione; cfr. Organizzazione mondiale del commercio, WTO S/C/M32 del 14 gennaio 1999.

[31] "*Purposive interpretation is also prominent in international law. It is the third method of treaty interpretation mentioned by art. 31(1) VLCT. While some authors argue that the 'object and purpose' of a treaty refer to two conceptually distinct features of the treaty, namely to its content and to the goal the parties wanted to achieve through it, this distinction has not gained any clout in international legal practice. Another provision linked to teleology is art. 31(3)(b) VLCT, which allows resorting to subsequent treaty practice (and hence to changing circumstances)*", così O. AMMANN, *Domestic Courts and the Interpretation of International Law*, Leiden/Boston, 2020, p. 209 ss.

su una crescita economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente. Essa promuove il progresso scientifico e tecnologico"; il mercato interno è definito dall'art. 26, par. 2 TFUE come "uno spazio senza frontiere interne in cui è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali".

Dunque, in continuità con il disegno europeo originario, l'Unione mantiene, attraverso queste norme, il "nucleo duro" del mercato comune[32].

È in questo contesto, a seguito della rilevanza e delle dimensioni che il progresso tecnologico ha assunto, che l'Unione ha deciso di ricomprendere nel progetto di un mercato unico europeo quello "digitale", inteso come quella parte di mercato interno in cui si verifica lo scambio di beni e servizi online per mezzo delle tecnologie informatiche, appunto, esso si propone di dar vita ad una società digitale europea unita e sostenibile, anche in ragione del progresso scientifico e tecnologico di cui l'UE si fa promotrice[33].

Peraltro, nel 2015, la Commissione europea ha adottato la sua *Strategia per il mercato unico digitale in Europa* con l'obiettivo di a) migliorare l'accesso online ai beni e servizi in tutta Europa per i consumatori e le imprese; b) creare un contesto favorevole affinché le reti e i servizi digitali potessero svilupparsi e c) massimizzare il potenziale di crescita dell'economia digitale europea[34].

[32] Così U. VILLANI, *Istituzioni di Diritto dell'Unione Europea*, Bari, 2024, p. 30. Sul mercato unico si vedano R. SANTANIELLO, *Il mercato unico europeo*, Bologna, 2007; L. DANIELE, *Diritto del mercato unico europeo e dello spazio di libertà, sicurezza e giustizia*, Milano, 2023. Più specificamente, sul mercato unico digitale, C. SCHMIDT, R. KRIMMERA, *How to implement the European digital single market: identifying the catalyst for digital transformation*, in *Journal of European Integration*, 2022, n. 1, p. 59 ss.

[33] G. M RUOTOLO, A Season in the Abyss. *Il nuovo copyright UE tra libertà di informazione, diritti fondamentali e mercato unico digitale*, in *Il diritto dell'Unione Europea*, 2019, n. 2, p. 369.

[34] Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia per il mercato unico digitale in Europa*, del 6 maggio 2015, COM (2015) 192 def.

Al contempo, l'Unione ha assunto come priorità anche la c.d. sovranità digitale europea[35], intesa come la capacità dell'UE stessa di agire in modo indipendente nel mondo digitale, sia in termini di meccanismi di protezione sia di strumenti offensivi per promuovere l'innovazione digitale[36].

È in questo contesto, ad esempio, che sono stati perseguiti significativi risultati in termini di liberalizzazione degli scambi e tutela dei diritti, specie dei consumatori, e della sicurezza informatica dell'Unione europea: si pensi, a mero titolo di esempio, all'abolizione delle tariffe di *roaming*[37], alla adozione di un regime di protezione dei dati[38], alla portabilità transfrontaliera dei contenuti online e alla fine dei c.d. blocchi geografici[39], al regime relati-

[35] Cfr. Consiglio dell'Unione europea, *Dichiarazione di Berlino sulla società digitale e su un governo digitale fondato sui valori*, dell'8 dicembre 2020. In dottrina, tra gli altri, F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *Il diritto dell'Unione Europea*, 2022, n. 2, p. 280.

[36] Si veda, al riguardo il *brief* predisposto da T. MADIEGA, *Digital sovereignty for Europe*, luglio 2020 per il Parlamento europeo, doc PE 651.992, disponibile su www.europarl.europa.eu.

[37] Regolamento (UE) 2022/612 del Parlamento europeo e del Consiglio, *relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione*, del 6 aprile 2022, in GUUE L 115 del 13 aprile 2022, p.1-37.

[38] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*, del 27 aprile 2016, in GUUE L 119 del 4 maggio 2016, pp. 1–88; Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, *riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati)*, del 13 dicembre 2023, in GUUE L del 22 dicembre 2023, p.1-71.

[39] Regolamento (UE) 2017/1128 del Parlamento europeo e del Consiglio, *relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno*, del 14 giugno 2017, in GUUE L 168/1 del 30 giugno 2017. Sul regolamento si v. C. PESCE, *Blocchi geografici ingiustificati,* in *I Post di AISDUE*, 5 aprile 2019, reperibile online; G.M. RUOTOLO, *La lotta alla frammentazione geografica del mercato unico digitale: tutela della concorrenza, uniformità, diritto internazionale privato*, in *Diritto del commercio internazionale*, 2018, n.2, p. 501 ss; D. VAIRA, G.M. RUOTOLO, *Responsabilità dei social network per user generated content e applicazione extraterritoriale delle misure inibitorie di lesioni dei diritti della personalità alla luce della recente giurisprudenza UE*, in *Ordine internazionale*

vo ai semiconduttori[40], alla regolamentazione dei servizi digitali[41] e dell'Intelligenza Artificiale[42].

Si è così costruito un sistema normativo molto stratificato e per nulla di facile lettura – e questo anche dal momento che, come è stato giustamente detto, le fattispecie digitali "*move too quickly for regulatory comfort*"[43] – il quale impone un'analisi costante sia delle norme che disciplinano, per così dire, direttamente il mercato, sia dell'impatto che esse hanno, indirettamente, su altri "regimi" (usiamo qui l'espressione in senso descrittivo e "materiale": ad esempio la concorrenza, la tutela dei consumatori, la proprietà intellettuale) e di comprendere a fondo rapporti e meccanismi di mutua influenza.

Tutti questi aspetti, peraltro, vanno necessariamente letti alla luce di quei principi e valori di rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, che l'art. 2 TUE non solo pone alla base del diritto dell'Unione europea, ma dichiara anche esser comuni ai paesi membri,

e diritti umani, 2020, n. 1, pp. 187-192; D. VAIRA, *Online Individual sharing as an expression of a common cultural mode: The case of Migrants and Geoblocks*, in G.C. BRUNO, F.M. PALOMBINO, A. DI STEFANO, G.M. RUOTOLO (eds.), *Migration and Culture: Implementation of Cultural Rights of Migrants*, Napoli, 2022, p. 91 ss.

[40] Regolamento (UE) 2023/1781 del Parlamento europeo e del Consiglio, *che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il regolamento (UE) 2021/694 (regolamento sui chip)*, del 13 settembre 2023, in GUUE L 229 del 19 settembre 2024, pp. 1-53.

[41] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, *relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Digital Services Act, DSA)*, del 19 ottobre 2022, in GUUE L 277 del 27 ottobre 2022, p. 1-102. Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, *relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (Digital Markets Act, DMA)*, del 14 settembre 2022, in GUUE L 265 del 12 ottobre 2022, pp. 1-66.

[42] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, *che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828*, del 13 giugno 2024, in GUUE L del 12 luglio 2024, pp. 1-144.

[43] R. BROWNSWORD, K. YEUNG, *Regulating Technologies: Tools, Targets and Thematics*, in R. BROWNSWORD, K. YEUNG (eds.), *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*, Oxford/Portland, 2008, p. 5.

nonché con la tutela dei diritti fondamentali, imposta tanto dall'ordinamento UE quanto dal diritto internazionale.

E questo anche in considerazione del fatto che, non di rado, l'UE, con una logica che altrove abbiano definito "frattalica"[44], tende a replicare nei suoi accordi internazionali, specie di contenuto commerciale, modelli normativi già testati *in foro interno*, anche al fine di esportarli: non a caso l'azione esterna dell'Unione[45] si fonda sui medesimi valori, ai sensi dell'art. 3, par. 5, e dell'art. 21, par. 1 TUE (dove sono denominati "principi").

Quindi, se da una parte l'approccio *market oriented* ha fatto dell'Unione una potenza competitiva sul mercato digitale globale, dall'altro ha contribuito ad evidenziare alcune difficoltà di regolamentazione delle nuove tecnologie dell'informazione: è emerso, ad esempio, chiaramente il potere esercitato dalle piattaforme online, specie quelle di grandi dimensioni (le c.d. *Very Large Online Platforms*, VLOPs, e i c.d. *Very Large Search Engines*, VLOSEs, del Digital Services Act) sul godimento delle libertà e dei diritti tutelati dall'ordinamento UE nell'ambiente digitale.

È in considerazione di questa consapevolezza, quindi, che gli strumenti di diritto UE delle tecnologie dell'informazione, seppur adottati nel contesto del mercato digitale e al fine di completarlo, contemplano disposizioni in materia di tutela dei diritti fondamentali, volte ad impedire la violazione degli stessi, posta in essere attraverso pratiche manipolative o un uso improprio delle tecnologie digitali.

5. *La direttiva 2024/1385 e gli obblighi di penalizzazione: la necessità di esplicita previsione della "equivalenza normativa" in materia penale e un caso di sua violazione*

Sulla scorta delle premesse sin qui sviluppate, passiamo ora brevemente all'analisi di alcuni aspetti della direttiva (UE) 2024/1385 del

[44] G.M. RUOTOLO, *Trattamenti e accordi preferenziali dell'Unione europea e degli Stati Uniti tra frattali, TAPED e transplants*, in G. ADINOLFI (a cura di), *Gli accordi preferenziali di nuova generazione dell'Unione europea*, Torino, 2021, p. 107 ss.

[45] Per un approfondimento sulle competenze dell'Unione europea, si v. C. NOVI, *Corte di giustizia e competenze esterne dell'Unione Europea*, Bari, 2023, p. 17 ss.

Parlamento e del Consiglio sulla lotta alla violenza contro le donne e alla violenza domestica, con particolare attenzione alle loro manifestazioni online.

Essa, come noto, è stata emanata al fine di prevenire e proteggere le donne dalla violenza di genere, aggravata dalle tecnologie dell'informazione, le quali favoriscono la creazione di un contesto in cui i responsabili potrebbero perpetrarla, con minori rischi di subirne le conseguenze[46].

Ora, va detto che, sebbene la denominazione dello strumento suggerisca che essa sia stata emanata al fine di tutelare *esclusivamente* le donne, al considerando 12 è precisato che anche altre persone sono oggetto di queste forme di violenza e dovrebbero quindi beneficiare delle stesse misure che la direttiva prevede per le "vittime"; il termine "vittima", pertanto, dovrebbe riferirsi a chiunque, indipendentemente dal genere.

Dunque, l'Unione europea, conscia dell'insufficiente protezione che i suoi precedenti strumenti, come le direttive 2011/36/UE[47] e 2011/93/UE[48], garantivano alle donne vittime di violenza[49], ha deciso di rafforzarne la tutela attraverso la previsione di norme più stringenti, mediante le quali imporre agli Stati membri l'armonizzazione delle regolamentazioni interne pertinenti.

[46] In generale, su questo aspetto, cfr. S. VANTIN, *La lama della rete. Forme della violenza contro le donne sul web*, in *Rivista italiana di informatica e diritto*, 2020, n. 2, p. 27 ss.; F. PAGNOTTA, *La violenza di genere nell'ambiente digitale. Aspetti e conseguenze di un'emergenza sociale ed educativa*, in *Q-Times Webmagazine*, 2019, n. 3, pp. 30-43; E. BOSCHETTO, A. CANDIELLO, A. CORTESI, F. FIGNANI, *Donne e Tecnologie Informatiche*, Venezia, 2011, p. 11 ss.; M. FERRARI, *Violenza contro le donne: l'Unione europea adotta finalmente la direttiva (UE) 2024/1385*, in *Eurojus*, 2024, p. 1 ss.

[47] Direttiva 2011/36/UE del Parlamento europeo e del Consiglio, *concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime*, del 5 aprile 2011, in GUUE L 101/1 del 15 aprile 2011, pp. 1-11.

[48] Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, *relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile*, del 13 dicembre 2011, in GUUE L 335 del 17 dicembre 2011, pp. 1-14.

[49] Direttiva 2012/29/UE del Parlamento europeo e del Consiglio, *che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI*, del 25 ottobre 2012, in GUUE L 315 del 14 novembre 2012, pp. 57-73.

In questo senso gli obblighi (di risultato) che la direttiva impone agli Stati membri sono molteplici e attengono anzitutto, sotto il profilo "sostanziale", alla penalizzazione di condotte quali a) le mutilazioni genitali femminili; b) il matrimonio forzato; c) la condivisione di materiale intimo o manipolato; d) lo *stalking* online; e) le molestie online; f) l'istigazione alla violenza e all'odio online, nonché g) l'istigazione, il favoreggiamento, il concorso o il tentativo di commissione delle condotte di cui sopra.

Al fine di punire questi comportamenti, sotto il profilo "procedurale", essa impone agli Stati membri ulteriori obblighi, che attengono a) alla previsione di mezzi di protezione delle vittime e di accesso alla giustizia; b) alla creazione di enti preposti all'assistenza alle vittime; c) alla previsione di misure preventive e d'intervento precoce; infine, d) alla cooperazione tra Stati per una normativa armonizzata in materia.

Ora, come evidente, alcune delle condotte che l'UE chiede agli Stati di penalizzare hanno "natura" informatica, nel senso che avvengono in un contesto digitale o per mezzo di nuove tecnologie: non a caso numerosi sono i richiami che la direttiva fa agli strumenti UE di disciplina delle fattispecie digitali di cui abbiamo detto nei paragrafi precedenti[50], come il GDPR, il DSA e l'AIA, dal momento che la condivisione online di materiale illegale ai sensi della direttiva, implica una serie di conseguenze giuridiche anche in materia di privacy e servizi digitali.

Per quanto concerne, in particolare, i servizi digitali e i loro fornitori, ad esempio, accertata la diffusione di materiale intimo o manipolato, o che istighi alla violenza o all'odio, di cui agli artt. 5 e 8 della direttiva, la stessa richiede la collaborazione tra Stati, prestatori di servizi

[50] La direttiva, ad esempio, contempera le esigenze di tutela con quelle di privacy delle vittime di violenza, specificando che il trattamento dei dati personali deve avvenire in ossequio alle disposizioni del Regolamento (UE) 2016/679, cit., oltre a quelle del Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*, del 27 aprile 2016, in GUUE L 119 del 4 maggio 2016, pp. 89-131.

di *hosting* e prestatori di servizi intermediari per la rimozione del materiale illegale o la disabilitazione dell'accesso allo stesso[51].

Anche questo strumento, peraltro, come tutti gli altri relativi alla disciplina di condotte online, adotta un approccio alla gestione del rischio, basato sull'individuazione tempestiva del materiale illegale, anche attraverso l'imposizione ai fornitori di strumenti di autoregolamentazione in grado di favorire la prevenzione dei comportamenti sanzionati[52].

Anche in questo caso, quindi, l'UE conferma un approccio consapevole all'incidenza delle nuove tecnologie sul godimento di diritti individuali, qui con un particolare accento su quello all'oblio[53].

Ancora, a noi pare che gli artt. 5-8 della direttiva – i quali descrivono le fattispecie in cui le tecnologie dell'informazione vengono utilizzate come strumenti di condivisione non consensuale di materiale intimo o manipolato, o di materiale che istighi alla violenza o all'odio, o come mezzi attraverso i quali porre in essere molestie e *stalking* – rappresentino forme di applicazione dei principi di neutralità tecnolo-

[51] Per approfondimenti sulla responsabilità di prestatori di servizi di *hosting* e intermediari cfr. G.M. RUOTOLO, *Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di* bis in idem, in *Quaderni di SidiBlog*, Napoli, 2021, p. 222 ss.

[52] A. PURPURA, *Osservazioni sul Digital Services Act: responsabilità e gestione del rischio nella prestazione di servizi intermediari*, in *Comparazione e diritto civile*, 2022, n. 3, pp. 1035-1065; L. D'AGOSTINO, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo Digital Services Act*, in *Medialaws*, 2023, n. 2, p. 16 ss.; G.M. RUOTOLO, *Spirits in the material world: artificial intelligence act e responsabilità per la diffusione online di informazioni*, cit., p. 409 ss.

[53] Per un approfondimento sul tema, si veda, M. RAMÓN, O. LINARES, *Il diritto all'oblio. Un'analisi della sua evoluzione dall'adozione del GDPR*, in *La cittadinanza europea online*, n. 2, 2023, pp. 233-251; F ZORZI GIUSTINIANI, *Cronaca dal cyberspazio: due sentenze sul diritto all'oblio*, in *Nomos*, 2019, n. 3, 1 ss; A. BUND, *The Curious Caseof the Right to Be Forgotten*, in *"Computer Law & SecurityReview"*, 2015, n. 31, pp. 336-350; D. LINDSAY, *The 'Right to be Forgotten' by Search Engines under Data Privacy Law*: *A Legal Analysis of the Costeja Ruling*, in *Journal of MediaLaw*, 2014, n. 6, pp. 159-179; L. SIRY, *Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten*, in *Kentucky Law Journal*, 2014, n. 3, pp. 311-344.

Per una ricostruzione filosofica del problema, si veda, J. CIANI SCIOLLA, *Diritto all'oblio e cooperazione internazionale: problemi e prospettive*, in *Rivista italiana di informatica e diritto*, 2022, n. 4, 157 ss.

gica ed equivalenza normativa: queste condotte, difatti, sono già punite quando commesse nel mondo "reale" e l'intervento normativo realizzato è volto ad estendere la punibilità ai comportamenti online.

In questo caso, però, in considerazione della natura penale delle misure adottate e del connesso divieto di analogia, è stato necessario procedere ad una esplicita previsione della "equivalenza".

Tuttavia, va detto, permangono alcune disparità di tutela tra le vittime di istigazione all'odio online e quelle offline, le quali si sostanziano, al contempo, a nostro parere, in una violazione del principio di neutralità tecnologica ed equivalenza normativa.

Si pensi, ad esempio, al fatto che la Decisione quadro del Consiglio sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale[54], prevede che gli Stati membri adottano le misure necessarie affinché i seguenti comportamenti intenzionali siano resi punibili: "a) l'istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica; b) la perpetrazione di uno degli atti di cui alla lettera a) mediante la diffusione e la distribuzione pubblica di scritti, immagini o altro materiale".

La pubblicità della condotta, dunque, appare elemento caratterizzante il comportamento da punire, senza il quale lo stesso non può essere, appunto, sanzionato. Ora, procedendo ad un'interpretazione teleologica della espressione "istigazione pubblica", e tenuto conto della specificazione di cui alla lettera b), che prevede la punizione di quelle condotte che sono poste in essere attraverso la "distribuzione pubblica" di materiale inneggiante all'odio, essa può esser concepita come relativa a una condotta posta in essere dinanzi ad un numero indefinito di persone.

Ebbene, l'art. 8 della direttiva 2024/1385 richiede che il materiale di istigazione all'odio sia diffuso a mezzo di strumenti informatici in

[54] Decisione quadro 2008/913/GAI del Consiglio, *sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale*, del 28 novembre 2008, in GUUE L 329 del 6 dicembre 2008, pp.55-58. Si veda anche la Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Un'Europa più inclusiva e protettiva: estendere l'elenco dei reati riconosciuti dall'UE all'incitamento all'odio e ai reati generati dall'odio*, del 9 dicembre 2021, COM (2021) 777 def.

modo da renderlo accessibile a un numero potenzialmente illimitato di persone. Tuttavia, il considerando 26 della stessa specifica che "se per accedere al materiale è necessario registrarsi o essere ammessi a un gruppo di utenti, le informazioni dovrebbero considerarsi divulgate al pubblico solo se gli utenti che chiedono l'accesso sono automaticamente registrati o ammessi *senza che qualcuno lo decida o scelga a chi dare l'accesso*" (enfasi aggiunta).

Ebbene, a noi pare che quest'ultima specificazione non tenga in alcun conto il fatto che alcune applicazioni di messaggistica (si pensi, ad esempio, a Telegram) prevedono la possibilità di creare gruppi sì privati, ma frequentati da svariate migliaia di persone, ai quali l'accesso è possibile solo previa accettazione da parte degli amministratori, e nei quali è certamente possibile far circolare contenuti che istigano all'odio e alla violenza contro le donne[55].

Una rigida applicazione delle norme che abbiamo descritto, quindi, potrebbe impedire l'integrazione del reato d'istigazione all'odio e alla violenza contro le donne quando il materiale illegale dovesse esser diffuso in gruppi privati in cui l'accesso non è automatico.

Ad ogni modo, proprio questa incongruenza ci pare confermare la centralità dei principi di neutralità tecnologica ed equivalenza normativa, di cui deve esser fatta consapevole applicazione anche con riguardo alla lotta all'uso delle tecnologie dell'informazione come strumenti di tutela delle vittime di violenza.

Abstract

Il Capitolo traccia alcune caratteristiche generali della regolamentazione di diritto internazionale e dell'Unione europea delle tecnologie dell'informazione a partire dal rapporto biunivoco che lega Internet e il diritto internazionale e ne inquadra alcuni elementi normativi peculiari, quali i principi di

[55] Con riguardo a discorsi d'odio e social media, G.M. RUOTOLO, *A Little Hate, Worldwide! Di libertà d'opinione e discorsi politici d'odio on-line nel diritto internazionale ed europeo*, in *Diritti umani e diritto internazionale*, 2020, n. 2, p. 549 ss.; D. VAIRA, We don't Need no Regulation. *La tutela dei diritti fondamentali tra diritto dell'Unione europea e autoregolamentazione. Alcune riflessioni alla luce della "giurisprudenza" dell'Oversight Board*, in *Quaderni AISDUE*, 2023, p. 701 ss.

neutralità tecnologica ed equivalenza normativa. Su queste basi, nel quadro normativo così delineato, gli Autori inquadrano la direttiva oggetto del volume.

KEYWORDS: diritto internazionale – equivalenza normativa – neutralità tecnologica – violenza – donne

NORMAS PARA COMBATIR LA VIOLENCIA DE GÉNERO ONLINE EN EL CONTEXTO DE LA REGULACIÓN INTERNACIONAL Y EUROPEA DE INTERNET: ALGUNAS CUESTIONES GENERALES Y METODOLÓGICAS

En el capítulo se describen algunas características generales de la regulación del derecho internacional y de la Unión Europea, en relación con las tecnologías de la información, partiendo del vínculo directo entre Internet y el derecho internacional. Asimismo, se enmarcan ciertos elementos regulatorios específicos, como los principios de neutralidad tecnológica y equivalencia regulatoria. Sobre estas bases, dentro del marco normativo así delineado, los autores formulan la directiva objeto del estudio.

PALABRAS CLAVE: derecho internacional – equivalencia regulatoria – neutralidad tecnológica – violencia – mujeres

LA CYBERVIOLENZA DI GENERE: ALCUNI SPUNTI DI RIFLESSIONE RELATIVI AL POSSIBILE CONTRIBUTO DEL DIRITTO INTERNAZIONALE PRIVATO AL CONTRASTO DELLA VIOLAZIONE DEI DIRITTI FONDAMENTALI DI GENERE

Sara Tonolo[*]

1. *Osservazioni introduttive*

La cyberviolenza è una violazione dei diritti fondamentali di natura generalmente transnazionale, vista la dimensione dello strumento utilizzato, che prevede l'impiego di tecnologia suscettibile di diffondere immagini e informazioni in paesi diversi, al fine di ledere la dignità personale a scopo ricattatorio o sanzionatorio. Molto frequentemente si tratta di una violenza rivolta contro le donne, come evidenziano studi recenti[1], che ricollegano a tale crimine ulteriori discriminazioni, come ad es. il ridotto numero di donne elette nelle istituzioni di governo dei vari paesi dell'Unione europea, a causa della violenza esercitata anche online nei confronti delle donne politicamente attive[2].

[*] Professoressa ordinaria di Diritto internazionale, Università di Padova. Email: sara.tonolo@unipd.it.

[1] European Parliament, *Cyberviolence against women: what it is and how to prevent it?*, 6 dicembre 2024, disponibile su https://www.europarl.europa.eu/topics/en/article/20241205STO25880/cyberviolence-against-women-what-is-it-and-how-to-prevent-it.

[2] European Union Agency for Fundamental Rights, *Violence against Women: an EU-Wide Survey,* 2014, disponibile su https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.

Il termine "cyberviolenza" indica l'uso di sistemi informatici per causare, facilitare o minacciare la violenza nei confronti di individui o gruppi, cagionando danni o sofferenze fisiche, sessuali, psicologiche o economiche, a ulteriore conferma di come le condotte di violenza online travalichino i confini della Rete e si ripercuotano sulla vita reale della vittima. Il cyberspazio si configura facilmente come mezzo agevolatore con riferimento alla commissione di atti illeciti, per la maggiore facilità con cui consente di raggiungere la vittima, che è un soggetto identificabile nella Rete, con ripercussioni potenzialmente destinate a prodursi in Stati diversi, ovvero tutti quelli raggiungibili dalla Rete. Più in generale, si tratta di utilizzo dei sistemi informatici che operano istantaneamente in tutti i paesi del mondo[3].

Nonostante l'ampia diffusione del fenomeno, che assume forme e contenuti sempre più gravi – talora penalmente rilevanti secondo quanto prevedono le norme dei singoli ordinamenti nazionali – dalla circolazione di video relativi alle violenze sessuali su WhatsApp[4], all'identificazione tramite tag di una ragazza vicino a un ragazzo in un post su Instagram al fine di supporre la possibilità di realizzare comportamenti illeciti su di lei, ma coerenti con una concezione patriarcale dei rapporti interpersonali[5], ai casi di *revenge porn*[6], alle violenze esercitate sugli avatar, tramite i quali le persone agiscono

[3] R.L. MC FARLAND, *Please do not publish this article in England: a Jurisdictional Response to Libel Tourism*, in *Mississipi Law Journal*, 2010, n. 19, disponibile su https://ssrn.com/abstract=1514988; W. L. PATRICK, *Sexual assault in the metaverse: Virtual reality, real trauma*, in *Psychology Today*, 2023 disponibile su https://www.psychologytoday.com/intl/blog/why-bad-looks-good/202301/sexual-assault-in-the-metaverse-virtual-reality-real-trauma.

[4] R. SRIVASTAVA, *From streets to smartphones: India grapples with online rape,* in *Reuters*, 2017, disponibile su https://www.reuters.com/article/world/from-streets-to-smartphones-india-grapples-with-online-rape-idUSKBN1DF0UM/.

[5] N. SUZOR, M. DRAGIEWICZ, B. HARRIS, R. GILLETT, J. BURGESS, T. VAN GEELEN, *Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online,* in *Policy & Internet*, 2019, n. 1, pp. 84 – 103.

[6] R. JEWKHES, E. DARTNALL, *More research is needed on digital technologies in violence against women*, in *The Lancet Public Health,* 2019, n. 6, pp. 270-271, disponibile su https://www.thelancet.com/journals/lanpub/article/PIIS2468-2667(19)30076-3/fulltext.

nel cyberspazio[7], manca, a livello internazionale, una disciplina sanzionatoria efficace.

Ciò, nonostante la cyberviolenza di genere venga indirettamente in rilievo ad es. nella Risoluzione n. 29/14 dell'Human Rights Council, secondo il quale la cyberviolenza o la violenza online rientrano nella fattispecie della violenza domestica[8], analogamente a quanto osservato entro il Report del 2018 dello *Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*[9], nonché nel documento del Gruppo di lavoro del Consiglio d'Europa relativo allo *stalking* sul web e alle altre forme di violenza in linea, realizzato nel 2018[10].

Particolarmente significativa risulta essere l'assenza di una disciplina specifica della cyberviolenza di genere entro la Convenzione di Budapest del 2001 sulla criminalità informatica[11]. La Convenzione di

[7] W. L. PATRICK, *op.cit.*; Y. HAGA, *Avatars, Personalities in the Metaverse: introductory Analysis on Conflict of Laws*, in *Rivista di diritto internazionale private e processuale*, 2023, n. 2, pp. 671-689.

[8]Human Rights Council, Resolution 29/14, *Accelerating efforts to eliminate all forms of violence against women: eliminating domestic violence*, del 2 luglio 2015, A/HRC/RES/29/14, disponibile su https://documents.un.org/doc/undoc/gen/g15/161/82/pdf/g1516182.pdf.

[9] Commission on Human Rights, Report of the Special Rapporteur on Violence against women, its causes and consequences, MS. DUBRAVKA ŠIMONOVIĆ, *On online violence against women and girls from a human rights perspective*, A/HRC/38/47, 18 June 2018, A/HRC/38/47, disponibile su https://digitallibrary.un.org/record/1641160.

[10] https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

[11] Convenzione sulla criminalità informatica di Budapest, adottata nell'ambito del Consiglio d'Europa, il 23 novembre 2001, Convention on Cybercrime (ETS No. 185), attualmente in vigore in Albania, Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Benin, Belgio, Bosnia Erzegovina, Brasile, Bulgaria, Capo Verde, Camerun, Canada, Cile, Colombia, Costa Rica, Costa d'Avorio, Croazia, Cipro, Repubblica Cèca, Danimarca, Repubblica Dominicana, Ecuador, Estonia, Fiji, Filippine, Finlandia, Francia, Ghana, Georgia, Germania, Grecia, Grenada, Israele, Islanda, Italia, Giappone, Kiribati, Liechtenstein, Lituania, Lussemburgo, Malta, Marocco, Mauritius, Monaco, Montenegro, Paesi Bassi, Macedonia del Nord, Nigeria, Norvegia, Panama, Paraguay, Perù, Polonia, Portogallo. Moldavia, Regno Unito, Romania, San Marino, Senegal, Serbia, Sierra Leone, Repubblica Slovacca, Slovenia, Spagna, Sri-Lanka, Svezia, Svizzera, Tonga, Tunisia, Turchia, Ucraina, Ungheria, USA.

Budapest definisce alcune condotte criminose rispetto alle quali gli Stati devono adottare misure sanzionatorie, ma si tratta di condotte che solo indirettamente rilevano nel quadro della violenza di genere. L'accesso illegale ad un sistema informatico è oggetto dell'art. 2 in quanto azione volta a ottenere informazioni all'interno di un computer con intento illegale, ma senza alcun riferimento specifico alla violenza di genere; analogamente, l'art. 4 sanziona l'attentato all'integrità dei dati; l'art. 5 l'attentato all'integrità di un sistema; l'art. 9 prevede una disposizione specifica in merito ai reati relativi alla pornografia infantile ma senza che vi sia una caratterizzazione specifica in termini di violenza di genere.

È auspicabile quindi che al Protocollo n. 1 sul razzismo[12] e al Protocollo n. 2 sulla *disclosure*[13] segua un Protocollo sulla cyberviolenza di genere, in considerazione delle gravi conseguenze che tali violazioni determinano in capo alle vittime di tali crimini[14].

La giurisprudenza della Corte europea dei diritti dell'uomo opera invece un chiaro inquadramento della cyberviolenza di genere[15], af-

[12] Protocollo di Strasburgo alla Convenzione di Budapest, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, del 28 gennaio 2003, (ETS No. 189), attualmente in vigore per Albania, Andorra, Armenia, Benin, Bosnia Erzegovina, Cipro, Croazia, Repubblica Cèca, Danimarca, Finlandia, Francia, Germania, Grecia, Islanda, Lettonia, Lituania, Lussemburgo, Macedonia del Nord, Marocco, Moldavia, Monaco, Montenegro, Paesi Bassi, Paraguay, Norvegia, Polonia, Portogallo, Romania, San Marino, Senegal, Serbia, Repubblica Slovacca, Slovenia, Spagna, Svezia, Ucraina. L'Italia ha sottoscritto il Protocollo n.1 nel 2011 ma non ha ancora provveduto alla ratifica dello stesso.

[13] Protocollo di Strasburgo alla Convenzione di Budapest, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, del 12 maggio 2022, (CETS No. 224), non ancora in vigore avendo ricevuto solo le ratifiche di Giappone e Serbia. L'Italia l'ha sottoscritto in data 12.5.2022.

[14] In Italia è tristemente noto il caso di Tiziana Cantone, che si è suicidata all'età di 31 anni in seguito alla circolazione online di immagini intime della stessa ad opera dell'ex compagno, caso in seguito al quale è stata adottata la Legge n. 69/2019, del 19 luglio 2019, in GU n. 173 del 25 luglio 2019, c.d. Codice Rosso, che ha introdotto il crimine di diffusione di materiali esplicitamente sessuali senza il consenso della persona interessata.

[15] Corte europea dei diritti dell'uomo, sentenza del 11 febbraio 2020, ricorso n.

fermando che le autorità nazionali non possono trattare episodi come l'utilizzo abusivo degli account di una donna da parte dell'ex marito o l'acquisizione di immagini e dati, come casi di violenza ordinaria, ma devono prevedere l'applicazione delle regole più stringenti fissate per i casi di violenza domestica, al fine di evitare la violazione dei diritti fondamentali garantiti dalla Convenzione europea dei diritti dell'uomo (di seguito CEDU)[16]. Dagli artt. 3 (divieto di trattamenti inumani e degradanti) e 8 (diritto al rispetto della vita privata, che include quello alla riservatezza della corrispondenza) CEDU deriva l'obbligo positivo di adottare misure preventive e sanzionatorie nei casi in cui una donna subisca intrusioni nel proprio computer, nei profili social, nonché furti di dati personali intimi e di immagini.

Particolarmente rilevante è la qualificazione della cyberviolenza nei confronti delle donne come violenza domestica ai sensi della Convenzione di Istanbul dell'11 maggio 2011 sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, internazionalmente in vigore dal 2014[17]. L'art. 3, lett. b) di questa Convenzione consente infatti di ricomprendere nella nozione di "violenza domestica" "tutti gli atti di violenza fisica, sessuale, psicologica o economica che si verificano all'interno della famiglia o del nucleo familiare o tra attuali o precedenti coniugi o partner, indipendentemente dal fatto che l'autore di tali atti condivida o abbia condiviso la stessa residenza con la vittima".

La fattispecie della cyberviolenza di genere viene ulteriormente dettagliata dalla Corte di Strasburgo nel caso *Volodina c. Russia*[18],

56867/15, *Buturugă c. Romania*. Il caso riguarda una cittadina rumena che aveva depositato una denuncia contro l'ex marito per i ripetuti episodi di violenza domestica e per l'utilizzo abusivo, da parte dello stesso, dei suoi account, inclusa la sua pagina Facebook, l'intromissione nel computer, lo *stalking* via web e l'acquisizione di dati e immagini. Il procuratore aveva archiviato queste denunce perché i comportamenti dell'uomo non erano stati considerati come "particolarmente gravi". La decisione era stata impugnata dalla donna e il tribunale di primo grado aveva disposto una misura di protezione applicabile per 6 mesi che, però, non era stata eseguita in modo effettivo.

[16] Convenzione sulla salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nell'ambito del Consiglio d'Europa, adottata il 4 novembre 1950 (ETS/5).

[17] Si v. sul punto M. DI STEFANO, *Violenza contro le donne e violenza domestica nella nuova Convenzione del Consiglio d'Europa*, in *DUDI*, 2012, n. 1, p. 169 e ss.

[18] Corte europea dei diritti dell'uomo, sentenza del 14 settembre 2021, ricorso n.

nell'ambito del quale viene sanzionata l'inerzia delle autorità statali rispetto a pubblicazioni di fotografie online senza consenso, creazione di un profilo falso, *revenge porn*, minacce via social e tracciamento dei movimenti, in evidente violazione del diritto al rispetto della vita privata della vittima di tali violenze. La Corte europea riconosce che in Russia sono state adottate leggi con meccanismi penali e civili per garantire la tutela della vita privata, ma nel concreto le autorità non hanno fornito alcuna protezione alla donna, se non dopo molto tempo. Eppure – osserva la Corte – la violenza online è direttamente collegata a quella offline e si tratta di un altro aspetto della violenza domestica da trattare con grande attenzione. Gli Stati, inoltre, anche in questo contesto, hanno obblighi positivi e devono intervenire per proteggere le vittime, conducendo indagini effettive. Invece, in questo caso di fronte alla gravità degli atti di cyberviolenza la risposta è stata decisamente inadeguata e ha dato il senso di impunità all'autore degli atti di cyberviolenza, con ciò vanificando l'effetto deterrente rispetto ad altri episodi.

Seguendo la tipizzazione giurisprudenziale operata dalla Corte di Strasburgo, l'Unione europea ha adottato la direttiva (UE) 2024/1385 sulla lotta contro la violenza alle donne e alla violenza domestica[19], che include la criminalità informatica nei reati previsti dal capo II della stessa, con specifico riguardo allo *stalking* e alle molestie online, alla condivisione di materiale privato online, all'istigazione alla violenza e all'odio online.

2. *Diritto internazionale privato e diritti umani a confronto negli spazi digitali*

L'uso delle nuove tecnologie incide inevitabilmente sui diritti fondamentali degli individui, che svolgono interazioni sociali tramite le piattaforme digitali, che consentono a chiunque di accedervi, creando

40419/19, *Volodina c. Russia.*

[19] Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio, *sulla lotta alla violenza contro le donne e alla violenza domestica*, del 14 maggio 2024, in GUUE L del 24 maggio 2024, pp. 1-36.

un proprio profilo per acquistare beni, biglietti aerei, ferroviari, ascoltare musica, vedere film, spettacoli teatrali, interagire con altre persone, ecc.[20] Si tratta di interazioni che hanno per natura una dimensione internazionale, come evidenziato ad es. dal fatto che i post e le immagini inseriti in una piattaforma social sono accessibili a miliardi di utenti della c.d. comunità digitale[21].

È in tale contesto che si può indagare il ruolo del diritto internazionale privato come strumento volto a rendere efficace ed effettiva la tutela dei diritti fondamentali, quale premessa concettuale per analizzare possibili spunti di contrasto alla cyberviolenza di genere entro la disciplina ora considerata. Tale ruolo si apprezza nel momento in cui il diritto internazionale privato mira a risolvere i problemi di coordinamento tra sistemi giuridici, tradizionali per la disciplina, ovvero l'individuazione del giudice competente ad esaminare una controversia connessa con più Stati, la determinazione della legge applicabile al caso, il riconoscimento della decisione resa in uno Stato diverso. In un ambito in cui i rapporti tra privati non sono più connessi a territori statuali[22], ma a spazi digitali sui quali è controversa l'appartenenza all'uno o all'altro Stato, piuttosto che all'Unione europea nel caso degli Stati membri della stessa, le regole del diritto internazionale privato si adeguano a nuovi criteri di localizzazione, declinando i metodi e i criteri propri della disciplina in maniera tale da assicurare la tutela fondamentale dei diritti nello spazio digitale[23]. Il diritto internazionale

[20] I. PRETELLI, *Protecting Digital Platform Users by Means of Private International Law,* in *Cuadernos de Derecho Transnacional,* 2021, n. 1, pp. 574–585; A. HEIN, M. SCHREIECK, T. RIASANOW, D. SOTO SETZKE, M., M. BÖHM, H. KRCMAR, *Digital platform ecosystems*, in *Electronic Markets,* 2020, n. 30, pp. 87-98; P. CONSTANTINIDES, O. HENFRIDSSON, G.G. PARKER, *Platforms and infrastructures in the digital age*, in *Information Systems Research*, 2018, n. 2, pp. 381– 400.

[21] Si v. Microsoft, *Digital Safety at Microsoft*, disponibile su https://www.microsoft.com/en-us/online-safety/digitalcivility?activetab=dci_reports%3aprimaryr3.

[22] Sulle difficoltà di localizzazione dei rapporti concernenti beni intangibili, si veda storicamente F. KAHN, *Gesetzeskollisionen, in Abhandlungen zum internationalen Privatrecht*, München & Leipzig, 1928 (1891), pp. 31-46.

[23] K. BOELE-WOELKI, C. KESSEDJIAN (eds.), *Internet, Which Court Decides? Which Law Applies? Quel tribunal decide? Quell droit s'applique?,* The Hague, 1998; B. FAUVARQUE-COSSON, *Le droit international privé Classique à l'épreuve des réseaux,*

privato adegua dunque metodi e approcci alla necessità di coordinare le regole volte ad individuare il giudice competente o la legge applicabile, in base agli effetti digitali delle singole fattispecie[24].

Ciò consente di tutelare alcuni diritti che potrebbero non apparire meritevoli di tutela in uno spazio non territoriale per natura, come lo spazio digitale, entro il quale per molto tempo non tutti hanno avuto l'esatta percezione di rispettare regole e diritti fondamentali. Si ricollega a tale tema il contrasto alla cyberviolenza digitale, che, come si è detto[25], può produrre danni gravi alle donne che la subiscono, in un contesto in cui violare la dignità femminile tramite la diffusione di immagini private, legate alla sfera intima, o seguire e controllare la vita privata tramite gli strumenti tecnologici, appare legittimato dall'assenza di regole precise in uno spazio "aterritoriale" per natura. Pertanto, l'individuazione del giudice competente ad esaminare una domanda di risarcimento danni delle vittime o dei loro parenti e a determinare la legge applicabile a tale domanda, condotta tramite le norme di diritto internazionale privato attualmente vigenti, va comunque orientata alla necessità di interpretare tali norme in maniera da rendere effettivo il contrasto a tale fenomeno. Si tratta di una ricerca non semplice, in cui si evidenzieranno lacune e criticità, ma anche alcuni spunti utili, nell'ambito di una più ampia evoluzione che il diritto internazionale privato sta subendo al fine di regolare le questioni rilevanti che contraddistinguono le fattispecie oggetto di realizzazione tramite le tecnologie digitali.

Si pensi ad es. alle *blockchain*, la tecnologia rivoluzionaria che può essere utilizzata in molti settori, assicurando la gestione sicura e decentralizzata delle informazioni o delle transazioni. Difficile localizzare gli effetti dell'impiego di tale tecnologia perché i nodi possono essere distribuiti in più paesi – difficile dunque individuare la legge applicabile e il giudice competente ai contratti conclusi tramite *blockchain* – i c.d. *smart contracts* – tramite indizi di collegamento propri della fattispecie.

in G. CHATILLON (ed.), *Le droit international de l'Internet,* Bruxelles, 2002, pp. 55-70.

[24] I. PRETELLI, *op. cit,* 212; A. HEIN, M. SCHREIECK, T. RIASANOW, D. SOTO SETZKE, M. WIESCHE, M. BÖHM, H. KRCMAR, *op. cit.*; P. CONSTANTINIDES, O. HENFRIDSSON, G.G. PARKER, *op. cit*.

[25] Si v. sul punto *supra* par. 1

Tecnologica è la via di accesso dei singoli a tali sistemi, dal momento che i diritti sui rapporti costituiti tramite *blockchain* sono inseriti in un *token* – un insieme di informazioni digitali registrate su una *blockchain* in grado di conferire un diritto ad un soggetto[26] – ovvero uno strumento informatico ricognitivo di una posizione giuridica su di un bene o su un rapporto obbligatorio emesso dal soggetto passivo a fronte di un apporto avente valore economico e che consente al soggetto attivo di esercitare uno o più diritti nei confronti dell'emittente.

Questa ricerca si inquadra, peraltro, in un ambito più ampio di interrelazione tra il diritto internazionale privato e la tutela dei diritti umani. È infatti innegabile che i diritti umani si pongono in un rapporto circolare con il diritto internazionale privato: da un lato, essi costituiscono la premessa per l'unificazione del diritto internazionale privato, garantendo agli Stati una base di valori comuni su cui costruire le regole uniformi (come accaduto nel quadro della comunitarizzazione del diritto internazionale privato); dall'altro lato, sono le norme del diritto internazionale privato a rappresentare un sicuro riferimento per promuovere la tutela dei diritti umani (si pensi ad es. al ruolo significativo della Convenzione dell'Aja del 1996 sulla responsabilità genitoriale nella promozione dei diritti fondamentali dei minori).

Il rapporto tra i due sistemi normativi è comunque complesso e di non facile coordinamento, come dimostra il dibattito tuttora in corso nella dottrina dei vari paesi sul punto[27]. Si tratta di un dibattito che at-

[26] Tribunale Firenze, sentenza del 21 gennaio 2019, n. 18/2019, disponibile su https://iusletter.com/wp-content/uploads/Tribunale-di-Firenze_20-gennaio-2019_18.pdf.

[27] P. KINSCH, *Droits de l'homme, droits fondamentaux et droit international privé*, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 2005, n. 318, pp. 9–332; E. JAYME, *Identité Culturelle et integration: le droit privé postmoderne. Cours général de droit international privé*, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 1995, n. 251, pp. 9–267, a p. 37; ID, *Menschrechte und Theorie de Internationalen Privatrechts*, in *Internationale Juristenvereinigung Osnabrück, Jahresheft*, 1991–1992, n. 2, p. 8 e ss.; R. PISILLO MAZZESCHI, *Responsabilité de l'Etat pour violation des obligations positives relatives aux droits de l'homme,* in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 2008, n. 333, pp. 175–506; Y. LEQUETTE, *Les mutations du droit international privé: vers un changement de paradigme?. Cours général de droit international privé*, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 2017, n. 387, pp. 20–633, a p. 628; F. SALERNO, *The*

traversa tutti gli ambiti della disciplina anche se con esiti differenti e con riguardo a obiettivi differenti. Elemento comune ai diversi ambiti è tuttavia il ruolo del diritto internazionale privato: in tutti gli ambiti di sua competenza esso si apprezza in quanto strumento interpretativo volto a coordinare le norme nazionali in vista delle peculiari esigenze di tutela dei diritti dell'uomo e dunque come strumento di supporto allo sviluppo degli stessi[28].

La complessità è condizionata anche dal contrasto tra categorie di diritti fondamentali garantiti, all'esito dell'emergere di nuovi diritti derivanti dall'evoluzione tecnologica. Si pensi ad es. al diritto all'oblio, ovvero al diritto di ottenere di essere dimenticati dal web, tramite la cancellazione dei propri dati personali oggetto di link in pagine web[29], diritto emerso a partire dalle note sentenze della Corte di giustizia UE nel caso *Google Spain*[30], secondo cui le informazioni possono essere rimosse dai motori di ricerca operanti nell'Unione europea se inadeguate, eccessive o non più pertinenti. Il "diritto all'oblio" prevale, in linea di principio, sull'interesse del pubblico ad accedere all'informazione "incriminata" nel corso di una specifica ricerca avente ad oggetto il nome di questa persona, a meno che non risulti, per motivi specifici quali il ruolo ricoperto da essa nella vita pubblica, che un'ingerenza nei suoi diritti fondamentali deve giustificarsi alla luce della prevalenza, nel bilanciamento degli interessi, di quello prevalente del pubblico ad avere accesso a detta informazione[31].

Nel 2019[32], sempre in seguito al rifiuto di Google di cancellare i

Identity and Continuity of Personal Status in Contemporary Private International Law, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 2018, n. 395, pp. 9–198 .

[28] F. SALERNO, *op .cit.*, p. 35 e ss.

[29] M. L. AMBROSE, J. AUSLOOS, *The right to be forgotten across the pond,* in *Journal of Information Policy*, 2003, n. 3, p. 2: "*Oblivion finds its rationale in privacy as a human/ fundamental right (related to human dignity, reputation)*".

[30] Corte di giustizia, 13 maggio 2014, causa C-131/12, *Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja González*.

[31] Corte di giustizia, sentenza del 13 maggio 2014, *Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja González*, cit., par. 99.

[32] Corte di giustizia, sentenza del 24 settembre 2019, cause riunite C- 136/17 e C-507/17, *GC e altri c. Commission nationale de l'informatique et des libertés (CNIL), Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*. Si v. inol-

link verso pagine web di soggetti terzi che comparivano nelle ricerche effettuate a partire dai nomi di soggetti coinvolti in fotomontaggi satirici e articoli di giornale relativi a casi di cronaca nera, inchieste giudiziarie e condanne penali, la Corte risponde affermativamente rispetto al quesito concernente la definizione come "trattamento dei dati personali" ai sensi dell'art. 2 lett. b) della direttiva delle attività del gestore di un motore di ricerca, consistenti nell'individuare informazioni pubblicate sul web da terzi e nell'indicizzarle automaticamente secondo le preferenze degli utenti. Tuttavia, essa riconosce che le peculiarità del trattamento effettuato dai gestori consentono di imporre loro soltanto l'obbligo di verifica *a posteriori*, sotto la vigilanza delle competenti autorità nazionali, in seguito a una espressa richiesta di cancellazione proveniente dall'interessato. La Corte, pur riconoscendo in via generale la prevalenza della tutela della riservatezza, afferma – per il gestore – l'obbligo di trovare un equilibrio con la libertà di informazione degli utenti, tenendo conto degli elementi pertinenti della fattispecie. In altri termini, il gestore dovrà comunque verificare se l'inserimento dei link tra i risultati della ricerca si presenta come *strettamente necessario* per proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad accedere alle informazioni, valutando la natura dell'informazione, la gravità dell'ingerenza nella vita privata (anche in ragione del carattere sensibile dei dati) e l'interesse pubblico a disporre dell'informazione, il quale potrebbe cambiare a seconda del ruolo rivestito dal titolare dei dati nella vita pubblica.

Rispetto alla sentenza del 2014 che non riconosce eccezioni, volte a tutelare la libertà di espressione di cui all'art. 11 della Carta dei diritti fondamentali dell'Unione europea, la sentenza del 2019 limita il diritto all'oblio nei casi in cui sia necessario tutelare tale libertà all'informazione. Però la Corte si limita ad affermare la necessità della cancellazione dei link nelle versioni dei motori di ricerca operanti nel territorio dell'Unione europea, riferendosi nel caso di una cancellazione c.d. globale ad "un danno sproporzionato alle libertà d'espressione, d'informazione, di comunicazione e di stampa, garantite, in particola-

tre sul tema del diritto all'oblio: Corte di giustizia, sentenza del 3 ottobre 2019, causa C-18/18*, Eva Glawischnig-Piesczek c. Facebook Ireland Limited*.

re, dall'art. 11 della Carta dei diritti fondamentali dell'Unione europea"[33].

3. *Giurisdizione e riconoscimento delle sentenze straniere in tema di responsabilità civile connessa alla cyberviolenza*

Problemi complessi sono determinati dalle eventuali azioni di responsabilità extracontrattuale per violazione dei diritti fondamentali, come nel caso delle azioni volte a garantire un risarcimento civile dei danni alle vittime di cyberviolenza.

Rispetto a tali azioni, differente appare essere la tutela delle vittime di cyberviolenza attraverso la soluzione delle questioni generali del diritto internazionale privato: individuazione del giudice competente ad esaminare la domanda di tutela della vittima, riconoscimento ed esecuzione della decisione che riconosca i diritti della vittima, determinazione della legge applicabile nel caso concreto.

Ciò, nonostante il fatto che nel dibattito concernente il più ampio tema della violazione dei diritti della personalità tramite Internet sia emerso anche l'orientamento in base al quale occorrerebbe elaborare una c.d. *lex electronica*, disciplina specificamente designata a regolare le fattispecie poste in essere tramite l'uso degli strumenti elettronici, ed applicata, ove possibile, da autorità giudiziarie cibernetiche[34]. Si è invece generalmente affermato come prevalente l'approccio volto ad individuare nell'applicazione dei tradizionali istituti del diritto internazionale privato la soluzione a tale questioni[35] (*old wine-private international law in new bottles – internet*[36]), ed è proprio in tale applicazione

[33] Corte di giustizia, *GC e altri c. Commission nationale de l'informatique et des libertés (CNIL),* cit., par. 38.

[34] S. HAYAKAWA*, Private Law in the Era of Internet*, in J. BASEDOW, T. KONO, *Legal Aspects of Globalization*, The Hague, 2000, pp. 27 – 34; A. MILLS, *The Law Applicable to Cross-border Defamation on Social Media: Whose Law Governs Free Speech in Facebookistan?,* in *Journal of Media Law*, 2015, n. 7, pp. 1-35.

[35] J. CARRASCOSA GONZALEZ, *The Internet – Privacy and rights relating to personality*, *Recueil des Cours de l'Académie de Droit International de l'Haye*, 2016, n. 378, pp. 261–486.

[36] P. O' CALLAGHAN, *Libel on the Internet,* in *Bar Review*, 2003, pp. 1-2, dis-

che si delineano alcuni spunti di possibile contrasto alla cyberviolenza di genere, deducibili dallo sviluppo normativo che ha riguardato altri ambiti, e che può costituire un modello per un'auspicabile evoluzione futura della disciplina internazionalprivatistica in materia.

Si tratta, tuttavia, di una disciplina oggetto di continua evoluzione e, allo stato, ancora condizionata dall'operatività dei criteri di giurisdizione e di collegamento attualmente in vigore, rivolti a situazioni che hanno una forte connessione con il territorio di un determinato Stato, quale ad es. il "luogo in cui l'evento dannoso è avvenuto o può avvenire"[37], con la conseguenza che essendo tali criteri non coerenti alla localizzazione nello spazio telematico, nel quale la violazione di un diritto della personalità ha una diffusione potenzialmente globale, si moltiplica proporzionalmente l'individuazione del giudice competente e della legge applicabile, rilevando in tale ambito la localizzazione delle azioni in ambiti non territoriali quali quelli dello spazio telematico (*domains*, social network, portali, piattaforme, forum, blog, ecc.).

Dal punto di vista dell'individuazione della giurisdizione, rilevano le norme del regolamento Bruxelles I *bis*[38]. Nel caso in cui i comportamenti ascrivibili alla cyberviolenza siano penalmente sanzionati entro gli ordinamenti nazionali[39], l'art. 7, par. 3, di tale atto prevede che l'azione di risarcimento danni o di restituzione nascente da illecito penale sia sottoposta all'autorità giurisdizionale presso la quale è esercita-

ponibile su http://homepage.eircom.net/~pocbl/articles/Libel_on_the_Internet.pdf.

[37] Si v. sul punto *infra* par. 4.

[38] Regolamento (UE) 1215/2012 del Parlamento europeo e del Consiglio, *concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (rifusione)*, del 12 dicembre 2012, in GUUE L 351/1 del 20 dicembre 2012, pp. 1-32; Sul punto si v. in generale F. SALERNO, *Giurisdizione ed efficacia delle decisioni straniere nel Regolamento (UE) n. 1215/2012 (rifusione)*, Vicenza, 2015, p. 82; ID, *Lezioni di diritto internazionale privato*, Milano, 2022, p. 111; U. MAGNUS, P. MANKOWSI, *Brussels I Regulation,* Munich, 2012, p. 436 ss.; F. POCAR, I. VIARENGO, F.C. VILLATA (a cura di), *Recasting Brussels I*, Padova, 2012; A. TRUNK, N. HATZIMIHAIL (eds.), *EU Civil Procedure Law and Third Countries. Which Way Forward?,* Baden-Baden, 2021, p. 53.

[39] Sul punto e sulla difformità degli ordinamenti nazionali in materia, attesa anche la molteplicità delle condotte riconducibili alla cyberviolenza, si v. in generale M.D. GOODMAN, S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace*, in *Oxford, International Journal of Law and Information Technology*, 2002, n. 2, p. 3.

ta l'azione penale, se può conoscere dell'azione civile in base alla propria legge. Non sono molti, tuttavia, gli ordinamenti che sanzionano tali fattispecie con una previsione criminosa *ad hoc*, come confermato dalla circostanza che la direttiva recentemente adottata per contrastare la violenza nei confronti delle donne[40], delinea ai considerando le motivazioni per le quali si rende necessario adottare norme minime in una materia trascurata dagli Stati. Si pensi ad es. al caso del crimine di *revenge porn*, che in molti paesi europei non ha una specifica previsione normativa volta a sanzionarne penalmente la condotta (eccetto Italia, Slovenia, Spagna), ma rientra nella più generale violazione del diritto alla privacy[41].

Ciò non senza trascurare che la tutela dei diritti fondamentali delle donne va coordinata con il rispetto di altri principi e diritti fondamentali, come chiarito ad es. dal considerando n. 20 della direttiva in esame: "La diffusione al pubblico tramite TIC di immagini, video o altro materiale ritraente atti sessualmente espliciti o le parti intime di una persona senza il consenso della persona non dovrebbe configurarsi come reato laddove necessaria per salvaguardare i diritti fondamentali tutelati dalla Carta, in particolare la libertà di espressione, compresa la libertà di ricevere e comunicare informazioni e idee in una società aperta e democratica, nonché la libertà delle arti e delle scienze, compresa la libertà accademica. Inoltre, il reato non dovrebbe riguardare il trattamento del materiale da parte delle autorità pubbliche, in particolare al fine di condurre procedimenti penali o di prevenire reati, individuarli e indagare su di essi, e gli Stati membri dovrebbero poter esentare una persona dalla responsabilità in determinate circostanze, come nel caso ad esempio di linee di assistenza telefonica o su internet che trattano materiale per segnalare un reato alle autorità".

Le azioni di risarcimento del danno derivante dalla diffusione di informazioni personali online, si propongono inoltre, secondo quanto prevede l'art. 7, par. 2 del regolamento Bruxelles I *bis*, dinanzi all'autorità giurisdizionale del luogo in cui l'evento dannoso è avvenu-

[40] Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio, cit.

[41] M. ŠEPEC, *Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence*, in *International Journal of Cyber Criminology*, 2019, n. 2, p. 418 e ss.

to o può avvenire. Per le violazioni dei diritti della personalità l'applicazione di tale criterio è particolarmente difficile perché si articola in sei momenti consecutivi, rispetto ai quali può rilevare l'individuazione del criterio di giurisdizione: la creazione del contenuto che viola i diritti fondamentali della vittima (lo scatto di una fotografia, o la creazione di un video); il trasferimento del contenuto ad una terza persona (l'invio di una mail, l'*upload* del video o della foto in un sito web); l'accesso della terza persona al contenuto lesivo (apertura dell'email o accesso a un sito web); la comprensione del contenuto lesivo da parte della terza persona; le conseguenze della violazione dei diritti della personalità della vittima (la vittima viene licenziata, riceve una domanda giudiziale di divorzio); gli effetti delle conseguenze dirette della violazione dei diritti della personalità (la vittima ha una perdita economica, la vittima si sente umiliata, la vittima si suicida)[42]. Ai fini dell'applicazione dell'art. 7 par. 2 del regolamento Bruxelles I *bis* l'analisi della giurisprudenza comparata ha evidenziato che il riferimento al luogo in cui si è verificata l'azione va riferito al trasferimento del contenuto ad una terza persona, mentre l'evento dannoso si individua con riguardo alla comprensione del contenuto dannoso da parte di una terza persona[43].

L'applicazione della norma dell'art. 7 par. 2 del regolamento Bruxelles I *bis* deve peraltro ispirarsi alla giurisprudenza della Corte di giustizia che ha da tempo elaborato tre fondamentali principi in relazione alle diverse tipologie di illecito, ovvero l'illecito extracontrattuale a distanza, l'illecito complesso e con danni plurilocalizzati, che pongono molti problemi interpretativi quando vengono realizzati tramite Internet (c.d. *cyber torts*)[44]. Rileva, in primo luogo, il principio della piena dicotomia tra azione ed evento o teoria ubiquitaria (*ubiquity rule* o *Ubiquitätsregel*), per la prima volta sancito nel caso *Mines de Potasse*[45], che attribuisce all'attore, nei casi di illeciti a distan-

[42] D.J. B. SVANTESSON, *Private International Law and the Internet*, Alphen aan den Rijn, 2021.

[43] J. CARRASCOSA GONZALEZ, *op. cit.*, p. 334.

[44] E. GABELLINI, *La competenza giurisdizionale nel caso di lesione di un diritto della personalità attraverso internet*, in *Rivista trimestrale di diritto e procedura civile*, 2014, n. 1, p. 271.

[45] Corte di giustizia, sentenza del 30 novembre 1976, in causa C- 21/1976, *Han-*

za, la facoltà di scegliere se adire il giudice del luogo del fatto dannoso (*locus actus*) o il giudice del luogo in cui si è verificato il danno (*locus damni*). Per l'illecito complesso viene poi in considerazione il principio del fatto causale iniziale, elaborato nella sentenza *Shevill*[46], in base al quale è dotato di competenza giurisdizionale il giudice del luogo in cui è localizzato l'evento causale iniziale che ha dato origine al danno (se tale fatto è di per sé idoneo a cagionare il danno stesso). Nel caso di danni plurilocalizzati si deve considerare il principio, elaborato sempre nel quadro del caso *Shevill*[47]*,* del trattamento a mosaico (*mosaic principle*)[48], in base al quale il giudice del luogo del fatto dannoso è competente a conoscere del risarcimento della totalità dei danni mentre il giudice del luogo del danno è competente per i soli danni cagionati nella circoscrizione del giudice adito. La Corte di giustizia dell'Unione europea ha poi ampliato il principio della dicotomia tra azione e danno, individuando un terzo foro adibile, da individuarsi, ad es. in materia di diffamazione online, nel centro di interessi della persona fisica diffamata[49] e nel centro di interessi della persona giuridica diffamata[50].

Nella sentenza *Shevill*, la Corte di giustizia ha confermato la teoria ubiquitaria, adeguandola a una controversia diffamatoria a mezzo stampa e ha elaborato il principio del fatto causale iniziale e del trattamento a mosaico. In particolare, la Corte ha stabilito che sono competenti a conoscere del risarcimento del danno cagionato alla reputazione e alla considerazione di persone fisiche o giuridiche[51] sia i giudici del luogo in cui è stabilito l'editore della pubblicazione diffamatoria in quanto "luogo di origine del fatto dannoso a partire dal quale la dif-

delskwekerij G. J. Bier BV c. Mines de Potasse d'Alsace SA.

[46] Corte di giustizia, sentenza del 7 marzo 1995, causa C-68/93, *Shevill e a*.

[47] Corte di giustizia, *Shevill e a.,* cit.

[48] P. FRANZINA, *La giurisdizione in materia contrattuale: l'art. 5 n. 1 del Regolamento n. 44/2001/ CE nella prospettiva della armonia delle decisioni*, Padova, 2006, p. 409.

[49] Corte di giustizia, sentenza del 25 ottobre 2011, cause riunite C-509/09 e C-161/10, *E Date Advertising.*

[50] Corte di giustizia, sentenza del 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ e Ingrid Ilsjan c. Svensk Handel AB*.

[51] Corte di giustizia, *Shevill e a*., cit., par. 23.

famazione è stata formulata e messa in circolazione"[52], sia i giudici del luogo di diffusione della pubblicazione quando la vittima sia ivi conosciuta (luogo del danno). Il giudice in cui è domiciliato l'editore conosce del risarcimento totale o integrale del danno, mentre il giudice del luogo in cui è diffusa la pubblicazione conosce del risarcimento parziale ossia dei soli danni cagionati, in tale Stato, alla reputazione e all'onore della vittima[53].

Nella sentenza *eDate*, la Corte di giustizia ha adattato i principi interpretativi formulati nel caso *Shevill* alla diffamazione tramite Internet, dal momento che, a differenza della diffusione di notizie lesive della reputazione tramite stampa, le informazioni divulgate online sono immediatamente e universalmente accessibili da un numero potenzialmente indeterminato di utenti in qualunque parte del mondo e in qualsiasi momento (c.d. ubiquità della Rete). La Corte ha pertanto stabilito che sussiste una difficoltà di attuazione e una minore utilità del criterio della diffusione quale luogo del danno che, nei casi di diffamazione a mezzo Internet, è, infatti, universale[54]. La vittima della diffamazione ha dunque la facoltà di scegliere se adire, oltre al foro generale del domicilio del convenuto, quale giudice del luogo del fatto competente a conoscere del risarcimento integrale del danno subito, il giudice del luogo in cui è stabilito il soggetto che ha messo in Rete i contenuti diffamatori o il giudice del luogo in cui si trova il centro di interessi dell'attore stesso, vittima della diffamazione (*forum actoris*)[55] o quale giudice del luogo del danno, competente a conoscere del risarcimento del solo danno subito sul territorio dello Stato membro del giudice adito, il giudice del luogo in cui l'informazione messa in Rete sia accessibile o lo sia stata[56]. La previsione della possibile operatività del *forum actoris*, che costituisce la significativa novità della sentenza *eDate*, corrisponde al duplice obiettivo della buona amministrazione della giustizia e della prevedibilità, per l'attore, del giudice adibile e,

[52] *Ivi*, par. 24.
[53] *Ivi*, parr. 29-30.
[54] Corte di giustizia, *E Date Advertising,* cit., parr. 45-48.
[55] *Ivi*, par. 48.
[56] *Ivi*, par. 51.

per il convenuto, del giudice dinanzi al quale può essere citato in giudizio[57].

Si tratta di una disciplina suscettibile di estendersi alle violazioni dei diritti della personalità delle vittime di cyberviolenza. Alla luce del principio del *favor laesi* che ispira l'operatività di tale disciplina, e attese le molteplici forme che può assumere la cyberviolenza[58], appare possibile ipotizzare il funzionamento del *forum actoris* per la violazione della dignità della vittima tramite un atto compiuto via Internet, seppure nei limiti indicati dalla Corte di giustizia dell'Unione europea nei casi in cui un soggetto lamenti comportamenti offensivi dell'intera collettività nazionale di appartenenza[59].

Più complesso è il tema del riconoscimento e dell'esecuzione delle decisioni straniere, soprattutto nei casi in cui le sentenze europee che limitino la libertà di espressione in forza della necessità di tutelare altri diritti fondamentali debbano essere riconosciute in paesi extra UE.

Rileva in questo ambito una tendenza recentemente sviluppata dall'Unione europea al fine di affermare la propria sovranità tecnologica o digitale[60].

[57] *Ivi*, par. 50.

[58] Corte di giustizia, *Shevill e a.*, cit., parr. 29 e 30.

[59] Corte di giustizia, sentenza del 17 giugno 2021, causa C-800/19, *Mittelbayerischer Verlag KG c. SM*. Un cittadino polacco ha convenuto in giudizio, davanti al Tribunale regionale di Varsavia, la società tedesca Mittelbayerischer Verlag ch, accusandola di aver violato i propri diritti all'identità e alla dignità nazionali tramite la pubblicazione su Internet di un articolo (redatto in lingua tedesca, ma accessibile anche in Polonia) asseritamente offensivo della nazione polacca. In tale contributo, infatti, si definiva "campo di sterminio polacco" un campo di concentramento nazista, sito nel territorio dell'attuale Polonia (all'epoca occupata dalla Germania), con il rischio di ingenerare nei lettori l'errato convincimento che i crimini ivi commessi dai soldati tedeschi fossero stati invece perpetrati dal popolo polacco.

[60] Il Presidente della Commissione europea Junker aveva parlato "dell'ora della sovranità europea" sin dal suo discorso sullo Stato dell'Unione del 12 settembre 2018. Il Consiglio dell'Unione ha fatto riferimento a tale concetto nelle sue conclusioni sull'importanza del 5G per l'economia europea e sulla necessità di attenuare i relativi rischi per la sicurezza, GUUE 2019, C 414/7. La Commissione europea, presieduta da Ursula Von Der Leyen, ha parlato di "sovranità tecnologica dell'Europa", nel 2020. Si v. Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni, *Una nuova strategia industriale per l'Europa*, del 10 marzo 2020, COM (2020) 102, pp. 4, 15.

Nei regolamenti adottati nel quadro della c.d. sovranità digitale dell'UE vengono disposte alcune norme ispirate al metodo unilateralistico, nell'affermare che si applicano – ad es. entro il *Data Act*[61] – "ai fabbricanti di prodotti immessi sul mercato dell'Unione e ai fornitori di servizi correlati indipendentemente dal loro luogo di stabilimento di tali fabbricanti e fornitori", ai "titolari dei dati, indipendentemente dal loro luogo di stabilimento, che mettono dati a disposizione dei destinatari di dati nell'Unione", "ai fornitori di servizi di trattamento dei dati, indipendentemente dal loro luogo di stabilimento, che forniscono tali servizi a clienti nell'Unione".

Il *Data Act* utilizza quindi una tecnica del diritto internazionale privato per definire la propria applicazione extra territoriale: se i soggetti considerati dal regolamento – gli attori principali del mercato dei dati – si rivolgono verso il territorio dell'Unione europea, il regolamento dispone che essi debbano adeguarsi al *Data Act* nella misura in cui le loro attività rientrano in quelle descritte dall'art. 1 par. 3 di tale fonte.

Si tratta di una scelta suscettibile di creare conflitti con altri ordinamenti giuridici interessati ad estendere la propria sovranità e la propria disciplina sulla Rete e sul trattamento dei dati, materie fortemente condizionate dalle scelte politiche degli Stati.

Ciò si tradurrà in un'inevitabile compressione dei diritti fondamentali degli individui. Si pensi ad es. ad una azione di risarcimento dei danni da responsabilità extracontrattuale fondata su violazioni del *Data Act,* ad es. rivelazione dei dati contenuti in una banca dati oggetto di comunicazione a terzi sulla base del *Data Act*, in violazione di quanto prevede l'art. 1 del regolamento ora in esame. Le norme dallo stesso poste si applicano indipendentemente dalla legge applicabile alla fattispecie (nel caso specifico individuate tramite le norme del regolamento Roma II[62]) con la conseguenza che se il titolare dei diritti sui

[61] Si veda il regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, *riguardante norme armonizzate sui dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva UE 2020/1828*, del 13 dicembre 2023, in GUUE L del 22 dicembre 2023, pp. 1-71, che sarà applicabile dal 12 settembre 2025.

[62] Regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, *sulla legge applicabile alle obbligazioni extracontrattuali ("Roma II")*, dell'11 luglio 2007, in GUUE L 199 del 31 luglio 2007, p. 40 ss. Su di esso si v.: F. POCAR, *Nelle nuove ob-*

dati agisce dinanzi al giudice di uno Stato membro potrà avere la tutela prevista dal *Data Act*, ma difficilmente questa stessa tutela gli verrà riconosciuta dai giudici degli Stati terzi. La sentenza pronunciata dal giudice di uno Stato europeo sarà dunque difficilmente riconoscibile in uno Stato terzo, con evidente compressione del diritto fondamentale di agire in giudizio per vedere tutelati i propri diritti in materia.

Nel caso in cui un paese terzo regoli in maniera diversa il trasferimento dei dati "le autorità incaricate dell'applicazione della legge di paesi terzi, che dispongono un tale trasferimento di dati non personali o l'accesso agli stessi dovrebbero avere carattere esecutivo quando sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, come ad esempio un trattato di mutua assistenza giudiziaria. In altri casi possono verificarsi situazioni in cui una richiesta di trasferimento di dati non personali o di accesso agli stessi basata sulla legislazione di un paese terzo sia in conflitto con l'obbligo di proteggere tali dati a norma del diritto dell'Unione o dello Stato membro pertinente, in particolare per quanto riguarda la tutela dei diritti fondamentali dell'individuo, quali il diritto alla sicurezza e il diritto a un ricorso effettivo, o gli interessi fondamentali di uno Stato membro connessi alla sicurezza nazionale o alla difesa, nonché la protezione dei dati sensibili sotto il profilo commerciale, inclusa la protezione dei segreti commerciali, e la protezione dei diritti di proprietà intellettuale, compresi gli impegni contrattuali dello Stato membro in materia di riservatezza conformemente a tale legislazione.

In assenza di accordi internazionali atti a disciplinare simili questioni, il trasferimento o l'accesso a dati non personali dovrebbero essere consentiti solo se è stato verificato che l'ordinamento giuridico del paese terzo impone che siano indicati i motivi e la proporzionalità della decisione, che la sentenza o decisione abbia carattere specifico e che l'obiezione motivata del destinatario sia sottoposta al riesame da parte di un organo giurisdizionale competente di un paese terzo, cui sia con-

bligazioni extracontrattuali alle parti una scelta sulla legge applicabile, in *Guida al Diritto,* 2007, n. 5, p. 11 ss.; P. FRANZINA, *Il regolamento n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali*, in *Nuove Leggi Civili Commentate,* 2008, n. 5, p. 971 ss.

ferito il potere di tenere debitamente conto dei pertinenti interessi giuridici del fornitore di tali dati"[63]. In tal caso l'approccio unilaterale del *Data Act* consente di assumere la tutela dei diritti fondamentali ivi indicati come limite alla circolazione delle sentenze emanate negli Stati terzi.

Si pensi ad es. alla giurisprudenza statunitense che utilizza la libertà d'espressione garantita dal primo emendamento della Costituzione al fine di contrastare il riconoscimento delle sentenze straniere in cui si applichi una legge straniera che abbia derogato alla libertà d'espressione in forza di altri diritti fondamentali da tutelare[64].

Non è dunque certo che l'affermata tutela delle donne vittima di cyberviolenza in una sentenza che condanni il responsabile al risarcimento dei danni civili riceva concreta applicazione in un paese terzo. D'altra parte, in Italia è tristemente noto il caso di Tiziana Cantone che si è suicidata per non essere riuscita ad ottenere la cancellazione di video intimi diffusi dall'ex fidanzato su YouTube, in seguito al quale è stato riformato il codice penale tramite l'adozione del c.d. "Codice rosso"[65]. Sarebbe pertanto opportuno che il principio del *favor laesi*, che consente alle vittime di cyberviolenza di adire la giurisdizione ad esse più vicina o più favorevole, orientasse anche l'applicazione delle regole attualmente vigenti in tema di riconoscimento delle sentenze straniere, o costituisse lo stimolo per sviluppare una più ampia cooperazione tra Stati in materia.

4. *Legge applicabile ai casi di responsabilità civile derivante da cyberviolenza*

La disciplina della responsabilità civile per violazione attraverso Internet dei diritti della personalità, quale quella che si verrebbe a de-

[63] Considerando 101, regolamento (UE) 864/2007, cit.

[64] Si veda ad es. *Yahoo! Inc.v.La Ligue contre le Racisme*, 169 FSupp. 2d 1181 (ND Cal.2001); *Yahoo! Inc.v.La Ligue contre le Racisme*, 433 F3d 1199 (9th Cir.2006) sul punto P. KINSCH, *op.cit.*, p. 239 e ss.

[65] G. CALETTI, *Il Testo Del Disegno Di Legge "Codice Rosso"*, in *Diritto Penale Contemporaneo*, 2019, disponibile su https://archiviodpc.dirittopenaleuomo.org/d/6622-il-testo-del-disegno-di-legge-codice-rosso-revenge-porn-costrizione-o-induzione-al-matrimonio-defor.

lineare nei casi di cyberviolenza, è un tema ampiamente dibattuto. In tale ambito, non risulta, tuttavia, prevalente l'orientamento in base al quale, come si è detto, occorrerebbe elaborare una c.d. *lex electronica*, disciplina specificamente designata a regolare le fattispecie poste in essere tramite l'uso degli strumenti elettronici, quale ad es. la c.d. legge di "*Facebookistan*", volta a realizzare le fattispecie realizzate sullo spazio non statuale del noto social media Facebook, c.d. *Facebookistan*[66].

È, infatti, ritenuto preferibile l'approccio c.d. classico, ovvero rivolto a regolare tali situazioni tramite la legge individuata dalle norme di conflitto del giudice adito.

La violazione dei diritti della personalità è tuttavia generalmente sottratta all'applicazione delle norme poste entro il diritto internazionale privato dell'Unione europea. Infatti, il regolamento Roma II, all'art. 1, par. 2, lett. g), esclude espressamente le obbligazioni extracontrattuali che derivano da violazioni della vita privata e dei diritti della personalità, compresa la diffamazione[67].

La disciplina relativa alla individuazione della legge applicabile a tali casi andrà cercata nelle norme di fonte nazionale.

Si tratta di una soluzione che non ha mancato di evidenziare numerose criticità e pertanto in seguito alla sentenza della Corte di giustizia dell'Unione europea in materia di criteri di giurisdizione in tema di azioni di responsabilità civile per violazione dei diritti della personalità[68], la Commissione giuridica del Parlamento europeo ha presentato un progetto di relazione recante raccomandazioni alla Commissione circa la modifica del regolamento Roma II, al fine di introdurre una norma concernente l'individuazione della legge applicabile alla re-

[66] A. MILLS, *The Law Applicable to Cross-border Defamation on Social Media: Whose Law Governs Free Speech in Facebookistan?,* in *Journal of Media Law*, 2015, n. 1, pp. 1-35.

[67] Sul punto si v. in generale: J. K. KUIPERS, *Towards a European Approach in the Cross- Border Infringment of Personality Rights,* in *German Law Journal*, 2011, n. 12, pp. 1681-1806; O. BOSKOVIC, *Règlement Rome II*, in *Répertoire Dalloz Droit international,* 2010; C. CAMPIGLIO, *La legge applicabile alle obbligazioni extra-contrattuali (con particolare riguardo alla violazione della privacy),* in *Rivista di diritto internazionale privato e processuale*, 2015, n. 4, p. 857 e ss.

[68] Corte di giustizia, *E Date Advertising*, cit.

sponsabilità civile da violazione della vita privata e dei diritti della personalità.

In Italia, rileva la norma contenuta nell'art. 62 della Legge 218/95, che sancisce l'applicabilità della legge del luogo in cui si è verificato l'evento. Un temperamento a questo collegamento viene poi offerto dalla II parte dell'art. 62, 1° c., che concede al danneggiato la facoltà di chiedere l'applicazione della legge dello Stato in cui è avvenuto il fatto generatore. In questo modo, in applicazione della c.d. teoria dell'ubiquità, da tempo seguita dalla giurisprudenza costante della Corte di giustizia di Lussemburgo, in tema di giurisdizione già relativamente all'interpretazione dell'art. 5, 3° c., della Convenzione di Bruxelles del 1968, che utilizza come criterio speciale di giurisdizione, in materia di delitti o quasi delitti, il luogo in cui l'evento dannoso è avvenuto[69], in seguito codificata ad opera del regolamento Bruxelles I, e confermata – come si è detto[70] - nel regolamento Bruxelles I *bis*, il danneggiato, che intenti l'azione di risarcimento, può scegliere la legge applicabile al caso.

Una deroga rilevante all'applicabilità della disciplina in esame ricorre però nel caso in cui tutte le persone coinvolte nel fatto illecito siano cittadine del medesimo Stato in esso residenti, dal momento che si applicherà la legge di tale Stato. Il quadro complessivo della regolamentazione della materia è poi completato dall'esclusione del rinvio (art. 13, 2° c., lett. c), pienamente condivisibile per quanto concerne questa disposizione, soprattutto in considerazione dell'accoglimento del collegamento della scelta di legge. Nel caso di richiamo di una disciplina che non contempli la fattispecie dannosa potrebbe rilevare il limite dell'ordine pubblico secondo quanto prevede l'art. 16 della Legge 218/95. Il riferimento del limite in esame all'esclusione di effetti inaccettabili, derivanti dall'operatività di norme straniere, consente peraltro di ampliarne, in via ermeneutica, la portata fino ad incidere non tanto sul richiamo dell'ordinamento straniero nel suo astratto contenuto generale, quanto sulle conseguenze che le disposizioni individuate all'interno di esso producono nel caso concreto. La conseguenza dell'accertato contrasto con l'ordine pubblico degli effetti dell'ap-

[69] Corte di giustizia, *Mines de Potasse d'Alsace*, cit.

[70] Si v. sul punto *supra* par. 3.

plicazione della legge straniera si individua nella completa disapplicazione di quest'ultima, non essendo proponibili interpretazioni rivolte all'adattamento o alla depurazione[71] del diritto straniero, in base agli assunti propri del sistema italiano di diritto internazionale privato. In caso di accertato contrasto con l'ordine pubblico della legge applicabile ad una determinata fattispecie, si effettuerà dunque dapprima il richiamo di un altro ordinamento che presenti una connessione significativa con la fattispecie contenente elementi di estraneità; in mancanza di altri collegamenti, si applicherà, a titolo residuale, la *lex fori*. L'ordine pubblico può dunque diventare uno strumento di tutela rilevante, nel caso in cui la legge richiamata a regolare la responsabilità civile da cyberviolenza non contempli tale fattispecie dannosa. Ciò soprattutto alla luce dell'importante evoluzione delle fonti internazionali poste a tutela delle vittime di cyberviolenza, con particolare riguardo alla cyberviolenza di genere[72], nonché dell'ordinamento italiano, che evidenziano la necessità di orientare l'interpretazione delle norme di diritto internazionale privato al fine di rendere effettiva tale tutela.

La soluzione, ispirata dal principio del *favor laesi*, è peraltro comune ad altri sistemi di diritto internazionale privato, entro i quali il c.d. *Günstigkeitsprinzip* ispira la ricerca della legge applicabile alla responsabilità civile, come ad es. nell'EGBGB a seguito della riforma del 1999 (art. 40), o nella specifica norma posta per individuare la disciplina della violazione dei diritti della personalità nella legge belga di diritto internazionale privato (artt. 99–100)[73]. Non si tratta di una so-

[71] Tali interpretazioni vengono proposte dalla dottrina tedesca sulla base di considerazioni di carattere generale, quale ad esempio la circostanza che l'alternativa ad essa, e cioè l'operatività della *lex fori* in forza dell'ordine pubblico, è spesso priva di legami con la questione controversa. In tale contesto appare dunque preferibile la sostituzione del diritto straniero con altre norme appartenenti allo stesso sistema giuridico, che vengono rese applicabili, in forza di un adattamento alle circostanze del caso, una volta eliminate le regole contrarie all'ordine pubblico del foro. Si veda sul punto: F. VISCHER, *General Course on Private International Law*, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 1992, n. 232, p. 104; P. LAGARDE, *Recherches sur l'ordre public en droit international privé*, Paris, 1959, p. 237; F. MOSCONI, *Exceptions to the Operation of Choice of Law Rules*, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 1989, n. 217, p. 109 ss.

[72] Si v. sul punto *supra*.

[73] J. VON HEIN, *Das Grünstigkeitsprinzip im Internationalen Deliktsrecht*, Tüingen,

luzione uniformemente seguita in tutti gli Stati membri dell'Unione europea, poiché ad es. in Spagna l'art. 10, par. 9 *código civil* fa riferimento alla residenza abituale della vittima[74].

Il regolamento Roma II, come noto, l'ha codificata solo in materia di responsabilità civile ambientale all'art. 7, coerentemente a quanto sancito dalla giurisprudenza della Corte di giustizia dell'Unione europea in materia a partire dal caso *Mines de Potasse*[75]. Al fine di contrastare la violenza di genere, è dunque auspicabile una riforma del regolamento Roma II, che, coerentemente alla estensione del principio del *favor laesi* in materia di scelta del giudice competente, regoli anche la determinazione della legge applicabile alla responsabilità civile derivante da cyberviolenza.

Ciò anche se si tratta di una soluzione non priva di alcune implicazioni problematiche.

Ricorrono ad es. le incertezze di ricollegare la fattispecie al luogo in cui si è realizzato l'evento dannoso o a quello in cui si è compiuto il fatto generatore dell'illecito, in assenza di scelta da parte del danneggiato. Tali difficoltà verrebbero poi ulteriormente acuite se si seguisse l'orientamento – sviluppatosi in Italia, in applicazione dell'art. 62 Legge 218/95 –, secondo cui la previsione della facoltà di scelta del danneggiato, come criterio di collegamento, non priva il giudice di un certo potere valutativo, al fine di consentirgli di applicare la legge che garantisca in maniera più efficace gli interessi del titolare del diritto che si afferma essere leso. Inoltre, mette conto rilevare che l'applicazione della legge del luogo in cui si è verificato l'evento può non risultare sempre facilmente individuabile nell'ambito degli illeciti, come la cyberviolenza, in cui il *locus delicti* è multiplo, non solo a causa della dissociazione tra atto generatore dell'evento dannoso e danno, ma anche a causa della frantumazione di tali elementi sul territorio di paesi diversi. Occorrerà accertare innanzitutto se è possibile applicare la legge del luogo in cui si è verificato un effetto secondario oppure se occorre seguire sempre e comunque quella del luogo in cui è stata posta in essere la lesione principale. Ad es., in materia di violazione del diritto al-

1999; G. SCHMIDT, *Ehrverletzungen in der elektronischen Presse,* Bern, 2020.

[74] Sul punto, si veda J. CARRASCOSA GONZALEZ, *op. cit.*, p. 394.

[75] Corte di giustizia, *Mines de Potasse d'Alsace*, cit.; Corte di giustizia, *Shevill*, cit.

la reputazione, si è osservato che si dovrà considerare il luogo in cui la pubblicazione ha avuto diffusione o il programma televisivo è stato trasmesso e il danneggiato era conosciuto; in caso contrario, non si potrebbe infatti ritenere effettivamente realizzato l'evento dannoso[76]. Inoltre, in assenza di indicazioni diverse, non è escluso che l'applicazione del collegamento del luogo dell'evento possa condurre a un *dépeçage* del fatto illecito ed all'applicabilità ad esso di leggi diverse, con le difficoltà che il contemperamento di esse può comportare specialmente per quanto riguarda la condotta dell'agente.

5. *Osservazioni conclusive*

La necessità di tutelare i diritti fondamentali nel contesto digitale è un tema ampio entro il quale si evidenzia anche la protezione delle donne vittime di cyberviolenza, fenomeno quanto mai diffuso proprio a causa dell'ampio raggio d'azione degli strumenti digitali.

Il diritto internazionale privato ha da tempo sviluppato metodi e strumenti per contrastare le violazioni dei diritti della personalità.

Si tratta di strumenti efficaci, relativamente all'individuazione del giudice competente, tema rispetto al quale il principio del *favor laesi* consente l'esercizio dell'azione a tutela delle vittime nei fori in cui sia ravvisabile un effetto della violazione. Come si è visto, in tale ambito, la difficoltà maggiore all'effettiva tutela delle vittime è meta-giuridica, ovvero collegabile all'oggettiva difficoltà che le vittime di tale violenza hanno ad agire in giudizio.

Poco coerente con l'efficace tutela delle vittime di violenza risulta essere invece l'attuale disciplina del riconoscimento delle decisioni estere, che, in assenza di strumenti di cooperazione internazionale, rimane rimessa alle norme dei singoli Stati, evidenziando delle difficoltà, come si è visto, all'atto dell'applicazione di norme unilaterali quali quelle recentemente adottate dall'Unione europea per affermare la propria sovranità digitale.

[76] Si v. ad es. Tribunale di Roma, sentenza del 16 dicembre 2009, n. 728, *RIPP*, per il noto caso della diffusione su YouTube della serie Grande Fratello; Tribunale di Milano, ordinanza del 16 marzo 2009, n. 112, *RIPP*.

Incerta appare essere anche l'individuazione della legge applicabile alla responsabilità civile derivante da cyberviolenza, alla luce della lacuna presente nella disciplina di fonte europea, attualmente vigente, ovvero il regolamento Roma II.

Nel contesto delle differenti discipline nazionali, quella italiana può forse rappresentare un modello cui ispirare un'eventuale riforma del regolamento Roma II, per rendere più uniformemente efficace la disciplina che individua la legge applicabile in materia, in vista di una migliore tutela in sede civile delle vittime di cyberviolenza.

Evidente, dunque, anche all'esito dell'analisi degli spunti che le attuali norme di diritto internazionale privato offrono al contrasto della violazione dei diritti della personalità realizzata tramite Internet, che si stia delineando una possibile evoluzione delle stesse[77], dalla quale può trarsi qualche spunto utile al contrasto della cyberviolenza nei confronti delle donne.

Una volta verificate le criticità prodotte nello spazio cibernetico da criteri di giurisdizione e di collegamento legati alla connessione territoriale della fattispecie di diritto internazionale privato – quale ad es. il luogo in cui si verifica l'evento dannoso – è possibile ipotizzare l'adozione in materia di nuovi criteri che considerino il reale impatto delle condotte realizzate tramite Internet sulle persone e sulla società. Seppure, in una realtà sempre più globalizzata, per individuare giudice competente e legge applicabile alle violazioni dei diritti della personalità realizzate tramite Internet, occorre allora definire, tramite norme *ad hoc,* delle connessioni giuridiche forti tra le violazioni realizzate nello spazio di Internet e le vittime, quali ad es. il luogo di residenza abituale della vittima[78], o dell'autore della violazione, il luogo in cui la vittima lavora, o il luogo in cui la famiglia della vittima ha la residenza abituale.

[77] B. GROSSFELD, *Global Accounting: where Internet meets Geography*, in *The American Journal of Compartive Law,* 2000, n. 2, pp. 261- 306; P.E. GELLER, *Conflicts of Law in Cyberspace: Rethinking International Copyright in a Digitally Netwrked World*, in *Columbia-VLA Journal of Law and the Arts*, 1996, n. 20, pp. 571 – 599.

[78] Per un'elaborazione di questo criterio anteriore alle violazioni realizzate tramite Internet, si v. P. BOUREL, *Du rattachement de quelques délits spéciaux en droit international privé*, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 1989, n. 214, pp. 251- 398.

Inoltre, poiché la complessità di Internet si rivela in continua evoluzione, appare anche opportuno prevedere una clausola di eccezione che consenta al giudice di individuare la soluzione più efficace ai fini di tutelare i diritti fondamentali della vittima, ad es. ispirandosi al principio di effettività o della connessione più significativa della fattispecie con un determinato sistema giuridico[79]. L'ordine pubblico è un limite generale all'operatività della legge straniera, che può rilevare, come si è detto[80], anche nel caso in cui l'ordinamento richiamato non prevede la fattispecie dannosa lesiva dei diritti fondamentali, ma alla luce della flessibilità e discrezionalità che contraddistingue l'operatività dello stesso[81], ipotizzare, oltre all'operatività di questo limite generale, la previsione di una clausola d'eccezione specifica[82], in sede di riforma del regolamento Roma II, potrebbe forse più coerentemente tutelare i diritti fondamentali delle donne vittime di violenza di genere.

Abstract

L'uso delle nuove tecnologie incide sui diritti fondamentali degli individui, che svolgono interazioni sociali tramite le piattaforme digitali, che consentono a chiunque di accedervi, creando un proprio profilo per acquistare beni, biglietti aerei, ferroviari, ascoltare musica, vedere film, spettacoli teatrali, interagire con altre persone, ecc. È in tale contesto che si può indagare il ruolo del diritto internazionale privato come strumento volto a rendere efficace ed

[79] Si veda in tal senso J. CARRASCOSA GONZALEZ, *op. cit.*, p. 307.

[80] Si v. *supra* par. 4.

[81] A. BUCHER, *L'ordre public et le but social des lois en droit international privé*, in *Recueil des Cours de l'Académie de Droit International de l'Haye*, 1993, n. 239, pp. 9 – 116.; P. HAMMJE, *Droits fondamentaux et ordre public,* in *Revue critique de droit international privé,*1997, n. 1, pp. 1 -31, a p. 9; O. FERACI, *L'ordine pubblico nel diritto dell'Unione europea,* Milano, 2012; S. MARINAI, *I valori comuni nel diritto internazionale privato e processuale comunitario*, Torino, 2007; F. SALERNO, *La costituzionalizzazione dell'ordine pubblico internazionale*, in *Rivista di diritto internazionale privato e processuale*, 2018, n. 2, p. 259 ss.; G. PERLINGIERI, G. ZARRA, *Ordine pubblico interno e internazionale tra caso concreto e sistema ordinamentale,* Napoli, 2019.

[82] F. VISMARA, *Le clausole di eccezione nel diritto internazionale privato*, Milano, 2018.

effettiva la tutela dei diritti fondamentali, quale premessa concettuale per analizzare possibili spunti di contrasto alla cyberviolenza di genere entro la disciplina ora considerata. Tale ruolo si apprezza nel momento in cui il diritto internazionale privato mira a risolvere i problemi di coordinamento tra sistemi giuridici, tradizionali per la disciplina, ovvero l'individuazione del giudice competente ad esaminare una controversia connessa con più Stati, la determinazione della legge applicabile al caso, il riconoscimento della decisione resa in uno Stato diverso. In un ambito in cui i rapporti tra privati non sono più connessi a territori statuali, ma a spazi digitali sui quali è controversa l'appartenenza all'uno o all'altro Stato, piuttosto che all'Unione europea nel caso degli Stati membri della stessa, le regole del diritto internazionale privato si adeguano a nuovi criteri di localizzazione, declinando i metodi e i criteri propri della disciplina in maniera tale da assicurare la tutela fondamentale dei diritti nello spazio digitale.

KEYWORDS: Diritto internazionale privato – cyberviolenza – diritti umani – responsabilità civile da cyberviolenza – tutela delle donne

LA CIBERVIOLENCIA DE GÉNERO: ALGUNAS REFLEXIONES SOBRE LA POSIBLE CONTRIBUCIÓN DEL DERECHO INTERNACIONAL PRIVADO EN LA LUCHA CONTRA LA VIOLACIÓN DE LOS DERECHOS FUNDAMENTALES DE GÉNERO

El uso de las nuevas tecnologías afecta a los derechos fundamentales de los individuos que realizan interacciones sociales a través de plataformas digitales que permiten el acceso a cualquier persona, mediante la creación de su propio perfil para comprar bienes, billetes de avión, de tren, escuchar música, ver películas, espectáculos teatrales, interactuar con otras personas, etc. Es en este contexto, se lleva a cabo el estudio sobre el papel del Derecho internacional privado como instrumento destinado a hacer eficaz y efectiva la protección de los derechos fundamentales, como premisa conceptual para analizar posibles puntos de contraste contra la ciberviolencia de género dentro de la esta disciplina. Este papel se aprecia en el momento en que el Derecho internacional privado busca resolver los problemas de coordinación entre sistemas jurídicos, en aspectos tradicionales de esta disciplina, es decir, la identifica-

ción del juez competente para examinar la controversia relacionada con varios Estados, la determinación de la ley aplicable, y el reconocimiento de la decisión dictada en un Estado diferente. En un ámbito donde las relaciones entre particulares no están conectadas a territorios estatales, sino a espacios digitales sobre los cuales es controvertida la pertenencia a uno u otro Estado, o bien a la Unión Europea en el caso de sus Estados miembros, las reglas del Derecho internacional privado se adaptan a nuevos criterios de localización, aplicando los métodos y criterios propios de la disciplina, de manera que aseguren la protección fundamental de los derechos en el espacio digital.

PALABRAS CLAVES: Derecho internacional privado – ciberviolencia – derechos humanos – responsabilidad civil por ciberviolencia – protección de las mujeres

CIBERVIOLENCIA CONTRA LAS MUJERES Y COOPERACIÓN JUDICIAL DIGITALIZADA EN PROCESOS DE SUSTRACCIÓN INTERNACIONAL DE MENORES

Rosario Espinosa Calabuig[*]

1. *Ciberviolencia contra las mujeres y sustracción internacional de menores: ausencia de respuestas ante una sociedad patriarcal*

La violencia contra las mujeres se aprecia lamentablemente en numerosos ámbitos de nuestra vida cotidiana y las herramientas para combatirla emergen desde frentes muy diferentes. Uno de dichos ámbitos concierne a un fenómeno tristemente muy extendido a nivel mundial, como es la sustracción internacional de menores, en particu-

[*] Catedrática de Derecho internacional privado, Universitat de València. Email: rosario.espinosa@uv.es

lar cuando es realizada por la madre que ha sido víctima de violencia machista por su pareja. Una violencia que, realizada en un entorno familiar, puede haberse ejercido por medios tecnológicos, como un simple mensaje de whatsapp o un correo electrónico, pasando a integrarse en la llamada ciberviolencia[1].

En este contexto, las herramientas a las que nos referimos se concretan, en el caso específico de la Unión europea en que se centra este capítulo, en varios instrumentos (reglamentos y directivas) elaborados por el legislador europeo en los últimos tiempos. Todos ellos aspiran, de una parte, a combatir la violencia contra las mujeres y la violencia doméstica (sería el caso de la directiva (UE) 2024/1385[2] y, de otra, a fomentar la cooperación judicial entre Estados para facilitar la solución de litigios transfronterizos, entre ellos los relativos a la sustracción de menores (sería el caso, entre otros, de los reglamentos (UE) 2020/1783 sobre notificaciones y 2020/1784 sobre obtención de pruebas[3], así como

[1] La tradición empírica sobre abuso y agresiones tecnológicas se ha desarrollado en torno a cuatro principales líneas de investigación: (a) ciberviolencia en la adolescencia (b) ciberviolencia ejercida por adultos hacia menores con una motivación sexual (c) ciberviolencia por razón de género, incluyendo también la ejercida hacia las mujeres por parte de sus compañeros sentimentales y (d) ciberviolencia producida en el seno de relaciones de pareja de menores y/o adultos, ya sea ejercida por hombres o mujeres en relaciones del mismo o de diferente sexo. C. RODRÍGUEZ-DOMÍNGUEZ, P.J. PEREZ MORENO, M. DURÁN, *Ciberviolencia en las relaciones de pareja: una revisión sobre su metodología de investigación*, en *Anales de Psicología*, 2020, vol.36, n.2, pp. 200-209. Disponible en: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0212-97282020000200002&lng=es&nrm=iso; T. DONOSO VÁZQUEZ, *Las ciberviolencias de género, nuevas manifestaciones de la violencia machista*, en T. DONOSO VÁZQUEZ, A. REBOLLO-CATALÁN, *Violencia de género en entornos virtuales*, Barcelona, 2018, pp. 15-29

[2] Directiva 2024/1385/UE del Parlamento europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica,* de 14 de mayo de 2024 en DOUE 1385 de 24 de mayo de 2024, pp. 1-36.

[3] En concreto, el reglamento 2020/1783/UE del Parlamento europeo y del Consejo, *relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil* ("obtención de pruebas") (versión refundida), de 25 de noviembre de 2020, en DOUE 405 de 2 de diciembre, pp. 1-39; y el reglamento 2020/1784/UE del Parlamento europeo y del Consejo, *relativo a la notificación y traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil* ("notificación y traslado de documen-

el reglamento (UE) 2023/2844 sobre digitalización de la cooperación judicial[4]).

Para abordar el estudio de todas estas cuestiones nos vamos a referir a uno de los casos más mediáticos de los últimos años en materia de sustracción internacional de menores cometida por una madre víctima de violencia machista y que, todavía en enero de 2025, sigue generando controversia. Hablamos del caso de *Juana Rivas v. Francesco Arcuri*, que ha puesto en juego la cooperación judicial entre dos países como España e Italia y ha tambaleado los pilares de la regulación existente en la materia. El caso conecta la violencia de género y doméstica (del Sr. Arcuri contra la madre y también contra los hijos)[5] con la sus-

tos") (versión refundida), de 25 de noviembre de 2020, en DOUE 405 de 2 de diciembre de 2020, pp. 40-78. Sobre el segundo, corr. errores en DO L 188, de 27 de julio de 2023. Junto a ellos, otros textos como el reglamento de ejecución 2022/422/UE de la Comisión, *por el que se establecen las especificaciones técnicas, las medidas y otros requisitos para la implementación del sistema informático descentralizado a que se refiere el Reglamento (UE) 2020/1783 del Parlamento Europeo y del Consejo,* de 14 de marzo de 2022, en DOUE 87 de 15 de marzo de 2022, pp. 5-8; el reglamento de ejecución 2022/423/UE de la Comisión, *por el que se establecen las especificaciones técnicas, las medidas y otros requisitos para la implementación del sistema informático descentralizado a que se refiere el Reglamento (UE) núm. 2020/1784 del Parlamento Europeo y del Consejo,* de 14 de marzo de 2022, en DOUE 87, de 15 de marzo de 2022.

[4] Reglamento (UE) 2023/2844 del Parlamento europeo y del Consejo, *sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales, y por el que se modifican determinados actos jurídicos en el ámbito de la cooperación judicial,* de 13 de diciembre de 2023, en DOUE 2844 de 27 de diciembre de 2023, pp. 1-29. Ver X. KRAMER, *op. cit.*, p. 6.

[5] En relación con los hechos delictivos cometidos en 2005 dentro de la jurisdicción española, el Sr. Arcuri fue condenado por un delito de lesiones en el ámbito familiar (art. 153.2 del código penal español) con una pena de tres meses de prisión y una orden de alejamiento respecto de la Sra. Rivas de algo más de un año (Juzgado de lo penal n. 2 de Granada, sentencia n. 242/2009, de 26 de mayo de 2009. En relación con la segunda denuncia por violencia de género presentada por la Sra. Rivas en España contra el Sr. Arcuri, por presuntos hechos cometidos entre 2013 y 2016 en Italia, el caso fue desestimado por falta de competencia penal internacional de los tribunales españoles. La Audiencia Provincial también desestimó el recurso de la Sra. Rivas el 27 de febrero de 2018 bajo el mismo razonamiento (Audiencia Provincial de Granada, sección 2ª, Auto (Decreto judicial) n. 135/2018, de 2 de febrero de 2018.

tracción de menores mediante procedimientos penales y civiles[6]. En enero de 2025 los abogados de *Juana Rivas* han vuelto a denunciar a su ex marido, el Sr. Arcuri, por supuestas amenazas realizadas a través de reiterados mensajes de texto en el móvil y llamadas telefónicas[7]. Estas

[6] El Sr. Arcuri denunció a la Sra. Rivas ante los tribunales españoles por un delito de sustracción internacional de sus hijos (art. 225 *bis* del código penal español), dado el reiterado incumplimiento de la orden de restitución por parte de la madre. La Sra. Rivas fue condenada (en primera instancia y ratificada en apelación) como autora de dos delitos de sustracción de menores. La pena impuesta fue de dos años y seis meses de prisión por cada uno de ellos, con la accesoria de privación del ejercicio de la patria potestad de sus hijos en seis años. Además, fue condenada a pagar al Sr. Arcuri una indemnización por daños y perjuicios (Audiencia Provincial de Granada, sección 1ª, sentencia n. 98/2019, de 7 de marzo de 2019). En el orden civil, mediante resolución de 14 de diciembre de 2016, el juzgado de primera instancia acordó la restitución inmediata de los menores al Estado de su residencia habitual antes de la sustracción (Italia). Se basaron en el reglamento Bruselas II *bis* con referencia al Convenio de La Haya de 1980. Una providencia de 24 de julio de 2017 acordó solicitar el auxilio de la Brigada Provincial de Policía Judicial UFAM Granada para la restitución de los menores. La ejecución del requerimiento de restitución tuvo que ser forzada a través de un procedimiento específico iniciado por el Sr. Arcuri. El recurso de apelación interpuesto por la Sra. Rivas contra la sentencia del Juzgado de Primera Instancia que acordó la restitución de los menores fue desestimado por sentencia de 21 de abril de 2017 de la Audiencia Provincial de Granada en base al art. 11 del reglamento Bruselas II bis (en relación con la excepción prevista en el art. 13 b) del Convenio de La Haya de 1980). Audiencia Provincial de Granada, sección 5ª, sentencia de 41 de abril de 2017 (Recurso n. 72/17, contra la sentencia del Juzgado de Primera Instancia n. 1442/16 de Granada). También en relación con la orden de restitución de la menor, la Sra. Rivas presentó varios recursos adicionales: dos ante el Tribunal Supremo español, que fueron desestimados por infracción de las normas procesales internas (de ahí que el Tribunal Supremo no se pronunciara sobre el fondo del asunto): Autos del Tribunal Supremo (decretos judiciales), de 17 de mayo de 2017 (Roj: ATS 4531/2017) y de 24 de mayo de 2017 (Roj: ATS 4818/2017) y recurso ante el Tribunal Constitucional, que fue igualmente desestimado por haber sido interpuesto extemporáneamente. (Providencia del Tribunal Constitucional de 16 de agosto de 2017 (n. de recurso 4151-2017 J). Disponible en: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2017_058/P%204151-2017.pdf). Ver C. OTERO GARCÍA CASTRILLON Y C. CORDERO ÁLVAREZ, *POAM Spanish national report*, 2020, pp. 13-18. Disponible en: *Best Practice Guide: Protection of Abducting Mothers in Return Proceedings: Intersection between domestic violence and parental child abduction. POAM Project*, 2020, en https://research.abdn.ac.uk/poam/resources/guide-to-good-practice/

[7] La denuncia presentada en enero de 2025 por hechos ocurridos mientras la Sra.

conductas en España podrían ser constitutivas de delitos de violencia contra la mujer según el código penal (CP), bien de amenazas (arts. 169-171.4 CP), coacciones (arts. 172.1-2 CP) u hostigamiento o acoso (art. 172 *ter* CP). Delitos todos ellos que admiten ser cometidos a través de medios tecnológicos[8].

Aunque desgraciadamente son numerosas las sustracciones internacionales cometidas anualmente (basta visitar la base de datos de la INCADAT – *International Child Abduction Data Base* – de la Conferencia de La Haya de DIPr.[9])[10], nos resulta interesante partir del caso de *Juana Rivas*. Éste resulta paradigmático en este capítulo para explorar las consecuencias de la violencia ejercida contra la mujer que decide escapar de su maltratador trasladando o reteniendo ilícitamente a sus hijos lejos del país donde todos ellos tenían su residencia habitual. Varias son las razones:

a) De un lado, el caso *Rivas* nos permite analizar el fenómeno de la violencia de género en el ámbito familiar y cómo ha afectado la tecnología en las nuevas formas de ejercer esa violencia que llevan a ha-

Rivas estaba en Granada en diciembre de 2024 pasando las navidades con su hijo pequeño, el único que queda bajo la custodia del Sr. Arcuri y que alega, como ya hizo el hermano mayor (que reside actualmente con la madre en Granada), que el padre es un maltratador. La denuncia alude a una serie de mensajes de texto reiterados en el móvil de la Sra. Rivas por parte del Sr. Arcuri con claro ánimo intimidatorio, y consistentes en amenazas veladas, además de 90 llamadas telefónicas. Al cierre de este capítulo el caso sigue suscitando controversia.

[8] Más ampliamente P. LLORIA GARCÍA, *La regulación penal en materia de violencia familiar y de género tras la reforma de 2015. Especial referencia al ámbito tecnológico*, en *Revista General de Derecho Penal*, 2019, n. 31, pp. 1 ss; F. VÁZQUEZ-PORTOMEÑE SEIJAS (Dir.), *Violencia contra la mujer. Manual de Derecho penal y procesal penal. Adaptado a la Ley 1/2015, de reforma del Código penal*, Valencia, 2016, p. 154; M.M. CUASANTE SÁNCHEZ*, Las manifestaciones de la violencia de género en redes sociales,* en *ReCrim*, 2019, p. 21 disponible en http://www.uv.es/recrim/recrim19/recrim19d01.wiki.

[9] Disponible en: http://www.incadat.com

[10] Sobre las estadísticas en este ámbito véanse las realizadas con ocasión de la 8ª Comisión Especial de la Conferencia de La Haya de Derecho internacional privado celebrada en octubre 2023, disponible en: https://www.hcch.net/es/publications-and-studies/details4/?pid=8488&dtid=57. Asimismo, N. LOWE, V. STEPHENS, *Global Report – Statistical study of applications made in 2021 under the 1980 Child Abduction Convention*, Prel. Doc. No 19A of September 2023, par. 28.

blar de la llamada ciberviolencia. De ellas nos centramos en el ciberacoso (*cyberharassment*) y el ciberacecho (*cyberstalking*).

b) De otro lado, el caso *Rivas* nos ayuda a explicar las características fundamentales de un proceso de sustracción internacional y la incidencia que puede tener sobre éste una eficiente cooperación judicial interestatal cuando dicha sustracción se ha realizado por motivos de violencia machista. Al hilo de dichas características analizaremos las repercusiones que puede tener la cooperación judicial digitalizada en este tipo de litigios.

El hecho de que la regulación actual – europea e internacional – sobre sustracción internacional de menores, se centre sólo, como ahora veremos, en el retorno inmediato del menor como forma de proteger su interés superior pasa por alto, no sólo el interés de la madre sustractora víctima de violencia, sino el del propio menor que posiblemente en estos casos esté mejor defendido fuera del país de su antigua residencia habitual donde aún reside el maltratador.

En la práctica, formas de violencia digital como el ciberacoso y el ciberacecho, pueden ser hoy habituales para cometer violencia en el ámbito familiar, incluido aquélla en que uno/a de los miembros de la familia comete una sustracción ilícita internacional. Sin embargo, no es fácil aún conectar la ciberviolencia contra las mujeres con los casos específicos de sustracción ilícita cometida por una madre víctima de este tipo de violencia[11]. La visita de bases como la mencionada INCADAT,

[11] El acoso hacia la mujer se demuestra en casos de separaciones y divorcios, pero no trasciende en casos de sustracción internacional. El acoso se ha visto en casos célebres como *González Carreño c. España* en que se demandó a España por su responsabilidad en relación con la violencia de género. Durante el proceso de separación, el acoso y la intimidación persistieron y, a pesar de las múltiples denuncias (47 en total), el agresor – ex marido de Ángela González Carreño – solo fue condenado una vez por una falta de vejaciones. Se acusó a España de que sus autoridades, al establecer un régimen de visitas no vigilado, "aplicaron nociones estereotipadas y, por tanto, discriminatorias en un contexto de violencia doméstica". Prevaleció el interés por no perjudicar las relaciones entre el padre y la hija, sin prestar atención al alto riesgo que existía para la menor. El caso supone un antes y un después en la responsabilidad del Estado ante la violencia de género, con la Sentencia del Tribunal Supremo español de 17 julio 2018 (Sala de lo Contencioso-Administrativo, Sección 4ª, sentencia n. 1263/2018 de 17 de julio de 2018), basándose en el Dictamen de julio de 2014 del Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW) (Naciones Unidas. Co-

entre otras, nos permite apreciar como la jurisprudencia comparada constata que en muchos casos la violencia contra la madre es minimizada o pasada por alto"[12], pues lo prioritario es el retorno inmediato del menor que se entiende salvaguardado con la adopción de medidas de protección en el Estado de residencia habitual del – supuesto – maltratador[13]. Pero, además, demuestra que, hoy por hoy, las palabras *cyber* o digital no están entre los buscadores de los casos de sustrac-

mité para la Eliminación de la Discriminación contra la Mujer. Comunicación n. 47/2012 de 16 de julio: *González Carreño c. España*). Ver A.M. GARCÍA ORTIZ, *La responsabilidad del Estado en materia de violencia de género,* en *ReCrim,* 2019, p. 24, disponible en: http://www.uv.es/recrim/recrim19/recrim19d01.wiki.

[12] Minimización de la violencia que se produce en tantos ámbitos. Ver A. DEL PRETE, S. REDÓN PANTOJA, *La invisibilización de la violencia de género en las redes sociales,* en *Multidisciplinary Journal of Gender Studies*, 2022, n. 11(2), pp. 124-143.

[13] Baste poner ejemplos como SAP Alicante (sección 6ª), 7 septiembre 2022, SAP A 1220/2022 – ECLI:ES:APA:2022:1220- sobre el retorno de unas menores de España a Polonia a pesar de la violencia contra la madre y procesos penales abiertos ante Tribunales polacos contra el padre. Así como casos recogidos en *Incadat*, por ejemplo, Family Court of Western Australia, sentencia de 12 de junio de 1998, *Falconer v. SO,* n. HC/E/AU 227, sobre el traslado desde Nueva Zelanda a Australia, en que los incidentes de violencia contra la madre presenciados por los hijos y admitidos por el padre no fueron suficientes para entender que el regreso les expondría al riesgo en el sentido del art. 13.1.b), además de falta de prueba suficiente de ésta y del abuso a los menores. Igualmente, el Tribunal de la Haya, sentencia de 22 de febrero de 2018, *X. (the mother) v. Y (the father),* n. HC/E/NL 1391, Estado requirente: Australia/Estado requerido: Países Bajos. Se ordena la restitución a Australia desde Países Bajos de una niña (nacida en Alemania) sustraída por su madre (origen Guatemala/Alemania) a su padre (origen australiano). La madre alega que con frecuencia fue víctima de violencia doméstica en presencia de su hija. Si la niña volviera a Australia, esto la colocaría en una situación intolerable, conforme 13(1)(b) del Convenio. El Tribunal consideró que la madre no pudo corroborar sus argumentos de forma adecuada. Las fotografías que presentó la madre no servían como pruebas, ya que no estaba claro cuándo se tomaron, ni podía determinarse cuál fue la causa de las lesiones. De modo sorprendente, a modo de *obiter dictum*, el Tribunal consideró que, aún si la violencia alegada por la madre se hubiese probado, no sería suficiente para afirmar que la restitución de la menor la expondría a daños físicos o psicológicos o la colocaría en una situación intolerable. Además, el Tribunal consideró que, "tal como se hizo evidente en los argumentos y pruebas que presentó la madre, en Australia hay instituciones y centros de protección contra la violencia doméstica". Afirmación, esta última, que lleva a minimizar nuevamente la relevancia de la violencia machista sobre la madre sustractora (http://www.incadat.com).

ción. Confiemos en que ello no se añada a la falta de sensibilidad constante de muchas instituciones y operadores jurídicos en la evaluación de la violencia de género en casos de sustracción internacional. La misma Conferencia de La Haya derecho internacional privado, que tan excelente labor lleva realizando desde hace años, no está otorgando a este tema la relevancia que se merece, a pesar de sus intentos.

Las dificultades en localizar casos de ciberviolencia contra una madre que ha sustraído ilícitamente a sus hijos como forma de escapar de dicha violencia o de un maltrato físico, se unen a las dificultades en definir qué actos pueden ser calificados como ciberviolencia y cuáles de éstos encajarían mejor en los casos de violencia realizada en el entorno de una sustracción internacional[14]. La directiva (UE) 2024/1385 enfatiza la necesidad de "establecer definiciones armonizadas de los delitos y las sanciones relacionados con determinadas formas de ciberviolencia en las que la violencia está intrínsecamente vinculada al uso de las Tecnologías de la Información y de las Comunicaciones (TIC) y esas tecnologías se usan para amplificar significativamente la gravedad de los efectos perjudiciales del delito, cambiando así las características de este" [15], pero no siempre será sencillo.

A este respecto, la directiva (UE) 2024/1385 se centra en establecer solamente normas mínimas para las formas más graves de ciberviolencia, de ahí que los delitos que se contemplan en ella se limiten a las conductas que puedan "causar daños graves o daños psicológicos graves a la víctima, o a las conductas que es probable que provoquen en la víctima un profundo temor por su propia seguridad o por la seguridad

[14] El reconocimiento de violencia ejercida mediante mensajes de texto mandados a la madre sustractora y calificados como *harassment* durante la causa se observa en el asunto *AD v. SD* (Extra Division, Inner House, Court of Session, Tribunal, sentencia de 17 de marzo de 2023, *AD v. SD,* n. HC/E/UKs 1556), resuelto por los tribunales escoceses -última instancia-, el 17.3.2023, en que se deniega en apelación la restitución desde EEUU a Escocia. El motivo fue haber identificado el riesgo grave hacia los dos menores en el sentido del art. 13.1.b) por las alegaciones de que *physical injury and sexual assault were corroborated by a large volumen of tex messages* y por entender que el padre era incapaz de cumplir las medidas de protección ordenadas por los tribunales de Illinois para proteger a los menores del mencionado riesgo grave, disponible en: http://www.incadat.com.

[15] Considerando 17 directiva (UE) 2024/1385, cit. p. 1 ss.

de personas a cargo", como pueden ser la madre sustractora o los hijos de ésta que han sido sustraídos ilícitamente de un país a otro. Es relevante tener en cuenta las circunstancias concretas del caso cuando se entre a valorar la probabilidad de que la conducta realizada cause daños graves. Dicha probabilidad podrá deducirse de "circunstancias fácticas objetivas"[16], cuya prueba no será fácil.

El ciberacoso – y en general la ciberviolencia –, pueden entenderse como una contradicción entre la idea social de Internet y las prácticas digitales de dominación, coerción o amenazas que definen este comportamiento pernicioso. Se trata de una forma de desigualdad digital en la medida en que unos sujetos, con más poder en otros ámbitos, limitan las posibilidades de otras personas para disfrutar de Internet con libertad y autonomía, tal como se expone en un Informe realizado por la Delegación de gobierno del Ministerio de Igualdad en relación con el ciberacoso. Esta desigualdad, prosigue el Informe, "tiene un efecto medible no sólo en las prácticas digitales, sino también y de forma muy importante, en muchas de las prácticas sociales y personales de las víctimas"[17]. El delito de acoso por mensajería o por WhatsApp se dará cuando las comunicaciones sean constantes y reiteradas en el tiempo, en un modo que alteren la vida de la víctima de modo negativo, al no ser ni deseados ni consentidos[18].

[16] Considerando 18 directiva (UE) 2024/1385, cit. p. 1 ss.

[17] Informe realizado por C. TORRES ALBERO, J.M. ROBLES, S. DE MARCO, *El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento, Delegación del Gobierno para la Violencia de Género, Ministerio de Sanidad, servicios sociales e igualdad*, Centro de publicaciones, Madrid, 2014, pp. 29-30.

[18] La Agencia de los Derechos Fundamentales de la Unión europea publicó en 2019 la macroencuesta *Violencia de género contra las mujeres: una encuesta a escala de la UE. Resumen de Conclusiones*. Luxemburgo, Oficina de Publicaciones de la Unión Europea. Disponible en: http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance_es_0.pdf De los datos a nivel mundial sobre violencia de género se desprendía que de los 186 millones de europeas el 11% de las mujeres habían sufrido acoso cibernético a través de la red, del email o del teléfono. Ver M.A. VERDEJO ESPINOSA, *Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención*, Sevilla, Universidad Internacional de Andalucía, 2015, p. 135.

El ciberacoso, en particular, es vivido con miedo en la medida en que las prácticas se asemejan al acoso físico, es decir, cuando se plantea la posibilidad de que el acosador pueda tener contacto físico con la víctima. El ciberacoso como forma de violencia de género implica agresión psicológica, sostenida y repetida en el tiempo, contra su pareja o expareja, utilizando para ello las nuevas tecnologías a través de plataformas o sistemas virtuales como el correo electrónico, sistemas de mensajería, WhatsApp, redes sociales, blogs o foros siendo su objetivo la dominación, la discriminación, el abuso de la posición de poder y debe suponer una intromisión, sin consentimiento, en la vida privada de la víctima[19].

Junto al ciberacoso (art. 7) que pueda realizarse contra una mujer que, en los casos que aquí interesan, haya sustraído ilícitamente a sus hijos, pueden darse supuestos de ciberacecho hacia ella (art. 6). En concreto, la directiva (UE) 2024/1385 define el ciberacecho como "una forma moderna de violencia que a menudo se comete contra familiares o personas que viven en el mismo hogar que el autor, aunque también lo cometen exparejas o conocidos. Normalmente, el autor hace un uso indebido de la tecnología para intensificar un comportamiento coactivo y controlador, la manipulación y la vigilancia, incrementando con ello el miedo y la ansiedad de la víctima y su aislamiento gradual de amigos y familiares y del trabajo. Por lo tanto, deben establecerse normas mínimas sobre el ciberacecho"[20]. No obstante, la diferencia entre ambos delitos no siempre estará clara en la práctica.

El concepto de *cyberstalking* (ciberacecho) es una combinación de las palabras inglesas *cyber* y *stalking* que pueden traducirse como "ciber-acecho" o "ciber-persecución". Este tipo de actividad utiliza la tecnología para acechar o acosar a una persona o a un grupo de personas e incluiría falsas acusaciones, vigilancia, amenazas, robo de identidad, daños al equipo de la víctima o a la información que en él contiene, uso de la información robada para acosar a la víctima, mensajes

[19] M.A. VERDEJO ESPINOSA, *Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención*, Sevilla, Universidad Internacional de Andalucía, 2015, p. 135, pp. 148-150. Ver asimismo http://www.abogacia.es/2014/11/26/la-denominada-violencia-cibernética-Internet-y-las-redes-sociales/

[20] Considerando 21 directiva 2024/1385/UE, *cit.* p. 1 ss. en relación con el art. 6.

acusatorios o vejatorios, etc.[21]. Ahora bien, su encuadre en uno u otro delito en el derecho español no ha estado exento de discusión[22].

Para la directiva (UE) 2024/1385, se trata de un delito que comprende la "vigilancia reiterada y continua de la víctima sin su consentimiento o sin autorización legal mediante TIC" así como el "seguimiento de las víctimas, sin su consentimiento o autorización, utilizando dispositivos tecnológicos conectados a través de la internet de las cosas, como los electrodomésticos inteligentes. Sin embargo, pueden darse situaciones en las que la vigilancia se realice por motivos legítimos, por ejemplo, en el contexto del seguimiento del paradero y la actividad en línea de los hijos por parte de sus progenitores[23]. Argumento que podría ser utilizado por el Sr. Arcuri en el Caso *Rivas* a su favor para justificar su comportamiento reiterativo y amenazante.

En este sentido, la directiva (UE) 2024/1385 reitera la necesidad de establecer normas mínimas sobre todos estos delitos, insistiendo en la necesidad de que, en concreto el ciberacoso, pueda cubrir las formas más graves del delito. Esto es, debe incluir "la participación reiterada o continua en conductas amenazantes dirigidas contra otra persona, al menos cuando esa conducta implique amenazas, mediante

[21] Informe realizado por C. TORRES ALBERO, J.M. ROBLES, S. DE MARCO, *op. cit*., p. 30.

[22] Tal como se puso de manifiesto por la Audiencia Provincial de Sevilla, en la sentencia n. 328/2009, de 8 de junio (fundamento Jurídico 2), "conductas tales como la realización de llamadas telefónicas repetidas al sujeto pasivo, el envío masivo de mensajes telefónicos de texto, los seguimientos o acechos en la vía pública y otros actos de similares características, que se engloban genéricamente en el término anglosajón "stalking" no pueden subsumirse en el delito de coacciones". De un lado, faltaría el elemento esencial de la violencia física, propio de estas figuras y, de otro, tampoco se obliga a la víctima a atender las llamadas o recibir los mensajes, de ahí que solo podrían incluirse en el ámbito de tutela de las violencias psíquicas habituales, siempre que lo permitiera el principio acusatorio, lo que no era el caso, según señala P. LLORIA GARCÍA, *op. cit*., p. 23 Para un análisis del ciberacecho/ciber*stalking* en el derecho español ver, entre otros, C. VILLACAMPA ESTIARTE, *La incriminación del acoso (predatorio) en la reforma penal de 2015*, en M.L. CUERDA ARNAU (dir.), *Menores y redes sociales*, Valencia, 2016, pp. 403 y ss; A. ALONSO DE ESCAMILLA, *El delito de stalking como nueva forma de acoso: cyberstalking y nuevas realidades*", en *La Ley penal: revista de derecho penal, procesal y penitenciario*, 2013, n. 105; A. MATALLÍN EVANGELIO, *Nuevas formas de acoso: stalking/cyberstalking-acoso/ciberacoso*, en M.L. CUERDA ARNAU (dir.), *op. cit*., pp. 332-337.

[23] Considerando 21 directiva 2024/1385/UE, cit., p. 1 ss.

TIC, de cometer delitos y sea probable que cause en la persona un profundo temor por su propia seguridad o por la seguridad de las personas a cargo" [24]. Dicho temor se ha evidenciado reiteradamente en la persona de *Juana Rivas* y sus hijos y puede ser uno de los argumentos de su defensa para que el hijo menor de la pareja no regrese a Italia, país en que la familia residía habitualmente en la época en que se realizó la sustracción ilícita por la madre.

2. *Sustracción de menores por madres víctimas de violencia: limitaciones*

Sin ánimo de extendernos en estos momentos, baste recordar que un traslado o retención de un menor se califica como ilícito cuando: a) Se ha producido con infracción de un derecho de custodia atribuido conforme al derecho del Estado en que el menor tenía su residencia habitual inmediatamente antes de su traslado o retención; y además, b) En el momento del traslado o de la retención, el derecho de custodia se ejercía de forma efectiva, separada o conjuntamente, o se habría ejercido de no haberse producido dicho traslado o retención.

Esta definición se desprende de los principales textos reguladores de la sustracción internacional de menores como son el Convenio de la Haya de 1980 sobre sustracción internacional de menores[25], en el art. 3, y el reglamento (UE) 2019/1111 (Bruselas II ter)[26] en el art. 2.11 que ha sustituido en agosto de 2022 al reglamento (UE) 2201/2003 (Bruselas II bis)[27].

[24] Considerando 24 directiva 2024/1385/UE, cit., p. 1 ss.

[25] Convenio de La Haya, *sobre aspectos civiles del secuestro internacional de menores,* de 25 de octubre de 1980, en BOE 202 de 24 de agosto de 1987, pp. 26099-26105. corr. errores en BOE 86 de 11 de abril de 1989, pp. 10385-10385; y BOE 21 de 24 de enero de 1996, pp. 2144-2144.

[26] Reglamento UE 2019/1111 del Consejo, *relativo a la competencia, el reconocimiento y la ejecución de resoluciones en materia matrimonial y de responsabilidad parental, y sobre la sustracción internacional de menores* (versión refundida), de 25 de junio de 2019, en DOUE L 178/1 de 2 de julio de 2019.

[27] Reglamento (CE) 2201/2003 del Consejo, *relativo a la competencia, el reconocimiento y la ejecución de resoluciones judiciales en materia matrimonial y de responsabilidad parental por el que se deroga el Reglamento CE nº 1347/2000,* de 27 de noviembre de 2003, en DOUE 338 de 23 de diciembre de 2003, pp. 1-29. La bibliografía es

Junto a tales normas de origen UE y convencional, en España conviven otras normas de fuente interna como son la Ley 15/2015, de la jurisdicción voluntaria que introdujo en la LEC un cap. IV bis sobre "Medidas relativas a la restitución o retorno de menores en los supuestos de sustracción internacional" (art. 778, quáter, quinquies y sexties)[28], además de la normativa en materia penal como, por ejemplo, el art. 544 LECr. y otras como la LO 1/1996 de protección del menor, según redacción dada por la LO 8/2015 de 22 de julio (art. 2.5.b)[29] o la ley 26/2015, de 28 de julio[30]. El último exponente de todas estas

muy extensa, entre otros, E. RODRÍGUEZ PINEAU, *El nuevo Reglamento (UE) 2019/1111 en materia matrimonial, responsabilidad parental y sustracción internacional de menores, LA LEY Derecho de familia*, 2020, n. 26, p. 1; B. CAMPUZANO DÍAZ, *El nuevo Reglamento (UE) 2019/1111: análisis de las mejoras en las relaciones con el Convenio de La Haya de 19 de octubre de 1996 sobre responsabilidad parental*, *Cuadernos de Derecho Transnacional*, v. 12, n. 2, p. 109; C. AZCÁRRAGA MONZONÍS, P. QUINZÁ REDONDO, *Sustracción internacional de menores y Convenio de la Haya de 1980. Comentario de la sentencia de la Audiencia Provincial de Las Palmas (Sección 3), n. 377/2017, de 29 de junio*, *Cuadernos de Derecho Transnacional,* 2018, n. 10, pp. 795-801; M. GONZÁLEZ MARIMÓN, *La sustracción internacional de menores en el espacio jurídico europeo*, Valencia, 2023; A.J. CALZADO LLAMAS, *La sustracción internacional de menores en el Reglamento 2019/1111 y su interacción con el Convenio de La Haya de 1980 y la LEC*, Madrid, 2023; M. HERRANZ BALLESTEROS, *El retorno seguro del menor ¿puente entre la excepción de grave riesgo y la obligación de devolución?, Bitácora Millennium DIPr: Derecho Internacional Privado*, 2024, n. 18, pp. 1-42; M. CELIS AGUILAR, *Sustracción internacional de menores. Estudio jurisprudencial, doctrinal y crítico del Convenio de La Haya de 1980. Aspectos clave y solución de problemas*, Madrid, 2023; M.A. RODRÍGUEZ VÁZQUEZ, *Supresión de exequatur y ejecución de resoluciones en materia de responsabilidad parental: la conveniencia de dos soluciones en el Reglamento 2019/1111, Revista Española de Derecho Internacional*, 2022, Vol. 74/2, pp. 349-383.

[28] Al respecto ver los comentarios que hice en su momento en R. ESPINOSA CALABUIG, *Traslado o retención ilícitos de menores tras la reforma de 2015: rapidez, especialización y… algunas ausencias*, en *Revista Española de Derecho Internacional*, 2016, vol. 68, n. 2, pp. 347-357; así como *Combatiendo la violencia contra la mujer en casos de sustracción internacional de menores: el ODS n. 1 5.2.*, en S. BORRÁS PENTINAT, M. FONT MAS, A. GONZÁLEZ BONDÍA, D. MARÍN CONSARNAU, A. PIGRAU SOLER (Dirs), *La comunidad internacional ante el desafío de los Objetivos de Desarrollo Sostenible*, Valencia, 2022, p. 507-527.

[29] Ley Orgánica 8/2015, *de modificación del sistema de protección a la infancia y a la adolescencia*, de 22 de julio, en BOE 175, de 23 de julio de 2015, pp. 61871-61889.

[30] Ley 26/2015, *de modificación del sistema de protección a la infancia y a la ado-*

normas fue la LO 8/2021, de 4 de junio, de protección integral de la infancia y la adolescencia frente a la violencia, con repercusiones relevantes en el ámbito de la violencia contra la mujer[31].

Mucho se ha escrito y dicho ya sobre la sustracción de menores motivada por la violencia ejercida contra la mujer, pero no parece que haya habido mucho avance real y efectivo. Por eso, si queremos un progreso en este ámbito, con una herramienta muy específica como es el DIPr., necesitamos un cambio de mentalidad y de actitud, así como un enfoque de género en la aplicación e interpertación de muchas de sus reglas. Dicho cambio no acaba de verse, lamentablemente, si echamos un vistazo a la jurisprudencia comparada como la que aparece en la ya mencionada base de datos de INCADAT de la Conferencia de La Haya de DIPr., sobre los casos de sustracción internacional de menores de los últimos 25 años[32].

Sorprende, en este sentido, como ya hemos denunciado en otras ocasiones[33], que todas las propuestas que se habían lanzado en 2017 en materia de violencia de género en el *Proyecto de Buenas Prácticas* sobre la aplicación del art. 13.1.b. del Convenio de La Haya de 1980[34] (muy completo), por parte de la Conferencia de la Haya de DIPr. no se hayan reflejado finalmente en la *Guía de Buenas Prácticas* publicada en 2021[35].

lescencia, de 28 de julio, en BOE 180, de 29 de julio de 2015.

[31] Ley Orgánica 8/2021, *de protección integral a la infancia y la adolescencia frente a la violencia*, de 4 de junio, en BOE 134 de 5 de junio de 2021.

[32] Disponible en: http://www.incadat.com En concreto hemos analizado los casos desde 1999 a 2024.

[33] Por ejemplo, en R. ESPINOSA CALABUIG, *Sorority, equality and European private international Law,* en *Freedom, Security and Justice: European Legal Studies,* 2023, n. 1, pp. 113-131.

[34] Ver ampliamente *Proyecto de Guía de Buenas Prácticas sobre el Artículo 13(1)(b) del Convenio de La Haya de 25 de octubre de 1980 sobre los Aspectos Civiles de la Sustracción Internacional de Menores*, HCCH, Oficina Permanente, Doc. Prel. n. 3 de junio de 2017, Anexo 2, pp. 1-97.

[35] *Guía de Buenas Prácticas en virtud del Convenio de 25 de octubre de 1980 sobre los Aspectos Civiles de la Sustracción Internacional de Menores Parte VI Artículo 13(1)(b),* Conferencia de La Haya de Derecho Internacional Privado - HCCH Oficina Permanente, 2021, pp. 1-81. La *Guía de Buenas Prácticas* resulta muy limitada, en comparación con el Proyecto presentado en 2017. En la Guía se alude de forma gené-

Confiemos en que la nueva directiva (UE) 2024/1385, así como los mecanismos de digitalización de la cooperación judicial entre los EE.MM., con los reglamentos antes citados y otros más a los que luego me referiré, permitan progresar, cuanto menos, en la toma en consideración de la mujer víctima de violencia en una situación tan concreta y recurrentemente olvidada como es la de la sustracción de menores.

2.1. *Falta de sensibilidad continuada en el derecho internacional privado: Convenio de La Haya 1980 y reglamento (UE) 2019/1111*

Partiendo de lo recién expuesto, no podemos olvidar que cuestiones como la misoginia o el machismo son también cuestiones del DIPr., en particular cuando el feminismo y la igualdad de derechos chocan con legislaciones que discriminan por razones de sexo[36]. También cuando las mismas autoridades al aplicar la ley lo hacen bajo consideraciones o concepciones arraigadas y estereotipadas que en nada benefician a la mujer. Durante tiempo la jurisprudencia comparada viene demostrando actitudes judiciales que pasan por alto o minimizan el problema de la violencia – física o psíquica – contra la mujer, madre sustractora[37]. Esta minimización constante de la violencia machista en

rica a la violencia doméstica "contra el niño y/o el padre o la madre sustractor" para valorar el grave riesgo del art. 13.1.b). No se otorga, ni en este apartado ni en toda la Guía, mayor relevancia específica a la violencia contra la mujer más allá de lo mencionado, si bien la gran mayoría de jurisprudencia que se aporta es sobre casos de violencia sufrida por la madre sustractora (sólo una sentencia se aporta en relación con el padre sustractor que alega violencia contra el menor, cometida por la pareja de la madre), además de la sufrida –directa o indirectamente- por el menor.

[36] K. KNOP, R. MICHELS, A. RILES, *From Multiculturalism to Technique: Feminism, Multiculturalism, and the Conflict of Laws Style*, en *Stanford Law Review*, 2012, n. 64, p. 589.

[37] Muy ilustrativa es la jurisprudencia comparada recogida y comentada en su momento por autoras como M. KAYE, *The Hague Convention and the Flight from Domestic Violence: How Women and Children are being returned by Coach and Four*, *International Journal of Law, Policy and the Family*, 1999, pp. 191-212, en relación con sentencias del ámbito anglosajón, así como M. REQUEJO ISIDRO, *Secuestro de menores y violencia de género en la Unión Europea, Anaurio Español de Derecho Internacioanl Privado.*, t. VI, 2006, pp. 179-194. Mucha de la cual se encuentra disponible en INCADAT (http://www.incadat.com).

el contexto de la sustracción de menores no parece que vaya a mejorar cuando esta violencia se ejerza por medios digitales, bien en forma de ciber acoso o ciber acecho, por poner un ejemplo, como se anunciaba al inicio del trabajo.

Es cierto que ha habido mejoras considerables en favor de la igualdad de derechos, pero aún quedan reminiscencias del pasado y a su desarrollo tampoco han ayudado las dificultades prácticas inherentes al DIPr. En el caso concreto de la sustracción internacional de menores, además de las diferencias entre los derechos procedimentales de los Estados miembros, que luego analizamos, emergen limitaciones que derivan de su propia regulación. Entre ellas:

a) A nivel internacional, nos encontramos con que el Convenio de La Haya de 1980 es insuficiente, ya que el art. 13.1.b. – que excepciona el retorno del menor en caso demostrado de "riesgo grave" sobre su persona[38] – no contempla los riesgos derivados de una situación de violencia contra su madre u otro familiar.

Aunque se ha reivindicado por algunas delegaciones en la Conferencia de la Haya la inclusión de la violencia de género en dicha excepción (por entender que, aunque el menor no sufra daño físico o psicológico, puede quedar expuesto a una situación intolerable), lo cierto es que siempre ha quedado en saco roto[39]. Al final, lo que se deduce del fracaso de reivindicaciones como la señalada o de que el *Proyecto de Guía de Buenas Prácticas* de 2017 no saliera adelante, es la falta de una sensibilidad continuada en la interpretación de la normativa reguladora de este sector por parte de muchos operadores jurídicos. A esta limitación legislativa a nivel internacional, se añade:

b) A nivel europeo, las repercusiones que ha tenido la puesta en práctica de una regla como la eliminación del exequátur en relación con decisiones como el retorno del menor tras un traslado ilícito (cometido, quizás, por causa de violencia de género, demostrada o no) que dicta el tribunal del Estado miembro de la residencia habitual del menor anterior a su sustracción y que prevalece sobre otra decisión an-

[38] La conocida como *excepción de grave riesgo* se refiere al *peligro físico o psíquico o que de cualquier otra manera ponga al menor en una situación intolerable*.

[39] Así ocurrió en la *14ª Sesión de la Conferencia, tomo III, Sustracción de Menores*, p. 302.

terior que se haya podido dictar en el Estado miembro en que el menor está retenido y que ordena su no retorno[40].

La aplicación muchas veces inflexible de dicha regla por parte del TJUE, tiene su base en que el interés superior del menor se satisface necesariamente con su retorno inmediato, en cuanto objetivo principal del reglamento Bruselas II ter y del Convenio de La Haya 1980[41]. Ello ha llevado a soslayar en ocasiones la valoración de aquello que realmente puede respetar mejor dicho interés superior, valorándolo en cada caso concreto, y que puede no ser su retorno al país en que tenía su residencia habitual[42]. Una valoración que parece más flexible por parte del TEDH y que el nuevo reglamento Bruselas II ter habría querido

[40] Para un análisis de dicha regla ver la bibliografía citada en nota n.27.

[41] Ampliamente R. ESPINOSA CALABUIG, L. CARBALLO PIÑEIRO, *Child protection in European Family Law*, en T. PFEIFFER, Q.C. LOBACH, T. RAPP (eds.), *Facilitating Cross-Border Family Life – Towards a Common European Understanding. EUFams II and Beyond*, Heidelberg, 2021, pp. 65-67 (https://doi.org/10.17885/heiup.853.c11710).

[42] Decisión seguida en España de modo igualmente inflexible como demuestra, por ejemplo, la citada SAP Alicante (sección 6ª), 7 septiembre 2022, SAP A 1220/2022 sobre la retención ilícita de unas menores por su madre en España (desde Polonia), que alega una interpretación errónea del art. 13.1.b) Convenio de La Haya e infracción art. 3.1 de la Convención Derechos del Niño 20.11.1980 "al no haberse tenido en cuenta el grave riesgo que corren las menores con el retorno: 1º al existir un procedimiento penal abierto contra el padre por existir indicios de delitos de violencia doméstica y sexual; 2º por existir una prohibición total de contactos por Auto del Tribunal de Apelación de Cracovia de 9 de abril de 2019; 3º por la situación de riesgo sufrida por la apelante con anterioridad a su llegada a España, lo que ha supuesto graves daños psicológicos para las menores". Para la apelante son insuficientes las prevenciones realizadas por los órganos judiciales polacos para garantizar la integridad física o psíquica de las menores o la previsible adopción de medidas de protección. Sorprende la respuesta de la AP al reconocer que, "aun siendo cierto que se sigue procedimiento penal contra el solicitante en el país de origen por un posible delito de abusos sexuales cometidos presuntamente contra la menor María Purificación , y uno o varios delitos de violencia o malos tratos en el ámbito familiar en 2018; entendemos que en el presente caso resulta de aplicación el art. 11.4º del reglamento 2201/2003/CE, cit.: Los órganos jurisdiccionales no podrán denegar la restitución de un menor basándose en lo dispuesto en la letra b) del artículo 13 del CLH si se demuestra que se han adoptado medidas adecuadas para garantizar la protección del menor tras su restitución".

recoger. El debate jurisprudencial es de sobra conocido con asuntos como *Sofia Povse*[43]o *Aguirre Zagarra*[44],entre otros[45].

Los reglamentos, tanto Bruselas II bis como ahora Bruselas II ter, aunque basan muchas de sus reglas en las del Convenio de La Haya de 1980, pueden incluso resultar más limitados al no contemplar posibilidades como la del art. 20 del Convenio. Aunque la utilidad del precepto despierta algunas dudas[46], puede que en la práctica permita englobar la violencia de género y excepcionar el no regreso del menor, cuando entran en conflicto los principios fundamentales del Estado requerido en materia de protección de los derechos humanos y de las libertades fundamentales. Esto es, que si la madre vuelve pueden verse vulnerados derechos humanos fundamentales, desde el derecho a la tutela judicial efectiva a la vulneración del art. 8 del Convenio Europeo de Derechos Humanos (CEDH)[47].

Dadas las limitaciones del reglamento Bruselas II ter en relación con la madre sustractora víctima de violencia machista, debe reivindicarse la aplicación de una perspectiva de género a sus reglas, en concreto a los foros de competencia judicial en él previstos tanto para la responsabilidad parental, como para los foros de la sustracción. Ello podría procurar la búsqueda del foro más apropiado para el interés del menor y, por ende, de la madre, en situaciones de violencia de género o doméstica. Se trataría en ese caso de realizar ciertas correcciones al

[43] Tribunal europeo de derechos humanos, sentencia de 18 de junio de 2013, demanda no. 3890/11, *Sofia Povse and Doris Povse c./ Austria*, disponible en: http://hudoc.echr.coe.int/eng?i=001-122449. Anteriormente el TJUE había resuelto con sentencia de 1 de julio de 2010, en el Asunto C-211/10 PPU, *Povse*.

[44] Tribunal justicia de la Unión europea, sentencia de 22 de diciembre de 2010, en el asunto C-491/10 PPU, *Aguirre Zárraga*.

[45] Ver M. GONZÁLEZ MARIMÓN, *El principio del interés superior del menor en supuestos de sustracción ilícita internacional: la jurisprudencia del TJUE y del TEDH*, en M.C. GARCÍA GARNICA, N. MARCHAL ESCALONA, *Aproximación interdisciplinar a los retos actuales de protección de la infancia dentro y fuera de la familia*, Madrid, 2019, p. 637.

[46] Sobre las dudas que despierta el art. 20 para utilizarlo en el ámbito de la violencia de género ver M. REQUEJO ISIDRO, *op.cit.,* pp. 190-191.

[47] D. COESTER-WALTJEN, *The future of The Hague Child Abduction Convention: the rise of domestic and international tensions, the European perspective, New York Journal of International Law and Politics*, 2000, n. 1, pp. 66-68.

reglamento 2019/1111 mediante una lectura, interpretación y aplicación de sus reglas con perspectiva de género, y poder así otorgar respuestas, no sólo más adaptadas a cada caso concreto, sino que afronten de modo más justo la violencia sobre la mujer y el impacto sobre sus hijos/as" [48]. Hoy por hoy dicha perspectiva es una utopía, a la vista de las decisiones mayoritarias judiciales que, como hemos señalado, suelen minimizar la violencia contra la mujer en litigios de sustracción.

2.2. Incidencia específica de la violencia machista sobre la sustracción de menores

Es posible señalar una serie de características habituales de la violencia de género que tiene unas repercusiones específicas en el ámbito de la sustracción internacional de menores.

De una parte, con carácter general, la violencia de género se caracteriza principalmente por[49]: a) La presencia de un componente estructural, al ser ejercida bajo la construcción de los roles de género y estereotipos sexuales, que se convierten en factores de riesgo. b) El objetivo de la violencia es el control, no es el daño, sino el control y sometimiento de la mujer a esos dictados de género. c) En la estrategia de control el agresor quiere aislar a la mujer de sus fuentes de apoyo para conseguir impunidad. La interacción de estos tres elementos contribuye, en la realidad, a la invisibilidad de la mayoría de casos y a la justificación de la violencia de género más de lo deseado, a pesar de los más de 600.000 casos anuales y 60 homicidios de media[50].

[48] En línea con lo defendido por otras autoras, en relación con las reglas sobre responsabilidad parental de Bruselas II ter, como C. RUIS SUTIL, *Custodia/visita, violencia contra las mujeres y salvaguardia del interés superior de los niños y niñas en situaciones privadas internacionales*, en P. JIMÉNEZ BLANCO E I. RODRÍGUEZ-URÍA SUÁREZ (dirs.), *Obstáculos de género a la movilidad tranfronteriza de personas y familas*, Madrid, 2024, p. 420.

[49] E. MARTÍNEZ GARCÍA, *Violencia de género en tiempos de distopía pandémica, V Feminario, Retos feministas tras una pandemia*, Diputación de Valencia, 2021, disponible en: http://www.feminariovalencia.es/

[50] Ver https://www.unwomen.org/es/what-we-do/ending-violence-against-women/facts-and-figures). Para un análisis pormenorizado por países: https://evaw-global-database.unwomen.org/en/countries

De otra parte, con carácter específico, la violencia de género circunscrita en el ámbito del traslado o retención ilícitos de menores, se manifiesta de modos diversos. En principio, suele referirse a alegaciones de violencia doméstica/familiar o maltrato infantil por las que el/la menor puede verse expuesto a un riesgo grave tras la restitución. Son los casos en que hay: a) Un comportamiento violento o inapropiado contra el/la menor tras la restitución, o b) Una exposición del menor a violencia doméstica entre sus padres tras la restitución, o c) Un daño causado a la madre sustractora a manos del padre privado del/la menor tras la restitución, d) La violencia de género puede afectar también a la incapacidad de regresar del progenitor sustractor en la medida en que podría expondría al menor a un riesgo grave derivado, por ejemplo, de una posible acción penal o de otra índole en el Estado de la residencia habitual anterior a la sustracción por el acto ilícito cometido; u otras causas relativas, por ejemplo, a la salud del/la menor o a la situación económica de la sustractora tras la restitución[51].

Ambas manifestaciones, general y específica, de la violencia contra la mujer adquiere matices relevantes cuando la violencia es realizada de forma digital, que afectan a cuestiones clásicas en este ámbito como la prueba de la violencia o la misma calificación del delito. Algunas de ellas las vemos a continuación.

[51] Ver con detalle *Proyecto de Buenas prácticas…, op. cit*., pp. 74-79. Por ejemplo, el asunto *Secretary for Justice v. Parker 1999 (2) ZLR 400 (H)* (High Court (Harare, Zimbabwe), sentencia de 30 de noviembre de 1999, *Secretary For Justice v. Parker 1999 (2) ZLR 400 (H),* n. HC/E/ZW 340. Se trataba de una sustracción desde Reino Unido a Zimbawe. La madre alegó en su defensa la aplicación del grave riesgo del art. 13.1.b) por el comportamiento agresivo del padre y las dificultades económicas y personales que podría enfrentar si regresaba. Sin embargo, los tribunales lo rechazaron por entender que no afectaba al art. 13.1.b), pues el comportamiento del padre y la mala relación de la pareja sólo afectaban a la madre, pero no a los hijos. En consecuencia, se ordenó el retorno de los dos menores al Reino Unido (http://www.incadat.com).

2.3. Ciberviolencia contra las mujeres en la directiva (UE) 2024/1385: el vínculo entre el interés superior del menor y el de la madre víctima de violencia machista

En este contexto, el equilibro de intereses involucrados (el de la madre maltratada y el del menor sustraído), así como el vínculo entre la violencia sufrida por la madre y la valoración del interés superior del menor en estos casos, pone sobre la mesa delicadas cuestiones de difícil solución práctica. Son muchas las dudas que emergen sobre lo que constituye en cada supuesto concreto el interés del menor, pero también el de la mujer en situación de vulnerabilidad, máxime con la regulación tan limitada que nos ofrece el DIPr. europeo actual con textos como los mencionados.

En este sentido, hay resoluciones judiciales que diferencian el riesgo para la madre y el riesgo para los hijos, estimando que sólo cuando se acredita este último cabe oponerse a la restitución del menor[52]. En ocasiones los tribunales han reconocido admitir "indirectamente y a priori el riesgo psíquico del menor por presenciar malos tratos de palabra o de obra sobre su madre" [53]. De hecho, hace tiempo

[52] Por ejemplo, Audiencia Provincial de Granada, sentencia n. 152/2017 de 21 de abril 2017 (Roj: SAP GR 486/2017). Con ocasión del asunto *Walsh v. Walsh, Nº 99-1747 (1st Cir. July 25*, 2000), (United States Court of Appeals for the First Circuit (Estados Unidos), sentencia de 25 de julio de 2000, *Walsh v. Walsh, Nº 99-1747,* n. HC/E/Usf 326), se pretendió argumentar que si la violencia es contra el menor si que procede aplicar la excepción del art. 13.1.), pero no si es contra la madre. Al final se rechazó el retorno, pero por entender que las medidas de protección que se adoptaran en el Estado de residencia del padre no iban a ser eficaces dado el reiterado incumplimiento de éstas por el padre (http://www.incadat.com).

[53] Audiencia Provincial de Las Palmas, sentencia de 25 de julio 2016 (Roj: SAP GC 2345/2016). Ver M.J. CAÑADAS LORENZO, *La incidencia de la violencia de género en la sustracción internacional de menores*, http://www.poderjudicial.es, pp. 3 ss. Asimismo, en el asunto *Al-Hadad v. Al Harash, 2020 ONCJ 269*, (Tribunal Primera Instancia de Canadá – Ontario, sentencia de 3 de junio de 2020, *Al-Hadad v. Al Harash, 2020 ONCJ 269,* n. HC/E/CA 1493) se denegó el regreso del menor desde Canadá a Alemania, por entender que el daño y abuso físico y emocional del padre hacia la madre repercutía también en cuanto abuso emocional en los menores, en el sentido del art. 13.1.b) del Convenio de La Haya, y a pesar de que en Alemania había medidas de protección suficientes. Destaca también el caso *State central authority to the Departmen of human services v. Mander* (2003), *FamCa 1128* (Family Court of Australia, sen-

que está demostrada la correlación entre la violencia conyugal o de pareja y el maltrato infantil. Y el daño causado a la madre viene reconocido cada vez más como constitutivo de daño al menor, por cuanto la violencia contra la madre también puede tener un efecto traumático para el/la menor que la presencia. No obstante, el impacto de dicha violencia sobre el menor y los riesgos futuros asociados deben ser evaluados en cada supuesto concreto[54].

En España la LO 8/2015, de 22 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, ya enfatizaba la necesidad de reconocer a los menores como víctimas de la violencia de género con el fin de visibilizar esta forma de violencia que se puede ejercer sobre ellos (Exposición de motivos). Más tarde, la LO 8/2021 que modifica la LO 1/2004 sobre violencia de género ha ido más allá al confirmar que la violencia de género comprende la violencia que, con el objetivo de causar perjuicio o daño a las mujeres, se ejerza sobre sus familiares o allegados menores de edad.

En esta línea se manifiesta la directiva 2024/1385 al definir a la víctima como "toda persona, independientemente de su género, que haya sufrido algún daño directamente causado por violencia contra las mujeres o violencia doméstica, e incluye a los menores que hayan sufrido algún daño porque hayan sido testigos de violencia doméstica" (art. 2.c). El legislador europeo ha considerado con acierto que, "debido a su vulnerabilidad, ser testigo de violencia doméstica puede ser devastador para los menores. Los menores que son testigos de violencia doméstica dentro de la familia o de la unidad doméstica suelen sufrir daños psicológicos y emocionales directos que afectan a su desarrollo y corren un mayor riesgo de padecer enfermedades físicas y

tencia de 17 de septiembre de 2003, *State central authority to the Departmen of human services v. Mander*, n. HC/E/AU 574), sentencia de 17.9.2003, en el que operó también la excepción del art. 13.1.b) para denegar el regreso de dos menores desde el Reino Unido a Australia. En esta ocasión se consideró que las amenazas y violencia del padre (con sucesivos procesos judiciales y sanciones penales) a la madre, de la que los menores habían sido testigos, suponían un grave riesgo para ellos. Es más, se consideró que, aunque el sistema inglés se caracteriza por ofrecer una buena protección a las víctimas de violencia, el regreso al Reino Unido de los menores supondría exponerlos a más incidentes de violencia.

[54] *Proyecto de Buenas prácticas…, op. cit*, pp. 74 ss.

mentales, tanto a corto como a largo plazo. El reconocimiento de que los menores que han sufrido daños causados directamente por haber sido testigos de violencia doméstica son a su vez víctimas supone un paso importante en la protección de los menores que sufren como consecuencia de la violencia doméstica" [55].

3. *Desafíos en la cooperación judicial digitalizada en el combate de la violencia contra la mujer en la sustracción de menores*

La digitalización constituye sin duda uno de los motores clave de la política de justicia de la UE, junto con la independencia judicial, si bien se manifiesta con diferencias todavía notables entre los EEMM. Aunque hay algunos más avanzados que otros, en general se aprecian aspectos como que, por ejemplo, todos disponen de videoconferencias, el personal de los tribunales puede teletrabajar a distancia de forma segura y son muchos también los que utilizan *blockchain* o Inteligencia Artificial[56].

Pero todavía queda mucho por hacer. Un paso importante en la regulación de la comunicación digital entre los Estados miembros ha sido la refundición del reglamento (UE) 2020/1784 en el ámbito de las notificaciones y el reglamento (UE) 2020/1783 en relación con la obtención de pruebas, aplicables desde el 1 de julio de 2022. Con ellos se ha dado un paso más en la comunicación digital al obligar a las autoridades competentes de los Estados miembros a comunicarse entre sí,

[55] Considerando 13 directiva (UE) 2024/1385, cit. p. 1 ss. Es más, el art. 31.1 señala que los Estados miembros "se asegurarán de que se preste a los menores un apoyo específico adecuado tan pronto como las autoridades competentes tengan motivos razonables para pensar que ese menor podría haber estado sometido a violencia contra las mujeres o violencia doméstica, o podría haber sido testigo de ellas. El apoyo prestado a los menores será especializado y adecuado para su edad, necesidades de desarrollo y situación individual, y respetará asimismo el interés superior del menor" (véase art. 31 completo).

[56] X. KRAMER, *Digitising access to justice: the next steps in the digitalisation of judicial cooperation in Europe,* en *Revista General de Derecho Europeo*, 2022, n. 56, pp. 1-9; M.B. NOODT TAQUELA, *Notificaciones electrónicas: más allá del espacio europeo,* en *Revista General de Derecho Europeo*, 2025, n. 66 (en prensa, gentileza de la autora).

por ejemplo, en relación con el intercambio de formularios normalizados, mediante un sistema informático descentralizado. Estos deben estar conectados a través de un sistema interoperable, como es el e-Codex. Este último se ha introducido con el reglamento (UE) 2022/850 del Parlamento europeo y del Consejo de 30 mayo 2022 relativo a un sistema informatizado de comunicación en los procesos civiles y penales transfronterizos (sistema e-CODEX) y por el que se modifica el reglamento (UE) 2018/1726[57]. En dicho texto se basa el reciente reglamento (UE) 2023/2844 sobre la digitalización de la cooperación judicial que aspira a la modernización del marco legislativo de los procedimientos transfronterizos de la UE en materia civil, mercantil y penal[58].

Todos estos instrumentos pueden tener unos efectos de gran relevancia sobre un proceso de sustracción internacional de menores, incluidos aquéllos en que la madre sustractora ha sido víctima de violencia machista. Muchos de los obstáculos y desafíos a los que se enfrenta dicho proceso (ejemplo, agilización en las pruebas de la violencia contra la madre, medidas de protección rápidas y eficaces), podrían minimizarse si, como aspira el legislador de la UE con el último reglamento (UE) 2023/2844, se alcanza una transformación digital de los sistemas judiciales en los que participen los profesionales del derecho. Dicha transformación haría posible un "intercambio electrónico transfronterizo de datos sobre asuntos entre las autoridades competentes que sea rápido, directo, interoperable, fiable, accesible, seguro y eficiente"[59]. Un intercambio electrónico de tales características sería efi-

[57] Propuesta de reglamento del Parlamento europeo y del Consejo, *relativo relativo a un sistema informatizado de comunicación en los procesos transfronterizos penales y civiles (sistema e-CODEX), y por el que se modifica el Reglamento (UE) 2018/1726*, de 2 de diciembre de 2020. Sobre la evolución de todo este proceso ver G. PALAO MORENO, *El Reglamento (UE) núm. 2020/1784 y su contribución al impulso de la digitalización de la cooperación judicial en materia civil y mercantil en la Unión Europea, Actualidad jurídica iberoamericana*, n. 21, 2024, pp. 190-223; E. CERRATO GURI, *Ciberviolencia de género: influencia internacional y europea en la obtención y conservación de la prueba electrónica, Revista General de Derecho Europeo*, n. 61, 2023, pp. 170 ss; E.A. ONTANU, *The digitalisation of European Union Procedures: A New Impetus Following a Time of prolonged Crisis, Law, Tecnnology and Humans*, 2023, vol. 5 (1), pp. 93-110.

[58] Ver X. KRAMER, *op. cit*., p. 6.

[59] Considerando 8, reglamento (UE) 2023/2844, cit. p. 1 y ss.

caz tanto para acelerar el retorno inmediato del menor en casos de traslado o retención ilícita, como para conseguir justo lo contrario, esto es, frenar dicho retorno cuando sea evidente que éste no se corresponde con el interés superior del menor, en los casos en que dicho traslado o retención han sido motivados por una situación de violencia contra su madre o contra el menor mismo.

El reglamento (UE) 2023/2844 tiene por objeto mejorar la eficiencia y la efectividad de los procesos judiciales y facilitar el acceso a la justicia mediante la digitalización de los canales de comunicación existentes. Ello supondrá "un ahorro de costes y tiempo, una reducción de la carga administrativa y una mayor resiliencia ante circunstancias de fuerza mayor para todas las autoridades que participan en la cooperación judicial transfronteriza"[60].

Es importante destacar que este reglamento no interfiere en la aplicación de los reglamentos (UE) 2020/1784 (notificaciones) y 2020/1783 (obtención de pruebas), que pueden ser fundamentales en un proceso de sustracción internacional. Ambos reglamentos ya establecen normas específicas sobre la digitalización de la cooperación judicial. Sin embargo, el reglamento (UE) 2023/2844 (digitalización) aclara la necesidad de introducir modificaciones en el primero de ellos (sobre notificaciones) con el fin de mejorar la notificación y el traslado electrónicos directos de documentos que deban realizarse directamente a una persona que tenga dirección conocida a los efectos de notificación y traslado en otro Estado miembro[61].

El éxito de la cooperación judicial digitalizada en un contexto tan específico como el de la sustracción de menores realizada por la madre víctima de violencia depende, a su vez, del éxito en cumplir con unos desafíos de gran relevancia, sobre los que inciden muchos de los reglamentos mencionados. El primer desafío alude a un problema visible y complejo que abarca dos aspectos: por una parte, la prueba de la violencia de género, realizada o no en un entorno digital, y su incidencia sobre la eventual orden de retorno del menor en el marco del reglamento 2019/1111[62] y el Convenio de La Haya 1980. Por otra, las me-

[60] Considerando 4, reglamento (UE) 2023/2844, cit. p. 1 y ss.

[61] Considerando 17, reglamento (UE) 2023/2844, cit. p. 1 y ss.

[62] Ver art. 27 (procedimiento de restitución de un menor), art. 28 (ejecución de

didas de protección que deban adoptarse en el caso de que, tanto si se demuestra o no la violencia contra la madre, se ordena que el menor regrese al Estado en el que tenía su residencia habitual antes de su sustracción. El segundo desafío se expone al final de este trabajo. Veamos ahora algunas consideraciones sobre el primero de los desafíos.

3.1. *La prueba, informaciones y notificaciones sobre la violencia contra la madre sustractora: relevancia del reglamento 2020/1783 (obtención de pruebas) y reglamento 2020/1784 (notificaciones)*

En la práctica, son múltiples las dificultades existentes en el sistema de la prueba en los procesos por violencia de género al referirse a actos realizados en un ámbito estrictamente privado, fundamentalmente en la intimidad del entorno doméstico o familiar, sin terceros ajenos a la familia, por lo que no suele haber testigos directos. Ello supone que la declaración de la víctima es la principal (sino la única) prueba de cargo contra el agresor. A ello se unen conductas de la víctima que dificultan la veracidad de los hechos. En ocasiones la relación de sumisión o de dependencia frente al agresor, los lazos afectivos todavía existentes, el miedo a represalias, entre otras, avalan este comportamiento de la víctima de violencia de género[63].

Por ello, la dificultad de demostrar la violencia provoca decisiones judiciales discutibles que ordenan el regreso del menor a pesar de dicha violencia (decisión que, recordemos, en la UE es ejecutable sin exequátur conforme al reglamento (UE) 2019/1111), bien por falta de

las resoluciones por las que se ordena la restitución de un menor) y art. 29 (procedimiento siguiente a la denegación de restitución del menor con arreglo al art. 13, 1 b) y el art. 13.2, del Convenio de La Haya de 1980.

[63] Ver A. MONTESINOS GARCÍA, *Especificidades probatorias en los procesos por violencia de género,* en *Revista de derecho penal y criminología*, 3ª época, 2017, n. 17, pp. 127-165, quien además subraya que los juicios rápidos en que se desarrolla gran parte de los procesos por violencia de género no resultan funcionalmente apropiados para llevar a cabo una investigación adecuada de este tipo de delitos. La obtención de elementos que corroboren la veracidad de la declaración de la víctima es esencial para evitar que situaciones de maltrato habitual se califiquen por el juez como simples episodios violentos aislados. La sencillez de la investigación típica de los juicios rápidos redunda, por tanto, negativamente en la escasa obtención de fuentes de prueba, en un proceso en el que la complejidad probatoria es manifiesta.

prueba o bien porque no se considera suficiente para constituir un grave riesgo para el menor en el sentido del art. 13.1.b) del Convenio de La Haya 1980. La perspectiva de género y la sensibilidad hacia la madre maltratada brillan por su ausencia. Los tribunales prefieren priorizar el regreso del menor supeditado al cumplimiento de unas medidas de protección en el país donde reside el autor de la violencia. Tales medidas se habrían querido reforzar con el reglamento (UE) 2019/1111 (art. 27.3.) y ya antes, en España, por la mencionada LJV, pero no siempre son garantía del interés del menor.

Son varios los extremos que, en general, hay que tener en cuenta en relación con la prueba de la violencia machista en el contexto de la sustracción de menores. Por una parte, es fundamental recabar información sobre acciones judiciales pendientes que hubiera contra el progenitor privado del menor y supuestamente maltratador, informes policiales, registros de consulados o embajadas, informes de refugios para víctimas de violencia doméstica y certificados médicos relativos a incidentes de violencia. Incluso posibles correos electrónicos u otra correspondencia pueden ser útiles para demostrar la existencia de los malos tratos[64]. Alguna jurisprudencia revela como pruebas pertinentes para no ordenar el retorno del menor, entre otras, la declaración de la madre y de los hijos, comunes o no de la pareja, declaraciones notariales de testigos o trabajadores sociales, pruebas periciales técnico-forenses, testimonios de familiares de la madre y documentación relativa a la puesta en conocimiento de las autoridades correspondientes como la Policía, Juzgados o el Ministerio competente en dicho ámbito[65].

No obstante, el éxito en la prueba de la violencia ejercida, por ejemplo, por medios digitales, incluyendo un teléfono móvil o un

[64] Ver *Guía de buenas prácticas, op. cit.,* p. 12.

[65] Citada por M.J. CAÑADAS LORENZO, *La incidencia de la violencia de género en la sustracción internacional de menores*, disponible en: http://www.poderjudicial.es, p. 7; I. REIG FABADO, *El traslado ilícito de menores en la Unión Europea: retorno vs. Violencia familiar o doméstica,* en *Cuadernos de Derecho Transnacional*, 2018, vol. 10, n. 1, pp. 610-619; M.D. ADAM MUÑOZ, *Las situaciones de violencia doméstica en los supuestos de sustracción de menores en el marco de la Unión europea*, en B. CAMPUZANO DÍAZ, M.P. DIAGO DIAGO, M.A. RODRÍGUEZ VÁZQUEZ, *De los retos a las oportunidades en el derecho de familia y sucesiones internacionales*, Valencia, 2023, pp. 317-344.

equipo informático, despierta dudas sobre su efectividad. Si nos centramos en el acoso realizado mediante mensajes de texto o de WhatsApp varias son las consideraciones que suelen hacerse sobre el valor probatorio de la violencia contra la mujer, en concreto de la ciberviolencia. Baste referirnos en estos momentos a que para que un mensaje enviado por correo electrónico, WhatsApp, Telegram o cualquier forma de mensajería inmediata, pueda aportarse en el proceso como prueba – documental y/o pericial – habrá que indagar cuál es su fuente para comprobar su veracidad y su validez. Por ejemplo, sobre un WhatsApp (como los mandados por el Sr. Arcuri a la Sra. Rivas) habrá que certificar su contenido mediante cotejo del letrado/a pertinente de la Administración de justicia y descartar posibles manipulaciones y, en cambio, sobre un correo electrónico que se encuentra en un ordenador habrá que hacer un clonado del disco duro.[66] Todos ellos son medios de prueba electrónica que se componen del soporte material, el teléfono smartphone, de la información que contiene el soporte, y de su posible relevancia jurídica[67].

En el contexto de la prueba de la violencia – digital o no – contra la madre sustractora deviene de gran interés el reglamento (UE) 2020/1784 en materia de obtención de pruebas, que pretende aumentar la eficacia y la celeridad de los procedimientos judiciales, reduciendo los retrasos y costes soportados por los particulares[68]. Se aboga, de

[66] Ver ampliamente el capítulo en este Libro realizado por M.J. JORDÁN DÍAZ-RONCERO, *La prueba en los procesos por violencia digital de género,* y la bilografia y jurusprudencia que en él se citan. Asimismo, P. ARRABAL PLATERO, *La prueba tecnológica: aportación, práctica y valoración*, Valencia, 2020, p. 398; O. FUENTES SORIANO, *El valor probatorio de los correos electrónicos*, en J. M. ASENCIO MELLADO (dir.) *Justicia penal y nuevas formas de delincuencia,* Valencia, 2017, p. 202, por lo que será necesario en caso de impugnación llevar a cabo prueba pericial tecnológica. Asimismo, la información disponible en https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/pericia-informatica/.

[67] Según la Audiencia Provincial de Valencia, Sección 4ª, sentencia n. 276/2017, de 25 de abril 2017, rec. 28/2017.

[68] Considerando 3, reglamento (UE) 2020/1783, cit. Ver N. MARCHAL ESCALONA, *El nuevo marco europeo sobre notificación y obtención de pruebas e extranjero: hacia un espacio judicial europeo digitalizado",* en *Revista Española de Derecho Internacional*, 2022, vol. 72, n. 1, pp. 155-179, pp. 158-159; L. FUMAGALLI, *Problemi vecchi e nuovi nella cooperazion per l'assunzione delle prove all'estero in materia civile: la rifusione de-*

este modo, por el uso de cualquier tecnología moderna de comunicaciones que asegure la rapidez en la transmisión de las solicitudes y las comunicaciones entre los Estados miembros a efectos de la obtención de pruebas. Para ello, las comunicaciones e intercambios de documentos se harán a través del ya citado sistema informático descentralizado, seguro y fiable, "que comprenda sistemas informáticos nacionales que estén interconectados y sean técnicamente interoperables, por ejemplo, y sin perjuicio de un progreso tecnológico ulterior, sobre la base de e-CODEX"[69].

Hay que resaltar que la aplicación del reglamento (UE) 2020/1784 no impedirá el intercambio de información previstos en otros reglamentos como puede ser el reglamento (UE) 2019/1111, incluso en los casos en que dicha información tenga fuerza probatoria, lo que deja la elección del método más adecuado a la autoridad requirente. Esta precisión podría tenerse en cuenta en un litigio sobre sustracción de menores en que resulte aplicable este último reglamento y hubiera que probar hechos que incidan sbre la definición del interés del menor.

Con el objeto de facilitar la obtención de pruebas, el reglamento (UE) 2020/1784 destaca que los tribunales de un Estado miembro puedan conforme a su *lex fori* obtener pruebas directamente en otro Estado miembro, si este último acepta la solicitud para obtener pruebas directamente, y de acuerdo con las condiciones establecidas por el órgano central o la autoridad competente del Estado miembro requerido. Cuando la obtención de pruebas consista en la toma de una declaración o el interrogatorio de un testigo, de una parte en el procedimiento o de un perito presente en otro Estado miembro, el tribunal requirente deberá obtener dichas pruebas directamente por videoconferencia u otra tecnología de telecomunicaciones", siempre que dicha tecnología está disponible. También se puede utilizar la videoconfe-

lla disciplina nell'unione europa, en *Rivista di diritto internazionale privato e processuale*, 2021, n. 4, pp. 844-877; V. RICHARD, *La refonte du règlement sur l'obtention des preuve en matière civile,* en *Revue critique de droit international privé*, 2021, n. 1(1) pp. 67-77.

[69] Ahora bien, el uso del sistema descentralizado podría verse imposibilitada debido a una interrupción del sistema o a la naturaleza de las pruebas, por ejemplo, cuando se transmitan muestras de ADN o de sangre (considerandos 7 y 2, reglamento (UE) 2020/1783, cit.).

rencia para oír a un menor con arreglo a lo dispuesto en el reglamento (UE) 2019/1111[70]. No obstante, las limitaciones que tales medios suscitan en la práctica deberán tenerse en cuenta[71].

Al reforzamiento de la cooperación en el ámbito de la prueba de la violencia contra la madre sustractora, se añade el de las comunicaciones judiciales directas. Ello puede servir para verificar, por ejemplo, si un tribunal extranjero constató la existencia de violencia contra la mujer y si en tal caso se dictaron órdenes de protección o hubo acciones judiciales, como consecuencia de infracciones a tales órdenes. En este ámbito puede ser de gran utilidad el reglamento (UE) 2020/1784 (notificaciones) que ha potenciado la digitalización en la cooperación judicial interestatal tan necesaria en procedimientos como los de sustracción internacional de menores.

Una primera novedad importante es que el reglamento (UE) 2020/1784 incorpora un sistema de cooperación directa entre organismos transmisores y receptores en los diversos Estados miembros, por medio de un sistema informático descentralizado seguro y fiable (arts. 5 y 8 a 15). Su objetivo es crear una red de sistemas nacionales y de puntos de acceso de gestión, que serán de responsabilidad nacional, en los que se garantizará tanto la interconectividad y la interoperabilidad segura y fiable de los sistemas informáticos nacionales, como el intercambio de datos.

Para ello se han previsto dos fases. Una primera fase afrontará el desarrollo de un sistema informático en todos los EEMM que permita la interconexión y la interoperabilidad de sus sistemas informáticos nacionales. Ello se hará a partir de un sistema de código abierto que permita la interconectividad de los sistemas nacionales con el e-CODEX, como ya mencionábamos en relación con el reglamento

[70] Considerando 21, reglamento (UE) 2020/1783, cit. p. 1 y ss.

[71] Por ejemplo, faltaría aclarar, al igual que en el reglamento (UE) 2023/2844, cit. p. 1 y ss. aspectos como qué plataformas usar para llevar a cabo las videoconferencias, que llevaría a admitir algunas como Zoom, Microsoft Teams o Skype, cuya baja calidad podría cuestionar, por ejemplo, el respeto del principio de inmediación. Sobre éstas y otras limitaciones derivadas de la legislación procesal española en el proceso de digitalización ver D. MARCOS FRANCISCO, *Hacia la plena digitalización de las comunicaciones en los procedimientos judiciales civiles en la Unión Europea y en España,* en *Revista General de Derecho Europeo*, 2025, n. 65, pp. 18-65.

(UE) 2020/1783 sobre obtención de pruebas. En una segunda fase de ejecución, se introducirá un programa informático de aplicación de referencia elaborado por la propia Comisión, para garantizar la integridad y fiabilidad del documento transmitido y la interoperabilidad del sistema para el intercambio de informaciones entre las diferentes autoridades estatales. En este proceso será esencial que se otorguen plenos efectos jurídicos a los documentos electrónicos (art. 6)[72].

La segunda novedad relevante que introduce el reglamento (UE) 2020/1784 es que hace posible el recurso a otras vías de auxilio judicial, de forma alternativa y excepcionalmente, como la notificación o traslado electrónico de documentos (art. 19), permitiendo además que pueda realizarse mediante el "punto de acceso electrónico europeo"[73]. En concreto, ha sido el reglamento (UE) 2023/2844 (digitalización) el que incorpora la creación de dicho punto de acceso electrónico europeo, dentro del Portal Europeo de e-Justicia, para garantizar el acceso a la justicia de todos[74].

[72] En este entorno no olvidemos otras herramientas elaboradas en la UE como el *Portal Europeo de e-Justicia* y el *Atlas Civil Europeo* (Disponible en: https://e-justice.europa.eu/home?action=home), así como la *Agencia de la Unión Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia* (EU-LISA) (reglamento (UE) 2018/1726 del Parlamento europeo y del Consejo, *relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA),* y por el que se modifican el reglamento (CE) 1987/2006 y la decisión 2007/533/JAI del Consejo y se deroga el reglamento (UE) 1077/2011, de 14 de noviembre de 2018, en DOUE 259 de 21 de noviembre de 2018). Igualmente, el reglamento (UE) 2019/818 del Parlamento europeo y del Consejo, *relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración* y por el que se modifican los reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816, de 20 de mayo de 2019, en DOUE 135 de 22 de mayo de 2019, pp. 85-135). Ver ampliamente G. PALAO MORENO, *op. cit*., p. 208; M. VELICOGNA, *Coming to Terms with Complexity Overload in Transbord e-Justice: The e-CODEX Platform*, en F. CONTINI, G.F. LANZARA (eds.), *The Circulation of Agency in E-Justice Law*, Springer, Heidelberg, 2014, pp. 309-330.

[73] Considerando 21 reglamento (UE) 2020/1783, cit. p. 1 y ss.

[74] Considerandos 10. 27 y 30 reglamento (UE) 2023/2844, cit. p. 1 y ss. Para ello, además de que se conozca su dirección, se requerirá que el destinatario hubiera prestado su consentimiento de forma previa y expresa, a favor del empleo de este medio

También la directiva 2024/1385 alude a la relevancia de la prueba, en concreto de la violencia ejercida de modo digital, de modo que la víctima pueda aportar pruebas sin sufrir victimización secundaria o reiterada. Por eso, junto con las denuncias presenciales, los EEMM deben ofrecer la posibilidad de formular denuncias en línea o mediante otras TIC accesibles y seguras, al menos en relación con los ciberdelitos, entre ellos el ciber acecho y el ciber acoso. En dicho entorno, la directiva insiste en la necesidad de que las víctimas puedan cargar material relacionado con su denuncia, como capturas de pantalla de la presunta conducta violenta. Pero, además, teniendo en cuenta las "particularidades de la violencia contra las mujeres y la violencia doméstica, y del mayor riesgo de que las víctimas retiren sus denuncias a pesar de haber sido víctimas de un delito, es importante que las pruebas pertinentes se recojan de manera exhaustiva lo antes posible, de conformidad con las normas procesales nacionales aplicables" [75].

Es deseable que tanto los reglamentos mencionados como la directiva puedan, progresivamente, hacer frente a las dificultades probatorias que inciden negativamente sobre un proceso de traslado ilícito de un menor cometido por una víctima de violencia de género. Dificultades que se añaden al difícil encuadre de estas situaciones en el ámbito del Convenio de La Haya 1980 para poder excepcionar el retorno del menor con base en el art. 13.1. b, como ya se expuso. La orden de regreso del menor se realiza muchas veces por la falta de prueba (o insuficiente) de la violencia o de la repercusión emocional sobre el menor, que se puede producir porque no se admitan determinados medios en el marco del proceso sobre el retorno[76]. La mayoría de las veces, además, las pruebas que podrían aportarse se encuentran en el Estado de la residencia habitual del menor anterior a su sustracción, lo

electrónico a efectos de la notificación y de traslado de documentos durante el transcurso del procedimiento judicial en cuestión (art. 4.6).

[75] Considerandos 29-32 directiva (UE) 2024/1385, cit. p. 1 ss.

[76] M. REQUEJO ISIDRO, *op. cit.,* p. 183, en relación con C.S. BRUCH, *The unmet needs of domestic violence victims and their children in Hague Child abduction Convention cases,* en *Family Law Quarterly*, 2004, vol. 38, n. 3, p. 529, que alude a las limitaciones probatorias del procedimiento inglés en este tipo de casos de violencia contra la mujer.

que dificulta su aportación en el procedimiento[77]. Todo ello provoca que la situación de violencia que se alega por la madre y que podría implicar una situación de riesgo para el menor en caso de retorno, no suela estimarse al final por los Tribunales[78].

Otro aspecto que puede incidir negativamente en el régimen de prueba de la violencia de género es el objetivo de la celeridad impuesto por la normativa actual en relación con el procedimiento de retorno del menor. El reglamento (UE) 2019/1111 alude al plazo máximo de 6 semanas desde que interpuso la demanda. Esta brevedad, pensada en interés del menor, no ayuda en un procedimiento de violencia de género, al reducir el periodo para valoración de dicha violencia y para eventuales comunicaciones interestatales que deban llevarse en este ámbito[79].

Tanto el cumplimiento de los plazos para ordenar el retorno del menor como para, en su caso, ordenar lo contrario por haberse demostrado los malos tratos y la inconveniencia de que el menor regrese, dependerá de la existencia de un sólido marco de cooperación interestatal, que incluya una comunicación directa entre las autoridades y los tribunales de diferentes países[80]. Será muy relevante la asistencia de las autoridades centrales y el apoyo en las redes existentes de cooperación judicial, incluida la Red Internacional de jueces de La Haya y jueces de enlace. Esto probablemente se vería reforzado por la concentración de

[77] M.J. CAÑADAS LORENZO, *op. cit*, p. 7.

[78] Ver los ejemplos de la nota 14.

[79] En este sentido la mencionada *Guía de Buenas Prácticas* de 2021 señala que "la obligación de actuar con urgencia no significa que el tribunal deba descuidar la evaluación adecuada de las cuestiones planteadas, incluidos los casos en que se opone la excepción de grave riesgo. Sin embargo, sí exige que el tribunal solamente recabe información y/o pruebas suficientemente relevantes para el caso, al igual que examine dicha información y/o pruebas, incluso la prueba o los dictámenes periciales, de manera rápida y sumamente precisa" *Guía de buenas prácticas, op. cit.,* p. 24. El requisito de la rapidez se expone repetidamente en el reglamento (UE) 2019/1111, cit. p. 1 y ss. (por ejemplo, arts. 23, 24, 27 y 28).

[80] Sobre dicho rol ver I. GOICOECHEA, H. VAN LOON, *The Key Role of Judges in the Development of Private International Law: Lessons Learned from the Work of the Hague Conference on Private International Law*, en V. RUIZ ABOU-NIGM, M.B. NOODT TAQUELA (dirs.), *Diversity and Integration in Private International Law, Edinburgh University Press,* 2019, p. 295.

la competencia en unos pocos jueces[81]. En el caso de sustracciones cometidas en un contexto de violencia de género sería deseable, asimismo, la presencia de jueces y personal especializado en la materia. Pero, sin duda, la puesta en práctica de los reglamentos 2020/1783 (prueba) y 2020/1784 (notificaciones) pueden, con el tiempo, mejorar dicho sistema de cooperación.

3.2. *Las medidas de protección tras la orden de retorno del/la menor: relevancia del reglamento (UE) 606/2013 (OPE) y la directiva 2024/1385*

La referencia a las medidas de protección en este ámbito comporta tener en cuenta, de un lado, las que deban adoptarse para proteger al menor sustraído ilícitamente tras dictarse, no obstante, la situación de violencia, la orden de su retorno al país de la residencia habitual anterior a dicha sustracción. De otro, las medidas que en su caso deban adoptarse para proteger a la madre que ha realizado el acto ilícito y que ha sido víctima de violencia.

En relación con las medidas de protección del menor se espera que se beneficien de las nuevas reglas introducidas por el reglamento Bruselas II ter, a través del capítulo III, sobre el regreso del menor. Destaca, en particular, el reforzamiento de las medidas provisionales que pudieran adoptarse en el procedimiento de retorno, incluida una mayor comunicación entre las autoridades judiciales y cooperación entre las Autoridades Centrales[82]. Estas reglas promueven también el contacto entre la persona que solicita el retorno el menor y este último, teniendo en cuenta su interés superior. Cuestión delicada si ha habido una situación de malos tratos hacia la madre y/o el menor. Se ha potenciado, además, la posibilidad de que éste sea escuchado en juicio, aunque su alcance y procedimiento seguirá dependiendo del derecho

[81] Según se señala en Considerando 41, reglamento (UE) 2019/1111, cit. p. 1 y ss.

[82] Ver, entre otros, A.J. CALZADO LLAMAS, *Las medidas provisionales y cautelares en los procedimientos de restitución de menores. Análisis del Reglamento UE 2019/1111 en su conexión con el ordenamiento jurídico español, Cuadernos de Derecho Transnacional*, marzo 2021, vol. 13, n. 1, pp. 87-109; I. PETRELLI, *The law applicable to provisional and protective measures with a focus on the EU system of ancillary reliefs, Yearbook of Private International Law*, 2019/2020, vol. 21, pp. 113-148.

nacional de los Estados miembros, lo que puede seguir produciendo problemas en la puesta en práctica de todas estas reglas. La digitalización de la cooperación judicial podrá, no obstante, ser de ayuda cuando sea efectiva entre los Estados miembros.

En la práctica la valoración de la excepción del art. 13.1.b) del Convenio de La Haya 1980 se vincula a la existencia de medidas de protección del menor en el Estado de residencia habitual anterior a su sustracción ilícita. Ahora bien, dicha excepción no debe limitarse a un análisis de las circunstancias anteriores o vigentes al momento de dicha sustracción, sino que "requiere mirar hacia el futuro, esto es, a las circunstancias que existirían si el niño/a fuera restituido inmediatamente[83]. Por ello es relevante, más que haya medidas de protección en el Estado de residencia habitual del –supuesto- maltratador, que éstas sean realmente "efectivas en circunstancias específicas" para proteger a los menores de un riesgo grave[84], o incluso de riesgo potencial[85].

[83] M. REQUEJO ISIDRO, *op. cit.,* p. 185. Asimismo, ver las apreciaciones de M. SOTO MOYA, *Fundido a negro tras el retorno de menores sustraídos por sus madres víctimas de violencia de género a sus países de residencia originaria*, en A. LARA AGUADO (dir.), *Protección de menores en situaciones transfronterizas. Análisis multidisciplinar desde las perspectivas de género, de los derechos humanos y de la infancia,* Valencia, 2023, pp. 878-901.

[84] Según se expuso con ocasión del ya citado asunto *AD v. SD*, en el que se denegó el retorno de los menores tras su sustracción ilícita por la madre desde EEUU a Escocia en relación a la violencia ejercida mediante amenazas por mensajes de texto reiterados del padre a la madre. En el mismo sentido, *Re T (abduction: Protective measures: agreement to return),* 2023 *EWCA Civ* 1415 (Tribunal de Apelaciones del Reino Unido – Inglaterra y Gales, sentencia de 1 de diciembre de 2023, *Re T (abduction: Protective measures: agreement to return),* 2023 *EWCA Civ 1415*, n. HC/E/Uke 1598) sobre el traslado ilícito de un menor por su madre al Reino Unido desde EEUU, que alegó violencia hacia ella por el padre del menor. Aunque los tribunales consideraron que la violencia no estaba suficientemente probada, no se podía ordenar el regreso del menor, por cuanto sin medidas adecuadas de protección existía un grave riesgo en el sentido del art. 13.1.b) del Convenio de La Haya (Disponible en: http://www.incadat.com).

[85] Tal como se señaló con ocasión del citado asunto *Walsh v. Walsh*, en el que se rechazó el retorno por "riesgo potencial" hacia los menores, más que por la violencia en sí que se había ejercido hacia la madre y los menores, por entender que las medidas de protección que se adoptaran, aunque fueran adecuadas, no iban a ser eficaces dados los antecedentes del padre en la violación de órdenes expedidas por los tribunales.

Ello explica que la excepción de grave riesgo deba comprender, si se estima necesario y apropiado, tener en cuenta la disponibilidad de medidas de protección adecuadas y eficaces en el Estado de residencia habitual"[86], lo que no siempre puede estar garantizado. Sin embargo, la jurisprudencia se acoge mayoritariamente a la existencia de tales medidas para ordenar el regreso del menor no obstante la situación de malos tratos[87]. En este ámbito, puede ser esencial la digitalización de la cooperación judicial entre el Estado de la residencia habitual del menor anterior a su sustracción y el Estado donde ahora se encuentra ilícitamente con su madre.

Si finalmente se ordena la restitución del menor a pesar de los malos tratos hacia su madre, habrá que tener en cuenta aspectos varios que pueden afectar a las medias de protección de ambos. Por ejemplo, habrá que comprobar: a) Si conviene dictar una medida de alejamiento; b) Si hay que prohibir el contacto con el menor o establecer que éste se realice con vigilancia; c) Si cabe adoptar otras medidas de protección no sólo para el menor sino para la madre sustractora, como

Ello generaba dudas sobre la protección de los menores en caso de ser restituidos por el riesgo alto físico y psicológico hacia ellos. Un riesgo que no debía ser inmediato, sino grave, conforme al Convenio de la Haya 1980 (Disponible en: http://www.incadat.com). La alusión al riesgo potencial se encuentra en otras decisiones como la SAP Barcelona de 15 julio de 2022 (sección 18) en una sustracción de una menor por su madre desde Reino Unido a España (Audiencia Provincial de Barcelona, sentencia n. 7839/2022). Para la AP dicho riesgo potencial se tiene en cuenta, pues no se excluye aunque no se haya probado el grave riesgo del art. 13.1.b), de modo que si se produjera quedaría contrarrestado por la adopción de medidas de protección del menor que garantizarían un retorno seguro del mismo.

[86] *Guía de Buenas prácticas, op. cit.,* p. 27.

[87] Por ejemplo, en la mencionada SAP Alicante (sección 6ª), n. 208/2022, de 7 septiembre 2022, se pone de relieve por el tribunal español que "consta que por los tribunales polacos se han adoptado medidas adecuadas para garantizar la protección del menor, mediante la adopción de medidas cautelares con el fin de evitar riesgos para la vida y/o integridad de las menores, consistentes inicialmente en la prohibición de la comunicación con las menores y la madre, y posteriormente con la posibilidad de comunicación con la menor María Purificación , supervisada y en presencia bien del curador judicial designado, bien de la madre de la menor. Siendo las medidas de protección adoptadas suficientes para salvaguardar la integridad de las menores, sin perjuicio de otras que pudieran ser adoptadas en los procedimientos abiertos ante los tribunales polacos".

prohibir la entrada en lugares en los que ésta decida residir o que frecuente o bien prohibir cualquier tipo de contacto con ella; d) Incluso, determinar si se prevén otras disposiciones de protección en relación con aspectos como la fijación de una vivienda separada y segura tras el retorno[88].

En relación con la madre maltratada, uno de los mayores problemas será reconocer efectos a las medidas de protección que haya que adoptar en cuanto víctima, ya que deberá afrontar un "sistema jurídico arduo, complicado y en continua evolución, integrado por fuentes de diferente origen"[89]. En la práctica, la eficacia extraterritorial de las medidas de protección a las víctimas debe hacer frente a las dificultades derivadas de las diferencias entre los ordenamientos en lo que atañe a la regulación y tratamiento de la violencia de género. Estas diferencias conciernen tanto al modo de valorarlas y aplicarlas[90], como a su propia naturaleza (civil, administrativa, cautelar o penal)[91], su ámbi-

[88] *Proyecto de Guía de Buenas prácticas, op. cit.,* pp. 35 ss. En España las medidas de protección para víctimas de violencia de género se encuentran reguladas, entre otras, en los arts. 61 ss. de la Ley orgánica 1/2004, de 28 diciembre de medidas de protección integral contra la violencia de género. Tales medidas son compatibles con cualquier medida cautelar y de aseguramiento que pueda adoptarse en procesos civiles y penales (art. 61). Ver M. LLORENTE SÁNCHEZ-ARJONA, *Medidas cautelares en los procesos por violencia de género*, en M. LLORENTE SÁNCHEZ-ARJONA, R. ZAFRA ESPINOSA DE LOS MONTEROS, (dirs.), *La violencia de género en la sombra*, Madrid, 2023, pp. 261-288.

[89] P. BLANCO-MORALES LIMONES, *La eficacia internacional de las medidas de protección en materia de violencia de género,* en *Diario La Ley*, noviembre 2014, n. 8427, p. 826.

[90] Por ejemplo, tales diferencias se ponen de manifiesto con ocasión del asunto *Saada v. Golan 18-CV-5292 (AMD) (RML),* (Tribunal Primera Instancia de Estados Unidos, sentencia de 24 de enero de 2024, *Saada v. Golan 18-CV-5292 (AMD) (RML),* n. HC/E/US 1578, sobre una sustracción de un menor desde Italia a EE.UU. por una madre, nacional estadounidense, víctima de violencia y abusos por su marido italiano. Hasta llegar al Tribunal Supremo se discutió sobre el carácter y conveniencia de las medidas de protección del menor, hasta que finalmente se decidió que las medidas en Italia no podían garantizar el interés superior del menor y éste se exponía al riesgo grave del art. 13.1.b). Disponible en: http://www.incadat.com. Ver los comentarios de dicho caso de C. HONORATI, *Protecting Mothers against Domestic Violence in the Context of International Child Abduction: Between Golan v Saada and Brussels II-ter EU Regulation, Laws* 2023, 12 (5), p. 79; M. HERRANZ BALLESTEROS, *op. cit.,* pp. 14-17.

[91] Hay que distinguir, además, entre las medidas de protección, los arreglos prác-

to de protección o las autoridades competentes, que se convierten en el principal obstáculo para garantizar la eficacia extraterritorial de tales medidas[92]. A ello se añade la disparidad entre las legislaciones en la misma concepción y definición de la violencia de género[93], incluyendo aquéllas que ni siquiera incorporan un concepto de violencia de género, ni de violencia doméstica o familiar[94]. Pero, además, el hecho de que la orden de restitución, como también la norma sobre la compe-

ticos y los compromisos. De un lado, los arreglos prácticos los puede establecer un tribunal como parte de la orden de restitución para facilitar el regreso del menor. No están destinados a abordar una situación de grave riesgo y deben diferenciarse de las medidas de protección. De otro, los compromisos aluden a una "promesa, garantía o aserción voluntaria" realizada ante un tribunal por el progenitor privado del menor, "de hacer o no hacer determinadas cosas" y que en el contexto de un proceso de restitución "puede tener, o no, fuerza ejecutiva en el Estado al cual se restituirá al niño". Las "medidas de protección" se entienden "en un sentido amplio y hace referencia a las medidas disponibles para abordar una situación de grave riesgo". *Guía de buenas prácticas, op. cit.,* pp. 9 y 11. Asimismo, téngase en cuenta que hay Estados contratantes del Convenio de La Haya 1980 en los que existe una práctica para que las órdenes de restitución se sujeten al cumplimiento de requisitos o compromisos específicos. Para asegurar que tales medidas de protección sean ejecutables, se puede exigir al solicitante que las registre en términos idénticos o equivalentes en el Estado de residencia habitual del menor. Suele hablarse de órdenes de "restitución segura" u "órdenes espejo". Para una consulta de dichos Estados ver https://www.incadat.com/es/convention/case-law-analysis.

[92] Ver T. FREIXES, L. ROMÁN, *Protección de las víctimas de violencia de género en la Unión Europea. Estudio preliminar de la Directiva 2011/99/UE sobre la orden europea de protección*, Tarragona, URV, UAB, 2014, pp. 14-17.

[93] La violencia de género se ha tratado durante mucho tiempo como un "problema personal e íntimo" en bastantes países de la UE. Por ejemplo, Bulgaria, Hungría, Luxemburgo, Letonia y Eslovenia en 2015 no habían hecho ninguna encuesta específica sobre la incidencia de la violencia. Mientras en España existe desde hace años una tipificación concreta, realizándose un recuento de los asesinatos de mujeres, en otros como Austria se ha seguido hablando de "traumas familiares" y no de violencia machista, o de "asesinatos de honor" cuando la víctima era una mujer musulmana., según indica M.A. VERDEJO ESPINOSA (coord.), *Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención*, Sevilla, Universidad Internacional de Andalucía, 2015, p. 135.

[94] Ver V. MERINO, *La concepción de la violencia de género en los ordenamientos de los Estados miembros,* en T. FREIXES, L. ROMÁN, (dirs.), O. OLIVERAS, R. VAÑÓ (coords.), *La Orden Europea de Protección. Su aplicación a las víctimas de violencia de género*, Madrid, 2015, pp. 50-58.

tencia judicial de los Tribunales de la residencia habitual anterior al acto ilícito, se base en dicha residencia (art. 9 reglamento Bruselas II ter)[95], se convierte en realidad en una baza del maltratador, al colocar de nuevo a la víctima en su territorio – si es que decide regresar – y, de este modo, el Estado y los poderes públicos se convierten en cómplices de que se perpetúe la violencia[96].

En la mejora del régimen regulador de las medidas de protección será importante la correcta utilización del reglamento (UE) 606/2013 sobre la Orden Europea de Protección (OEP) en supuestos de violencia contra las mujeres, regulada por la directiva (UE) 2011/99[97]. Sin olvidar las diferencias entre ambos textos (el primero sobre medidas dictadas de ámbito penal y en la directiva, en cambio, de ámbito civil). También otras normas como la directiva (UE) 2012/29, de 25 octubre,

[95] Al hilo del asunto *MCP* (Tribunal de Justicia, sentencia de 24 de marzo de 2021, *SS v. MCP,* en el asunto n. C-603/20 PPU-MCP, el TJUE ha recordado que este foro fue el resultado de un delicado equilibro entre, "por un lado, la necesidad de evitar que el sustractor obtenga un beneficio de su acto ilícito y, por otro lado, la conveniencia de permitir que el órgano jurisdiccional más próximo al menor conozca de las acciones relativas a la responsabilidad parental". Ver H. VAN LOON, *The Brussels IIa Regulation: towards a review?, en Parlamento Europeo, Cross-border activities in the EU- Making life easier for citizens, Workshop for the JURI Committee*, *Directorate General for internal policies. Policy Department C: Citizens' Rights and Constitutional Affairs*, 2015, pp. 178-207 disponible en: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/510003/IPOL_STU(2015)510003_EN.pdf, p. 185; M. GONZÁLEZ MARIMÓN, *Competencia judicial internacional ante un caso de sustracción internacional de menores de un Estado miembro de la UE a un Estado tercero: comentario a la STJUE de 24 de marzo de 2021*, en *Revista General de Derecho Europeo,* 2021, n. 55, pp. 229-244; B. CAMPUZANO DÍAZ, *La propuesta de reforma del Reglamento 2201/2003: ¿se introducen mejoras en la regulación de la competencia judicial internacional?,* en M. GUZMÁN ZAPATER, C. ESPLUGUES MOTA (dirs.), *Persona y familia en el nuevo modelo español de Derecho internacional privado*, Valencia, 2017, pp. 91 y ss.

[96] Ver M. REQUEJO ISIDRO, *op. cit*., p. 185.

[97] Directiva (UE) 2011/99 del Parlamento europeo y del Consejo, sobre la orden europea de protección, de 13 de diciembre de 2011, en DOUE 338 de 21 de diciembre de 2011, pp. 2-18.

de protección de la víctima de delito[98] y en España la Ley 4/2015, de 27 de abril, del Estatuto de la víctima[99].

En la práctica, el reglamento (UE) 606/2013 no debería interferir en la aplicación del reglamento Bruselas II ter. Las decisiones adoptadas conforme a este último se reconocerán y ejecutarán conforme a sus reglas. No obstante, la coordinación entre ambos reglamentos y la directiva puede no ser tan sencilla. La heterogeneidad de las medidas de protección en violencia de género entre los Estados miembros, reflejo de sus propias tradiciones jurídicas y culturales, genera problemas a la hora de homologar la protección de las víctimas. Además, la diversidad existente entre las regulaciones penales y la complejidad del procedimiento de reconocimiento mutuo previsto por la directiva restarán también efectividad práctica a la OEP, que dependerá de la actitud y disposición a colaborar entre los Estados miembros y la coordinación ejercida desde la UE[100]. Habrá que evitar situaciones en las que se dicte una orden de retorno del menor por no haberse podido demostrar a tiempo, en el país en que el menor está retenido, la situación de violencia producida en el país de la residencia habitual anterior al acto ilícito y no se haya reconocido a tiempo una OEP emitida contra el supuesto maltratador. De ahí la relevancia de de un marco reforzado y efectivo de cooperación interestatal.

La directiva (UE) 2024/1385 insiste en la necesidad de garantizar la protección de las víctimas, para lo que es esencial que las autoridades competentes y organismos pertinentes (no limitados a autoridades policiales y judiciales) participen en la evaluación de los riesgos a que están expuestos las víctimas, así como las medidas de apoyo adecuadas. Ello debe realizarse con base en unas directrices claras elaboradas por los Estados miembros que tengan en cuenta los factores sobre los que evaluar el riesgo que emana del autor o sospechoso. En este sentido, se considera relevante que las autoridades revisen periódicamente

[98] Directiva (UE) 2012/29 del Parlamento europeo y del Consejo, por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y por la que se sustituye la Decisión marco 2001/220/JAI del Consejo, de 25 de octubre de 2012, en DOUE 315, de 14 de noviembre de 2012, pp. 57-73.

[99] Ley 4/2015, del Estatuto de la víctima del delito, de 27 de abril, en BOE 101 de 28 de abril de 2015.

[100] T. FREIXES, L. ROMÁN, *op. cit.,* p. 17.

dicho riesgo, por ejemplo, en momentos importantes del proceso, como el inicio de éste, o cuando se dicte sentencia o una orden o, incluso, en el contexto de procedimientos de revisión del régimen de custodia o visita del menor[101]. El mayor desafío en la práctica será compatibilizar la adopción de medidas de protección del menor y de la madre víctima de violencia, tras volver ambos al país de residencia habitual anterior de la sustracción: el país en el que reside el autor de la violencia ejercida sobre la madre y/o sus hijos/as. Dicha compatibilización exige, no sólo un esfuerzo entre las autoridades estatales involucradas en todo el proceso, sino también un cambio de mentalidad y actitud en muchos casos. Un cambio que conecta con la reflexión realizada al final de este capítulo.

Por último, aunque brevemente, hay que mencionar que en el ámbito de las medidas de protección de las víctimas de violencia de género se ha valorado la posibilidad de emplear algoritmos predictivos, como los realizados por la policía en tareas de prevención o en la fase investigación de un proceso a través, por ejemplo, del sistema VioGen en España. Este sistema constituye el algoritmo más desarrollado que utilizan las fuerzas y cuerpos de seguridad españolas. Su protocolo permite que los agentes valoren el riesgo que tiene una mujer – que ya ha denunciado – de sufrir una nueva agresión por su pareja o expareja. Recientemente en enero de 2025 los ministerios del interior y de igualdad han presentado el nuevo Sistema VioGen2, plataforma di-

[101] Es importante señalar que la directiva destaca algunas medidas en relación con la protección de mujeres y menores. (arts. 14-24). Se insiste en que los Estados miembros se aseguren de que las víctimas puedan denunciar actos de violencia a las autoridades competentes a través de canales fáciles de usar y seguros, con posibilidad de denunciar en línea o a través de otras TIC accesibles y seguras, sin perjuicio de las normas procesales nacionales relativas a la formalización de denuncias en línea, incluyendo la posibilidad de aportar pruebas por tales medios. Pero, además, han de velar por que, cuando el titular de la patria potestad esté implicado en el acto de violencia, "la capacidad de un menor para denunciar el acto no esté supeditada al consentimiento del titular de la patria potestad y por que las autoridades competentes adopten las medidas necesarias para proteger la seguridad del menor antes de que dicha persona sea informada de la denuncia" (art. 14). Estas medidas podrán incluir las siguientes: a) las medidas previstas en los artículos 23 y 24 de la directiva (UE) 2012/29; b) acordar órdenes urgentes de alejamiento, de prohibición o de protección (art. 19) y otras medidas distintas.

gital de nuevo cuño que incorpora la tecnología más avanzada en la materia, y el Protocolo 2025, que aglutina y actualiza todas las novedades introducidas por las sucesivas Instrucciones dictadas por la Secretaría de Estado de Seguridad desde 2018[102]. VioGén2 incorpora nuevos indicadores en los formularios de valoración del riesgo y una mejor calibración de los algoritmos que determinan dichos niveles, lo que reduce el riesgo de error en la valoración realizada[103].

Tales herramientas – mediante algoritmos predictivos – se podrían usar en el marco de un proceso (concretamente penal), con vistas a predecir la reincidencia de un sujeto, tal como ocurre en países como EEUU. Se trataría, por lo tanto, de que el juez pudiera calcular el riesgo de reincidencia del sujeto autor de la violencia en el momento de decidir determinadas medidas cautelares, teniendo en cuenta la peligrosidad de dicho sujeto. Teniendo en cuenta que estos sistemas algorítmicos analizan resoluciones pasadas e identifican qué situaciones han llevado a determinados resultados, la decisión que adoptara el juez tendría en cuenta todas estas cuestiones. Ahora bien, entre las dudas que suscita el uso de estas herramientas predictivas en la justicia penal

[102] Para adoptar una orden de protección en España debe identificarse si existe una "situación objetiva de riesgo para la víctima", para lo cual las fuerzas y cuerpos de seguridad españolas disponen del mencionado Sistema VioGen. El sistema nace en 2007 como resultado de aplicar los arts. 31.3 y 32 de la LO 1/2004 sobre Violencia de género y su objetivo principal es promover medidas policiales de protección a mujeres víctimas de violencia y menores a su cargo. La Instrucción 1/2025, de la Secretaría de Estado de Seguridad, por la que se establece un nuevo protocolo para la valoración y gestión policial del nivel de riesgo de violencia de género y seguimiento de los casos a través del sistema VioGén-2 sustituirá a la anterior Instrucción 4/2019 y entrará en vigor a partir del 30 de junio de 2025.

[103] Disponible en: https://www.interior.gob.es/opencms/es/detalle/articulo/Interior-disena-un-nuevo-modelo-de-respuesta-policial-a-la-violencia-degenero/ En relación con la ciberviolencia de género, se establece que "cuando se detecten este tipo de conductas mediante amenazas, coacciones, acoso u otras formas de agresiones, se pondrá especial atención en la tramitación de los atestados siempre conforme al presente Protocolo, incluyendo la valoración policial de riesgo. En estos supuestos será preceptivo, en el tratamiento de las evidencias digitales, que se observen todas las garantías y se adopten las medidas oportunas para asegurar su adecuada recogida, preservación y custodia, lo que permitirá su presentación en el proceso judicial como elemento probatorio".

está la posible existencia de sesgos en sus resultados, que pueden atentar el principio de igualdad, al replicar estereotipos de género[104].

4. *Valoración final. Dificultades continuadas en la lucha contra el patriarcado, también en la cooperación judicial digitalizada*

Nos hemos referido ampliamente al desafío principal en la lucha contra la violencia machista en el ámbito de la sustracción de menores, centrado principalmente en las diferencias procedimentales entre los Estados y aspectos como la prueba de la violencia, la celeridad de los procedimientos o las medidas de protección (del menor y de la madre). Aspectos que pueden complicarse cuando dicha violencia se realiza de forma digital.

Queremos terminar refiriéndonos a un segundo desafío, más delicado y complejo, al que se enfrenta dicha lucha. Un desafío que alude a un problema aparentemente invisible, pero profundamente arraigado y difícil de eliminar. Nos referimos a la insensibilidad que se observa muchas veces en la actuación de las autoridades, organismos y, en general, operadores jurídicos en todo este contexto. Dicha actuación responde a una visión de la mujer anclada en estereotipos, típica de una sociedad patriarcal como la nuestra, que poco a poco debe desaparecer. La violencia institucional es una modalidad más de violencia de género que debe evitarse y combatirse por todos los medios[105].

[104] Ampliamente, E. MARTINEZ GARCÍA, *Justicia e inteligencia artificial sin género,* en S. BARONA VILAR (ed.), *Justicia algorítmica y neuroderecho*. Valencia, 2021, pp. 209-227; A. MONTESINOS GARCÍA, *Algoritmos predictivos y perspectiva de género en el proceso penal, IDP*, 2023, n. 39, pp. 1-11; N. MACCHIAVELLI, *La violencia de género y el uso de algoritmos como herramienta efectiva para la protección de los derechos fundamentales",* en *Anuario de filosofía del derecho*, 2022, XXXVIII, pp. 59-74; R. BORGES BLÁZQUEZ, *Algoritmización de la concesión de medidas cautelares en el proceso penal para la protección de víctimas de violencia de género. ¿Es capaz Viogen de interpretar el "periculum in mora"?,* en *Actualidad Jurídica Iberoamericana,* agosto 2024, n. 21, pp. 384-407.

[105] A este respecto la directiva 2024/1385/UE, *cit.* p. 1 y ss. recuerda que "La violencia contra las mujeres es una manifestación persistente de la discriminación estructural contra las mujeres, resultado de relaciones de poder históricamente desiguales entre mujeres y hombres" (...). "Hunde sus raíces en los roles, comportamientos, acti-

La perspectiva de género en la regulación – europea, internacional e interna – y en su interpretación y aplicación es urgente. De lo contrario, volverán a producirse acusaciones como las que tuvieron lugar con ocasión del célebre asunto *González Carreño c. España* en que el Comité para la eliminación de la discriminación contra la mujer (CEDAW) acusó a España de seguir un patrón de actuación que "obedece a estereotipos y minimiza la situación de las víctimas de violencia doméstica colocándolas en una situación de especial vulnerabilidad"[106].

De nuevo, el 9 de diciembre de 2021, las Naciones Unidas reclamaron al Gobierno español que hiciera más, "para proteger a los niños de la violencia doméstica y los abusos sexuales, garantizar que sus tribunales superen los prejuicios contra las mujeres y aplicar un enfoque centrado en los niños y de género"[107]. Al hilo de dicha reclamación en España la *Asociación de Mujeres Juezas* hizo un llamamiento el 10 de diciembre de 2021, para "que se adopten las medidas necesarias para asegurar el efectivo cumplimiento de la normativa de protección a la infancia y adolescencia contra cualquier forma de violencia**,** entre ellas la inclusión de la utilización del Síndrome de Alienación Parental como forma de violencia de género en la Ley 1/2004 de Medidas de Protección Integral contra la Violencia de Género", en línea con la LO 8/2021 de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia (arts. 11.3 y 26.3.a)[108].

Se trata, en definitiva, de evitar respuestas judiciales en que la madre sustractora víctima de violencia de género es percibida como "hostil y manipuladora"[109] o como en el caso de *Juana Rivas*, "que

vidades y atributos construidos socialmente que una sociedad determinada considera adecuados para las mujeres y para los hombres. Por tanto, se debe tener en cuenta una perspectiva que tome en consideración el género al aplicar la presente Directiva" (considerando 10).

[106] Dictamen de 16 de julio de 2014 del Comité para la Eliminación de la Discriminación contra la Mujer en virtud del Protocolo Facultativo de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer (Comunicación número 47/2012).

[107] Disponible en: Http://www.ohchr.org

[108] Disponible en: Http://www.mujeresjuezas.es

[109] Ver M. KAYE, *op. cit*., pp. 197-198 y M. REQUEJO ISIDRO, *op. cit*., p. 185.

no muestra haberse arrepentido" o que es "una madre indigna"[110].

Urge combatir estos problemas – visibles e invisibles – que acechan a la violencia machista en el ámbito de la sustracción internacional de menores, y más allá de éste. Sólo así se podrá avanzar en situar "la dignidad humana en el corazón de la ley desde un compromiso con la solidaridad social"[111]. Es más, en un contexto tan específico como el que hemos analizado dicho avance debe propulsarse con el derecho internacional privado como herramienta jurídica y con un compromiso desde y con el feminismo.

Acorde con tales compromisos – solidaridad social y feminismo – es necesario propulsar una digitalización eficiente de la cooperación judicial, por ahora en el ámbito de la UE, aunque sean aún muchas las dificultades tecnológicas de la digitalización de la justicia y de los procedimientos judiciales. El éxito en dicha digitalización puede ser muy útil en los procedimientos sobre sustracción de menores, incluidos los producidos por una madre víctima de violencia machista. Tras más de una década fomentando el uso de la comunicación digital con diferentes instrumentos, parece que la refundición del reglamento (UE) 2020/1783 (notificaciones) y el reglamento (UE) 2020/1784 (prueba) puede suponer un avance hacia la obligatoriedad de los medios digitales de comunicación[112]. La consolidación con el tiempo del sistema e-Codex puede apoyar la digitalización a nivel técnico que, sin duda, se verá reforzada con el reglamento (UE) 2023/2844 sobre la digitalización de la cooperación judicial, al potenciar los medios electrónicos de comunicación, facilitar las videoconferencias y validar los documentos y firmas electrónicos. Mecanismos que resultan esenciales para una co-

[110] En Diario *El País*, el 16 de diciembre de 2021, *Cuatro catedráticos de penal diseccionan el auto de Juana Rivas: "Lo del Juez Piñar es gravísimo, supura veneno*, disponible en: www.elpais.com Para un análisis del caso, L.A. PÉREZ MARTÍN, *Protección de los menores en el ámbito internacional: Reflexiones sobre la sustracción internacional de menores y la violencia de género en torno al caso de Juana Rivas*, en V. BASTANTE GRANELL (coord.), *La protección del menor: Situación y cuestiones actuales*, Granada, 2019, pp. 73-88.

[111] Siguiendo a Henri Battifol, como recuerda H. MUIR WATTS, *Batiffol*, en J. BASEDOW y Otros (eds.), *Encyclopedia of Private international law*, Cheltenham, UK, 2017, vol. 1, p. 170.

[112] Ver X. KRAMER, *op.cit.,* p. 6.

rrecta y ágil tramitación de un procedimiento como el de sustracción de menores, que permita ponderar justamente los intereses implicados según el supuesto litigioso, tanto si ha existido violencia contra la parte sustractora como sino.

El éxito del proceso de digitalización de la justicia debe, en todo caso, verse acompañado de una visión de género, lejos de estereotipos y al servicio de la protección efectiva de la víctima[113]. De hecho, la directiva (UE) 2024/1385 alude entre las directrices para las autoridades competentes "detectar y evitar los estereotipos de género"[114]. De igual modo, el *Informe GREVIO, España, 2024*[115] anima a las autoridades españolas a "seguir promoviendo los principios de igualdad entre mujeres y hombres, los roles de género no estereotipados, el respeto mutuo y la resolución no violenta de conflictos en las relaciones interpersonales".

De no ser así, una madre víctima de violencia machista como ha sido *Juana Rivas*, que ha escapado de su maltratador huyendo con sus hijos de Italia a España, seguirá soportando los obstáculos de una justicia todavía lenta y patriarcal. La digitalización debe evolucionar con los tiempos y ello incluye una perspectiva de igualdad y de equilibrio de los intereses en juego.

[113] Ver el interesante análisis de N. IGAREDA, *El derecho a la libertad versus la libertad de expresión en la machosfera,* en *Derecho y Género,* 2024, n. 1, pp. 56-79, así como I. CROSAS REMÓN Y P. MEDINA-BRAVO, *Ciberviolencia en la red. Nuevas formas de retórica disciplinaria en contra del feminismo*, en *Papers*, 2019, n. 104(1), pp. 47-73.

[114] Art. 21, h).

[115] Informe GREVIO 2024, esto es, *Grupo de Expertos sobre la Acción contra la Violencia hacia las Mujeres y la Violencia Doméstica*, *Convenio del Consejo de Europa para prevenir y combatir la violencia contra las mujeres y violencia doméstica (Convenio de Estambul),* publicado el 21 de noviembre de 2024 (disponible en: www.coe.int/conventionviolence). En él se analizan los avances realizados en la prestación de apoyo, protección y justicia a las víctimas de la violencia contra las mujeres y la violencia doméstica (p. 54).

Abstract

La ciberviolencia ejercida contra las mujeres se manifiesta también en un fenómeno como es el de la sustracción internacional de menores cometida por la madre que es víctima de dicha violencia. En este contexto, el ciberacoso (*cyberharassment*) y el ciberacecho (*cyberstalking*) pueden ser formas de ejercer la violencia machista contra la madre sustractora y/o sus hijos/as por parte del maltratador, como consecuencia del impacto de la tecnología en el ejercicio de la violencia en un entorno familiar. El combate de esta violencia debe integrarse hoy en el proceso de digitalización de la cooperación judicial que, en el ámbito específico de la UE, se ha visto propulsado en los últimos tiempos y que puede tener repercusiones relevantes sobre un procedimiento de retorno – o no – del menor sustraído ilícitamente por su madre. Son numerosos los desafíos a los que dicho combate se enfrenta.

PALABRAS CLAVE: Ciberviolencia contra la mujer – Sustracción internacional de menores – Cooperación judicial digitalizada – Convenio de La Haya 1980 – Reglamento (UE) 2019/1111

CYBERVIOLENZA CONTRO LE DONNE E COOPERAZIONE GIUDIZIARIA DIGITALIZZATA NEI PROCEDIMENTI DI SOTTRAZIONE INTERNAZIONALE DI MINORI

La cyberviolenza contro le donne si manifesta anche nel fenomeno della sottrazione internazionale di minori commessa dalla madre vittima di tale violenza. In questo contesto, il *cyberharassment* e il *cyberstalking* possono essere forme di violenza maschilista contro la madre rapitrice e/o i suoi figli da parte del maltrattante, come conseguenza dell'impatto della tecnologia nell'esercizio della violenza in ambito familiare. La lotta contro questa violenza deve ora essere integrata nel processo di digitalizzazione della cooperazione giudiziaria che, nel settore specifico dell'UE, è stato promosso negli ultimi tempi e che può avere ripercussioni rilevanti su una procedura per il ritorno – o meno – del bambino illecitamente rapito dalla madre. Le sfide che questa lotta deve affrontare sono numerose.

KEYWORDS: Cyberviolenza contro le donne – sottrazione internazionale di minori – cooperazione giudiziaria digitalizzata – Convenzione dell'Aia del 1980 – regolamento (UE) 2019/1111

UNA (RE)VISIÓN CONSTITUCIONAL DE LOS DERECHOS CLÁSICOS Y EMERGENTES ANTE NUEVAS FORMAS DE CIBERVIOLENCIA CONTRA LA MUJER

*Mónica Martínez López-Sáez**

SUMARIO: 1. Apuntes preliminares en aras a la contextualización, a la claridad conceptual y a la perspectiva de género. – 2. El régimen constitucional de los derechos personalísimos ante nuevos riesgos digitales. – 2.1. Breves premisas acerca de la redefinición/protección reforzada de "viejos derechos" y el reconocimiento de "nuevos derechos". – 2.2. Los derechos personalísimos en el ordenamiento constitucional español. – 2.3. El derecho a la intimidad y el derecho a la protección de datos: dos derechos autónomos pero interconectados en el entorno digital. – 3. Análisis casuístico: la sextorsión como supuesto de ciberviolencia contra la mujer y garantías para la tutela de sus derechos. – 3.1. Aproximación a la problemática social y jurídica. – 3.2. El derecho al olvido como garantía específica para la protección efectiva de la dignidad de la víctima de ciberviolencia – 4. Reflexiones finales.

1. *Apuntes preliminares en aras a la contextualización, a la claridad conceptual y a la perspectiva de género*

La violencia contra las mujeres se considera un problema de "salud pública mundial de proporciones epidémicas"[1], que sigue siendo "símbolo brutal de la desigualdad" y una "clara manifestación de dis-

* Profesora Ayudante Doctora en Derecho constitucional, Universidad de València, e-mail: monica.martinez-lopez@uv.es Esta contribución es un desarrollo, actualización y re-enfoque del artículo M. MARTÍNEZ LÓPEZ-SÁEZ, *Propuestas de regulación frente a una nueva brecha digital por razón de género: ciberviolencia contra la mujer a la luz del marco europeo de protección de datos*, en *Revista de Estudios Jurídicos y Criminológicos,* 2021, n. 4, pp. 211-233.

[1] OMS, *Resumen de orientación Estimaciones mundiales y regionales de la violencia contra la mujer: prevalencia y efectos de la violencia conyugal y de la violencia sexual no conyugal en la salud*, Ginebra, 2013, p. 1.

criminación"[2]. Los estudios a nivel europeo confirman ya no sólo las desigualdades entre hombres y mujeres en ámbitos como el laboral, sino que se han materializado en todos los ámbitos, de naturaleza pública o privada, demostrando los atentados contra la salud, la seguridad y la autonomía de las mujeres y niñas desde hace décadas[3].

Los resultados de la segunda *Encuesta sobre violencia de género en la UE*[4] no sólo confirman lo que confirmaba la primera[5] y así como los datos a nivel mundial[6], sino que ya no deja lugar a dudas sobre la urgente necesidad de combatir la violencia contra las mujeres: en la UE, una de cada tres mujeres (el 30,7 %) han sufrido violencia física o amenazas y/o violencia sexual por parte de algún agresor, fuera pareja o expareja o no tuviera relación sentimental con ella) a lo largo de su vida, y, en un porcentaje sorprendentemente similar, una de esas tres (el 30,8%) han sufrido acoso sexual en el trabajo a lo largo de su vida.

La cantidad de mujeres que sufren violencia, en general, y violencia digital, en particular, ocurre, en parte, como resultado de las ideas socio-culturales sobre el sexo y los roles y actitudes que le corresponden. Para muestra, un botón: las investigaciones realizadas hasta la fecha reflejan que las mujeres y niñas son las principales víctimas de las manifestaciones más graves de la violencia facilitada por las Nuevas Tecnologías de la Información y la Comunicación (en adelante, las

[2] M.J. RIDAURA MARTÍNEZ, *El sentido actual de la Ley Orgánica de Medidas de Protección Integral contra la Violencia de Género*, en M. MARTÍN (a cura di), *Estudio Integral de la Violencia de Género: un análisis teórico-práctico desde el Derecho y las Ciencias Sociales,* Valencia, 2018, p. 138.

[3] Agencia de Derechos Fundamentales de la UE, *Violencia de género contra las mujeres: una encuesta a escala de la UE. Resumen de las conclusiones,* Luxemburgo, 2014.

[4] Agencia de Derechos Fundamentales de la UE, *Encuesta sobre violencia de género en la UE - Principales resultados. Experiencias de las mujeres en la UE-27,* Luxemburgo, 2024. Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/eu-gender_based_violence_survey_key_results.pdf

[5] *Supra,* cit., n. 4.

[6] OMS, *Resumen de orientación Estimaciones mundiales y regionales de la violencia contra la mujer: prevalencia y efectos de la violencia conyugal y de la violencia sexual no conyugal en la salud*, Ginebra, 2021, https://www.who.int/es/news-room/fact-sheets/detail/violence-against-women.

NTIC)[7]. De tal forma que la violencia de género, incluida la discriminación, el acoso y agresión sexual o emocional, etc., ahora también se comete, se facilita y se propaga en el mundo virtual: "el fenómeno de las redes sociales y la mensajería instantánea provocará […]una amplificación de las conductas coercitivas, una extensión del control y la manipulación, así como la persistencia y […] presencia del agresor […] que le produce a la víctima una sensación de desamparo e impotencia ante los hechos […] que está sufriendo […] una grave alteración en su salud física y mental y […]su vida cotidiana"[8].

Las NTIC permiten una transmisión de datos e información constantes y han creado un escaparate panóptico abierto al mundo, todo lo cual ha cambiado la forma de relacionarnos con el mundo e incluso han cambiado la forma de concebir la intimidad o la propia imagen. Las NTIC no sólo tienen el poder y potencial de conexión, apertura, progreso, sino también de reforzar y difundir determinadas estructuras que impactan negativamente a ciertos colectivos, incluidas las mujeres[9]. La revolución tecnológica y la transformación digital han traído no sólo nuevas maneras de relacionarse con los demás o nuevas formas de comunicación y reivindicación social hacia la igualdad entre hombres y mujeres, sino también nuevas formas de atacar y silenciar a las mujeres[10].

Los comportamientos y fenómenos sociales dañinos que observamos en nuestro día a día se vierten en la Red, y esta, por su propia naturaleza, los intensifica y agrava su alcance y consecuencias. Esta nueva realidad, llamada por algunos como "ciberviolencia de género"[11], es

[7] Instituto Europeo de la Igualdad de Género, *Cyber violence against women and girls*, Luxemburgo, 2017, p. 3.

[8] R. SALA ORDOÑEZ, *L'estat embrionari de la violència de gènere digital*, en *Món Jurídic, Revista de l'il·Lustre Col·Legi de l'advocacia de Barcelona,* 2019, n. 323, pp. 20-21.

[9] B. YALCINOZ-UCAN, H. ESLEN-ZIYA, *Disclosing gender-based violence online: strengthening feminist collective agency or creating further vulnerabilities?* en *Feminist Media Studies*, 2023, n. 24 (5), pp. 1186-1203.

[10] AA. VV., *Intimate Partner Violence, Risk and Security: Securing Women's Lives in a Global World*, Nueva York y Oxon, 2018.

[11] M.S. QUESADA AGUAYO, *La violencia de género y el ciberacoso en las redes sociales: análisis y herramientas de detección*, en M. A. VERDEJO (a cura di), *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención*, Sevilla, 2015, p. 148.

solo una manifestación añadida y ampliada del paradigma sociocultural existente trasladado a la cultura online, convirtiéndose la red en herramienta para la opresión y abuso hacia las mujeres: "el fenómeno de las redes sociales y la mensajería instantánea provocará en estos patrones de conducta una amplificación de las conductas coercitivas, una extensión del control y la manipulación, así como la persistencia y […] presencia del agresor […] que le produce a la víctima una sensación de desamparo e impotencia ante los hechos […] que está sufriendo […] una grave alteración en su salud física y mental y […] en gran medida su vida cotidiana"[12].

Por todo lo anterior, resulta necesario centrar nuestra atención, cuando hablamos de la aparición de nuevas formas de "violencia digital"[13], en aquella ejercida mediante la divulgación de información personalísima y la materialización de determinados comportamientos hostiles que producen daños a nivel físico y psicológico, desde la perspectiva de género.

En efecto, la innovación y transformación tecno-digital, sobre todo en lo que al acceso instantáneo y constante a la información, comunicación o incluso a la geolocalización, se refiere, han creado oportunidades singulares para perpetrar actos precursores o propios de este tipo de violencia. Además, la velocidad y universalidad en la difusión, acceso y perdurabilidad de contenidos sensibles y datos personales ha otorgado a los maleantes una gran facilidad para poner en entredicho la seguridad e intimidad de las mujeres, en muchos casos, mediante la vigilancia constante y conductas dañinas a distancia. Con todo lo anterior, se puede apreciar cómo el mundo virtual, en tanto que reflejo del mundo real, está plagado de desigualdades. Como bien apunta Llorente Sánchez-Arjona: "resulta paradójico" que habiendo avanzado como Estado democrático, se "mantenga la esencial de la cultura patriarcal" y se sigan reproduciendo "comportamientos claramente atentatorios contra la igualdad de género"[14].

[12] R. SALA ORDOÑEZ, *L'estat embrionari de la la violència de gènere*, cit., pp. 20-21.

[13] Así lo llama, por ejemplo, la Agencia Española de Protección de Datos en sus recomendaciones *Ayuda a las víctimas de violencia de género y violencia digital,* https://www.aepd.es/es/areas-de-actuacion/recomendaciones

[14] M. LLORENTE SÁNCHEZ-ARJONA, *La ciberviolencia de género: nuevas formas de*

De tal forma que a la desafortunadamente "clásica" desigualdad entre hombres y mujeres tenemos que añadirle una suerte de "brecha digital por razón de género", que entendemos en este y otros trabajos[15] como el traslado de las desigualdades, estereotipos y actos de violencia que sufren las mujeres, por el mero hecho de ser mujer, al ámbito digital. Esta nueva brecha digital por razón de género incluye conductas de diversa índole: desde insultos, chistes o rumores publicados y diseminados en la Red, revelación y difusión de información personal (en ocasiones íntima), hasta la exclusión, intimidación, incitación al odio en las redes o prácticas vinculadas al ciberacoso, ciberacecho, cibercontrol o sextorsión.

La necesidad de estudiar la violencia digital desde esta perspectiva concreta de género tiene su fundamento, por un lado, viendo los datos estadísticos y las investigaciones realizadas hasta la fecha que confirman que las mujeres y niñas son las principales víctimas de las manifestaciones más graves de la violencia digital[16] y, por otro lado, debido a los estereotipos y prejuicios sociales que siguen vigentes.

Al igual que a nivel mundial, la violencia de género en Europa afecta de manera desproporcionada a las mujeres, revelando patrones desiguales y discriminatorios, y comprende no sólo el ejercicio de actos físicos o psicológicos presenciales sino también aquellos actos que tienen cabida a través de las NTIC. A esto se le añade que tanto las causas como las consecuencias de este fenómeno se deben, en gran medida, a expectativas obsoletas, estereotipos y prejuicios de lo que es mas-

victimización, en C. ARANGÜENA FANEGO, M. DE HOYOS SANCHO, E. PILLADO GONZÁLEZ (dirs.), *El proceso penal ante una nueva realidad tecnológica europea,* Valencia, 2023, p. 414.

[15] V. FERREIRO, *La brecha digital digital, una nueva forma de discriminación hacia las mujeres. La toma de decisión en los usos de internet*, Palma, 2014.

[16] J. FLORES FERNÁNDEZ, *Privacidad, factor de riesgo y protección en la violencia digital contra las mujeres*, en M. A. VERDEJO (a cura di), *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención* Sevilla, 2015, p. 313; V. J. VILLANUEVA-BLASCO, S. SERRANO-BERNAL, *Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género*, en *Revista de Psicología y Educación*, 2019, vol. 14, n. 1, p. 23; todo ello confirmado con estadísticas mundiales: OCDE, *Report: Bridging The Digital Gender Divide. Include. Upskill. Innovate,* 2018, p. 23, https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf.

culino y femenino[17], a la normalización de la hipersexualización y cosificación de la mujer, y, en última instancia, a una jerarquización sociocultural que ha creado relaciones (inequitativas) de poder[18].

Las conductas supracitadas se han englobado por el conocido término "ciberviolencia de género", aunque en este caso hemos optado por el término "ciberviolencia contra la mujer", con el fin de abarcar otros supuestos en los que la mujer, fuera del ámbito sentimental, se encuentra igualmente afectada. Tal y como ya establecimos en otro lugar, podríamos definir violencia contra las mujeres, como una categoría concreta de patrones y conductas violentas y coercitivas dirigidas contra la mujer por el mero hecho de serlo, y que resulta o puede resultar en un daño físico, psicológico, económico, o de cualquier otro tipo de sufrimiento. Si bien no existe una definición común ni universalmente reconocida, las definiciones, tanto en el ámbito internacional como europeo, son compatibles con esta idea[19]. De hecho, la directiva objeto de esta obra[20], lo define en términos similares: "todo acto de violencia de género dirigido contra una mujer o una niña por el hecho de ser mujer o niña, o que afecten de manera desproporcionada a mujeres o niñas, que causen o sea probable que causen daños o sufrimientos de naturaleza física, sexual, psicológica o económica, incluidas las amenazas de realizar tales actos, la coacción o la privación arbitraria de libertad, tanto si se producen en la vida pública como en la vida privada"[21].

Con independencia de los matices de su conceptualización, la violencia contra la mujer indudablemente constituye una discriminación y

[17] M. S. QUESADA AGUAYO, G*énero y discriminaciones asociadas al hecho de ser mujer,* en M. ROMÁN (a cura di), *Manual Agentes de Igualdad,* Sevilla, 2009, pp. 30-42.

[18] M. S. QUESADA AGUAYO, *La violencia de género y el ciberacoso,* cit., p. 133.

[19] A nivel europeo (entendido en su sentido más amplio), se ha definido como los *"actos de violencia basados en el género que implican o pueden implicar para las mujeres daños o sufrimientos de naturaleza física, sexual, psicológica o económica, incluidas las amenazas de realizar dichos actos, la coacción o la privación arbitraria de libertad, en la vida pública o privada"*. Vid. art. 3(a) del Convenio de Estambul del Consejo de Europa.

[20] Directiva (UE) 2024/1385 del Parlamento europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, de 14 de mayo de 2024, en DOUE 1385 de 24 de mayo de 2024, pp. 1-36.

[21] Vid. art. 2(a) de la directiva (UE) 2024/1385, cit.

una violación generalizada del disfrute de los derechos más fundamentales y personalísimos de este colectivo, menoscabados especialmente por el abuso de las NTIC. Por ello, a continuación realizaremos una revisión del *status quo* jurídico-constitucional de los derechos en juego.

2. *El régimen constitucional de los derechos personalísimos ante nuevos riesgos digitales*

2.1. *Breves premisas acerca de la redefinición/protección reforzada de "viejos derechos" y el reconocimiento de "nuevos derechos"*

Según García Pelayo, "el derecho constitucional vigente, como todo [D]erecho, no es la pura norma, sino la síntesis de la tensión entre la norma y la realidad con la que se enfrenta"[22]. Así, en línea con las ideas vinculadas a la "constitución viviente", el derecho no sólo no está exento de reformarse y reinventarse ante los cambios y revoluciones en los que participa, sino que debe hacerlo, en tanto que le corresponde y se le interpela a acomodarse a realidades nuevas; independientemente de si son impuestas por la transformación tecnológica y digital o por las necesidades humanas. Por lo tanto, es de suma importancia garantizar la protección de la persona, no sólo frente a posibles injerencias estatales, sino también frente a las inimaginables amenazas contra la dignidad humana que puedan surgir en un "escenario marcadamente tecnológico y vanguardista pero que continúa mantenimiento la esencia de la cultura patriarcal imperante durante siglos"[23] y principalmente basada en el acceso instantáneo y universal y en la difusión masiva de información (en muchas ocasiones, de carácter personal).

El derecho, por tanto, debe regular los nuevos entornos digitales (y de quienes lo utilizan y operan en él), teniendo en cuenta su especificidad, pero también debe adecuar el ordenamiento jurídico para asegurar el ejercicio y protección efectiva de los derechos y libertades fundamentales; encontrándose con la difícil tarea de encontrar el equilibrio entre el progreso y la garantía del libre desarrollo de la persona-

[22] M. García Pelayo, *Derecho Constitucional Comparado*, Madrid, 1984, p. 45.
[23] M. Llorente Sánchez-Arjona, *La ciberviolencia de género,* cit., p. 414.

lidad y la protección de la dignidad. Considerando la compleja realidad sociodigital y la subsecuente pluralidad ordinamental que han generado las NTIC (principalmente debido a la perpetuidad y accesibilidad universal, en la red internet, de todo tipo de información), el derecho ha tenido que replantearse y revisar las normas y "positivizar" nuevas situaciones necesitadas de tutela y problemáticas jurídicas desconocidas hasta la fecha.

La necesidad de "juridificar" nuevas situaciones necesitadas de protección no es otra cosa que la de revisar, reforzar y redefinir los derechos ya reconocidos (los "viejos" o "clásicos" derechos) y dotarlos de nuevos mecanismos de tutela y adecuados para garantizar su protección y ejercicio efectivos. Los derechos fundamentales pueden y deben redefinirse para adaptarse a situaciones siempre cambiantes de nuevos contextos y realidades (incluidas las nuevas realidades sociotecno-digitales). En las últimas décadas ha habido determinados derechos que han sufrido especialmente, bien sea, como bien apunta Chueca, por "sobrecargas funcionales", "inadecuaciones en su configuración" o directamente por menoscabos en su protección y ejercicio efectivo[24].

Por ello, se han reivindicado o bien "nuevos" derechos, o bien la actualización de los "viejos", además de la creación de nuevos mecanismos de tutela, con el fin de trasladar normativamente la realidad actual y, sobre todo, con el fin de proteger a la persona de los daños colaterales que ha generado el uso de las NTIC en su dignidad. En otras palabras, el derecho ha mutado, igual que ha mutado la "informática", con el fin principal de garantizar el ejercicio de los derechos y libertades que ahora se expresan de manera más intensa, se desarrollan de manera más inconsciente y se vulneran de manera más gravosa, a través de las nuevas tecnologías. Por supuesto, estos cambios deben canalizarse a través de medidas adecuadas, proporcionales y equilibradas para asegurar que nos beneficiamos del potencial y las oportunidades que nos brindan estas tecnologías para el progreso social a la vez que "se faciliten instrumentos eficaces para la defensa de la autonomía, la

[24] R. CHUECA, *Las fronteras de los derechos fundamentales en la constitución normativa,* Madrid, 2019, p. 16.

dignidad y los derechos fundamentales en la era del Big data y la computación ubicua"[25].

Ante este nuevo panorama, el derecho de la UE, y en particular, el derecho constitucional español, ha intentado dar una mayor cobertura a las garantías protegidas por los derechos tradicionales, obligando tanto al aparato legislativo como judicial a ampliar horizontes. En lo que a la redefinición de los "viejos" o "clásicos" derechos se refiere, nos referimos al reconocimiento de nuevos cauces procesales para salvaguardar el libre desarrollo y dignidad de la persona en el marco de una nueva era tecnodigital. En lo que al reconocimiento de "nuevos" o "emergentes" derechos se refiere, la creación jurídica (bien normativa, bien jurisprudencial) de estos no ha sido otra cosa más que precisar nuevos aspectos que forman parte de esa faceta "digital" de la persona, o lo que han llamado algunos, el "cuerpo electrónico"[26]. Esto en gran medida pretende evitar, o al menos minimizar la pérdida paulatina de control. Entre los primeros cabe destacar el derecho a la intimidad, en todas sus facetas, consagrado expresamente en el art. 18.1 de la Constitución Española (CE). Y entre los segundos cabe destacar, sin duda, el derecho a la protección de datos, también llamado libertad informática, *Habeas Data* o autodeterminación informativa, implícitamente consagrado en el art. 18.4 de nuestra Carta Magna.

Precisamente, sobre este último punto, en el caso español, cabe decir que una de las principales novedades que incorporó la CE de 1978, siendo una de las pocas constituciones de la posguerra que lo hizo, fue la incorporación de un precepto específico que reconociera la protección de las personas frente al uso de la entonces todavía embrionaria "informática". El constituyente español tuvo suficiente visión para establecer un mandato legislativo[27] para limitar las NTIC en

[25] A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua,* Madrid, 2015, p. 251.

[26] S. RODOTÀ, *El derecho a tener derechos,* Madrid, 2014, p. 81.

[27] Aunque el legislador tardó más de una década en cumplir este mandato, finalmente se materializó en sendas leyes que se han ido reformando ante las exigencias de la integración europea y la necesidad evidente de actualizar los sistemas de protección de los derechos, para dar mejor respuesta ante la transformación socio-digital. Actualmente contamos con la ley orgánica 3/2018, *de Protección de Datos Personales y garantía de los derechos digitales,* de 5 de diciembre de 2018, y la ley orgánica 7/2021,

la medida que resultara necesario para garantizar el pleno ejercicio de los derechos de la ciudadanía. A pesar de la materialización normativa de limitar la informática, la falta de aclaración constitucional y el insuficiente desarrollo legislativo obligaron al Tribunal Constitucional español a perfilar el contenido y alcance del artículo 18.4 de la CE, como veremos más adelante.

2.2. *Los derechos personalísimos en el ordenamiento constitucional español*

Corresponde, como es bien sabido, a la teoría kantiana la concepción de la dignidad humana como valor fundamental de las nociones de persona; dignidad que engloba una dimensión moral de la personalidad, fundamentada en la propia libertad y autonomía de la persona. De ahí que la dignidad de la persona, como veremos a continuación, se encarne como principio legitimador de los denominados derechos de la personalidad, entendidos estos como el "conjunto de derechos que conceden un poder a las personas para proteger la esencia del ser humano y sus más importantes cualidades"[28]. En efecto, y tal como apunta Alegre Martínez, en tanto en cuanto su condición de ser racional, la persona merece y necesita autorrealizarse en un entorno que permita una búsqueda y desarrollo de quién es o quiere ser como persona, libre de injerencias o reprimendas, tanto en el ámbito público como privado[29].

Y es, justamente esta especial conexión entre los derechos de la esfera personal, o si se prefiere moral[30], y la dignidad huma-

de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, de 26 de mayo de 2021.

[28] V. LÓPEZ-IBOR MAYOR, C. PLAZA MARTÍN, *El Defensor del Pueblo: derecho, tecnologías de la información y libertades*, en *Informática y derecho: Revista iberoamericana de derecho informático,* 1994, n. 6-7, p. 276.

[29] M. A. ALEGRE MARTÍNEZ, *La dignidad de la persona como fundamento del ordenamiento constitucional español,* León, 1996, p. 19. Para desarrollos más recientes sobre los riesgos y retos actuales para la dignidad, vid. F. REY MARTÍNEZ, *La dignidad humana en serio. Desafíos actuales de los derechos fundamentales,* México, 2013.

[30] Para un estudio más amplio sobre la dignidad como valor básico y fundamento

na[31], la que ha hecho que la doctrina clásica haya clasificado algunos de ellos como "derechos de la personalidad", incluidos el derecho al honor, el derecho a la imagen, el derecho a la intimidad, el derecho al respeto a la vida privada y el derecho a la protección de datos[32]. Todos ellos están vinculados a la dignidad como autonomía y libertad moral, y así lo ha entendido, por ejemplo, el Tribunal Constitucional español: "la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás"[33]; o que la intimidad, como derecho "estrictamente vinculado a la propia personalidad y que deriva, sin duda, de la dignidad de la persona humana […][supone] la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario según las pautas de nuestra cultura para mantener una calidad de vida humana"[34]. Lo que significa afirmar la pretensión genérica de reconocer al individuo unos derechos que le corresponden por el mero hecho de ser persona.

El reconocimiento de la dignidad como base misma de estos derechos personalísimos significa una doble garantía para el individuo: una garantía negativa contra intromisiones y una garantía positiva que preserva el reducto más privado. De ahí que estemos hablando de un espacio específico de libre disposición al servicio del desarrollo y la libre configuración de la personalidad. Esta última en la actual era digital, necesariamente implica también "un control autónomo sobre los datos

de la satisfacción de las necesidades de la esfera moral, vid. A. E. PEREZ LUÑO, *Derechos Humanos: Estado de Derecho y Constitución*, Madrid, p. 234.

[31] T. PRIETO ÁLVAREZ, *La dignidad de la persona. Núcleo de la moralidad y del orden público, límite al ejercicio de las libertades públicas*, Cizur Menor-Navarra, 2005, p. 162.

[32] Resulta evidente que la libertad informativa, en una era como la actual, se ve reducida por la transformación digital y la innovación tecno-informática, que comprometen o menoscaban gravemente su pleno ejercicio, en particular aquellas relativas al tratamiento de datos de carácter personal. Por consiguiente, el derecho a la protección de datos, se configura como un nuevo o emergente derecho personalísimo.

[33] Tribunal Constitucional, sentencia de 11 de abril de 1985, n. 53/1985 (FJ 8), y, más reciente, la sentencia de 24 de noviembre de 2010, n. 115/2010.

[34] Tribunal Constitucional, sentencia de 28 de febrero de 1994, n. 57/1994.

propios, sobre la propia identidad informática"[35]. En definitiva, del poder de decisión sobre nuestra propia identidad en construcción[36].

2.3. *El derecho a la intimidad y el derecho a la protección de datos: dos derechos autónomos pero interconectados en el entorno digital*

Ya lo dejó sobradamente claro nuestro Tribunal Constitucional: en la sentencia de 20 de junio de 1993, n. 254/1993, y las sentencias de 30 de noviembre de 2000, n. 290/2000 y 292/2000, se reconoció lo que ahora llamamos derecho a la protección de datos (pero se llamó entonces libertad informática o autodeterminación informativa) como un derecho fundamental y autónomo, distinto del derecho a la intimidad (el *privacy* anglosajón). El derecho a la protección de datos, al contrario que el derecho a la intimidad, no implica un espacio o ámbito propio reservado, ni impide las injerencias o intromisiones de terceros. Sólo con leer el texto constitucional, nos percatamos de la diferencia. El artículo 18.1 CE limita el qué (qué información no puede ser revelada) y el artículo 18.4 CE limita el cómo, pero no el qué (información personal puede ser revelada o divulgada bajo unos fines legítimos y de conformidad con unos principios). Así lo ha confirmado el TC, quien además ha explicado como el derecho fundamental a la protección de datos tiene un contenido más amplio que el derecho a la intimidad: no se circunscribe a datos íntimos o a aquellos que pueden afectar a la intimidad, sino que abarca todo tipo de información que identifica o hace identificable a una persona y que, por ende, esta debe poder ejercer un control sobre los mismos.

La privacidad (o mejor dicho, la intimidad[37]) constituye una necesidad vital, sin la cual el hombre no puede formar ni desarrollar su personalidad, siendo en el marco de ese ámbito de privacidad en el

[35] V. FROSINI, *Informática y Derecho*, Bogotá, 2022, p. 23.

[36] S. RODOTÀ, *El derecho a tener derechos,* cit., p. 162.

[37] Nos encontramos ante un dilema *iusconceptual* de difícil resolución pues ha devenido práctica habitual utilizar el concepto "privacidad" como término genérico para referirse a distintos derechos personalísimos (o vertientes de los mismos) en la era digital, aunque este sea, en realidad, la traducción literal del privacy anglosajón, y por tanto, hace realmente referencia, al menos en el ordenamiento jurídico español, a nuestro derecho a la intimidad.

que configura sus pensamientos, sus creencias y su conciencia. Pero también es el marco de la privacidad, donde el individuo va fraguando el modelo de relación que quiere compartir con los demás, y que le permitirá desenvolverse con ellos.

Además de la interacción social y la participación, la intimidad también juega un papel importante en la formación de la identidad. La finalidad de la confidencialidad, como la dimensión intrínseca de muchos derechos de la esfera personal, es proteger a los más allegados; A veces se define como "la libertad frente a injerencias desproporcionadas a la construcción de la identidad"[38]. El famoso derecho *to be let alone*, nombrado por los padres de la privacidad en Estados Unidos, es similar a otros derechos personalísimos en que comparten esa necesidad de mantener cierta información en secreto o al menos de dar esa información sólo a un grupo limitado de personas seleccionadas por el titular de dicho derecho. Según la STC 185/2002, el derecho a la intimidad "tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona [...] frente a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares. De suerte que el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar, frente a la divulgación del mismo por terceros y una publicidad no querida. [...] Lo que el art. 18.1 CE garantiza es, pues, el secreto sobre nuestra propia esfera de vida personal y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los contornos de nuestra vida privada". En otras palabras, tiene el fin de garantizar a la persona un ámbito reservado de su vida, excluido tanto del conocimiento ajeno como de las intromisiones de terceros, sean de índole pública o particular, en contra de su voluntad.

Todo esto ha cambiado. El derecho de toda persona a definir libremente su proyecto de vida queda en entredicho por las NTIC: "la potestad de control que debería brindar la libertad, se ve coartada y limitada por el empleo de técnicas informáticas, que comprometen o menoscaban gravemente su práctica, en particular aquellas relativas al tratamiento de datos de carácter personal, como potencial agresión a

[38] E. GOFFMAN, *Presentation of the self in everyday life,* Nueva York, 1959, p.7.

la dignidad y libertad personal, y concretamente, al libre desarrollo de la personalidad y a la autónoma construcción de la identidad"[39]. Hoy en día, no sólo nos relacionamos y desarrollamos nuestra identidad, personalidad y nuestras relaciones personales a través de estas nuevas herramientas, dejando huellas digitales allá dónde vamos, sino que la información personal que directa o indirectamente le confiamos al ciberespacio o a terceros en nuestro proceso de retroalimentación y experimentación personal y social, se han convertido en componente estratégico del control y construcción (*mutatis mutandis*, del descontrol y destrucción) del libre desarrollo de la propia identidad, a través de un menoscabo de los derechos intrínsecamente ligados a ella.

En cuanto a la tutela judicial, cabe apuntar que el derecho a la intimidad, bien sea entendida en su faceta de intimidad personal, familiar o informativa[40], además de contar con una protección de índole penal[41], también cuenta con una protección civil mediante la ley orgánica 1/1982, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, de 5 de mayo de 1982, cuando se trata de injerencias o intromisiones ilegítimas[42].

3. *Análisis casuístico: la sextorsión como supuesto de ciberviolencia contra la mujer y garantías para la tutela de sus derechos*

3.1. *Aproximación a la problemática social y jurídica*

La violencia contra las mujeres sigue aumentando a un ritmo sin precedentes y se materializa ahora también en el ámbito virtual, a través no sólo de la divulgación y difusión de datos de carácter personal de carácter especialmente sensible o íntimo, sino asimismo a través de comportamientos violentos que afectan seriamente a la salud física y

[39] M. MARTÍNEZ LÓPEZ-SÁEZ, *El derecho al olvido como garantía frente a situaciones de vulnerabilidad en la UE y España,* Madrid, 2020, 100.

[40] Para ver el contenido de las mismas, vid. L. REBOLLO DELGADO, *El derecho fundamental a la intimidad,* Madrid, 2005, p. 273 y ss.

[41] Vid., en el caso del objeto de estudio de esta contribución, principalmente el art. 197 CP.

[42] Vid. particularmente su art. 7.

mental de las mujeres (lo que se podría englobar como "technology-facilitated sexual violence")[43]. Esto es especialmente claro y grave en el caso de la sextorsión.

La sextorsión es una nueva forma de violencia contra la mujer: es la amenaza, extorsión y/o chantaje sexual por internet, también conocido como "porno vengativo"[44], "pornovenganza" o "ciberintimidación sexual". Se amenaza a la persona, mayoritariamente a la mujer, con la difusión de contenido íntimo-sexual si esta se niega a acceder a sus pretensiones, habitualmente de carácter sexual. El desequilibrio de poder es claro: la intención de dominar y doblegar la voluntad a través del chantaje.

Sin embargo, antes de adentrarnos en esta cuestión en cuanto a las amenazas socio-digitales y las respuestas jurídicas previstas en la normativa europea de protección de datos es de obligada referencia al menos realizar una aproximación del impacto de la violencia de género y su manifestación concreta en el ámbito digital, para así entender la propuesta del derecho al olvido en tanto mecanismo para la recuperación del trauma y la restitución de la dignidad.

Con independencia de la naturaleza concreta del acto, se ha demostrado que la violencia sexual, en general, y la facilitada por las NTIC en particular, tienen repercusiones todavía más graves para el bienestar emocional y psicosocial de aquellas mujeres que la sufren. En el caso de las víctimas de sextorsión, si bien la información personal de índole íntima o sexual[45] suele cederse, en su origen, con el consenti-

[43] A. POWELL, N. HENRY, *Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults,* en *Journal of Interpersonal Violence*, 2016, vol. 34, n. 17, pp. 3637-3665; M. DROUIN, J. ROSS, E. TOBIN, *Sexting: a new, digital vehicle for intimate partner aggression,* en *Computers in Human Behaviour,* 2015, n. 50, p. 197.

[44] M. I. MARTÍNEZ GONZÁLEZ, L*as nuevas tecnologías como herramientas de prevención y actuación frente a la violencia de género*, en M.A. VERDEJO ESPINOSA (a cura di), *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención*, Sevilla, 2015, p. 304.

[45] Suelen ser fotografías enviadas, mediante la práctica del sexting, y varían desde contenidos sugestivos o provocativos hasta desnudez total o parcial, seguida de otros datos personales además de la imagen, tales como el nombre, el correo o el usuario en las redes sociales o su teléfono móvil. Vid. K. WALKER, E. SLEATH, *A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of*

miento de la víctima, el problema radica en la difusión asincrónica de información a terceros. Esto ocurre a menudo en el contexto de una ruptura, siendo una versión de venganza o chantaje, aunque la extorsión también puede venir de aquellas personas que no tiene relación sentimental con la víctima[46]. En este sentido, algunos consideran más apropiado hablar de abuso o "explotación sexual basada en imágenes"[47].

Aquí, a pesar de no haber dos actos traumáticos seguidos, pues, en principio (aunque no siempre), el contenido audiovisual fue tomado y enviado originalmente con el consentimiento de la mujer, su posterior difusión (y consiguiente y potencial viralización) es igualmente una injerencia ilegítima (e incluso más gravosa) en sus derechos personalísimos, en especial el derecho a la intimidad y a la protección de datos, y, en última instancia, a su bienestar emocional: algunos estudios incluso han demostrado que los efectos para la salud mental de aquellas que lo sufren vienen a ser idénticos a los de las víctimas de agresiones sexuales[48].

Además de los daños psicológicos asociados a este fenómeno, las víctimas de este tipo de ciberviolencia sexual sufren diversos daños irreparables que afectan a su vida personal y, sobre todo, profesional.

sexually explicit media, en *Aggression and Violent Behavior,* 2017, n. 36, p. 9.

[46] Aunque, como acertadamente apuntan algunos autores, el porno vengativo no necesariamente se hace como práctica vengativa ni por parte de una persona conocida: *"The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners and the motive is not always revenge. Images can also be obtained by hacking into the victim's computer, social media accounts or phone, and can aim to inflict real damage on the target's "real-world" life".* Vid. INSTITUTO EUROPEO DE IGUALDAD DE GÉNERO, *Cyberviolence against women,* cit., p. 2.

[47] A. POWELL, N. HENRY, *Sexual Violence in a Digital Age*, cit., p. 118; C. MCGLYNN, E. RACKLEY, R. HOUGHTON, *Beyond Revenge Porn: The Continuum of Image-Based Sexual Abuse,* en *Feminist Legal Studies*, 2017, n. 25, pp. 25-46.

[48] K. WALKER, E. SLEATH, *A systematic review*, cit. pp. 21-22; S. BATES, *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors,* en *Feminist Criminology,* 2016, vol. 12, n. 1, pp. 39-40: *"sexual assault survivors report that the loss of control over their bodies and their own sexual agency contributes to their feelings of stress, anxiety, and distress. The loss of control participants in the present study experienced contributed to feelings of anxiety and despair, and was a major facet of why revenge porn was so violating".*

Relaciones y familias quedan destrozadas y los medios de subsistencia en ocasiones se ven comprometidos. No son pocos los casos en los que se ha recurrido a despidos disciplinarios por culpa de fotos que se han publicado o distribuido por las redes sociales sin el consentimiento de la afectada[49]. En efecto, como hemos dicho en varias ocasiones, la universalización y perennidad de la red no solo dificulta sino que, en determinadas circunstancias, imposibilita la capacidad de desprenderse de eventos pasados y traumáticos.

Desafortunadamente, en España este supuesto de ciberviolencia no está tipificado, pero se puede englobar, y así se ha confirmado en sede judicial, en un elenco variado de tipos penales según el sujeto y el contenido de la práctica (desde las meras amenazas o extorsión, pasando por la explotación sexual, abuso de menores o corrupción de menores, relevación de secretos y otros delitos contra la intimidad[50], e incluso, en algún caso abuso o agresión sexual[51]). De esta última cabe destacar una serie de elementos a los que hemos hecho y seguiremos haciendo referencia: "el riesgo para cualquier persona, pero muy en especial para una mujer […] de que la imagen de su cuerpo desnudo, mostrando, además, actos de contenido sexual sobre el mismo, pueda ser distribuida por una red social de la que participan muchas personas de su entorno social y afectivo, adquiere una relevante gravedad […][y no sólo en cuanto a su derecho de intimidad sino también por cuanto supone una] profunda alteración de sus relaciones personales y de su propia autopercepción individual y social". Volveremos a esto más adelante.

A modo de recordatorio, la directiva 2012/29/UE[52], incorpora una definición autónoma de "violencia por motivos de género" en la que se incluye toda forma de violación de los derechos y libertades fundamentales de la víctima, por motivo de su sexo, entre las que destaca todo tipo de comportamientos físicos y psicológicos que produzcan o

[49] N. LEE, *Facebook Nation: Total Information Awareness,* Luxemburgo, 2021, p. 234.

[50] Tribunal Supremo, sentencia de 23 de julio de 2018, n. 377/2018.

[51] Tribunal Supremo, sentencia de 26 de mayo de 2021, n. 447/2021.

[52] Directiva (UE) 2012/29 del Parlamento Europeo y del Consejo, *por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos*, de 25 de octubre de 2012, en DOUE 315, de 14 de noviembre de 2012.

puedan producir cualquier tipo de daño o sufrimiento[53]. Esta definición amplia de violencia de género, como vimos, también incluye la violencia de género efectuada por medios digitales en tanto en cuanto incluye conductas que causan un daño emocional. Además, recordemos que en ella se hace especial hincapié en la protección de las víctimas frente a futuras victimizaciones o represalias, así como en la protección de su intimidad y derecho fundamental a la protección de datos, en su camino por el aparato institucional (en lo que concierne a su acceso al apoyo especializado y a las garantías que proporciona el proceso penal) y en su camino personal hacia la recuperación, incluidas la prohibición y limitación en la difusión de sus datos personales[54].

De igual manera, recordemos que la citada directiva (UE) 2024/1385 acoge una definición todavía más amplia de violencia contra la mujer, y de ahí que hayamos acogido este término: "todo acto de violencia de género dirigido contra una mujer o una niña por el hecho de ser mujer o niña, o que afecten de manera desproporcionada a mujeres o niñas, que causen o sea probable que causen daños o sufrimientos de naturaleza física, sexual, psicológica o económica, incluidas las amenazas de realizar tales actos, la coacción o la privación arbitraria de libertad, tanto si se producen en la vida pública como en la vida privada"[55]. También, implícitamente ampara la persecución de la sextorsión cuando en su art. 5.1(c) establece que los estados miembros deberán garantizar como conductas punibles amenazar con cometer, entre otras conductas, hacer accesible digitalmente imágenes, vídeos o materiales similares que representen partes o actividades sexualmente explícitas con el fin de coaccionar a una persona para que realice o acceda a que se realice determinado acto o se abstenga de realizarlo.

3.2. *El derecho al olvido como garantía específica para la protección efectiva de la dignidad de la víctima de ciberviolencia*

En la era socio-digital actual, los autores de los hechos deleznables supracitados gozan de una gran libertad y anonimato, mientras que las

[53] Recordemos el contenido del Considerando 17 de la misma.

[54] Recordemos el Considerando 54 de la misma.

[55] art. 2(a) de la misma.

que lo sufren tienen una realidad agravada añadida. Una vida libre de agresiones e intimidación (sea presencial o a distancia) no sólo es un derecho fundamental de toda persona, sino que, en el caso de las mujeres víctimas de violencia de género, este derecho requiere garantías especiales debido a que este colectivo se encuentra "en una situación de crisis personal grave" lo que debe significar "que el cumplimiento normativo tenga que humanizarse en este contexto"[56].

Por ello, es necesario un mecanismo efectivo que permita a estas mujeres no quedar atrapadas en un círculo vicioso en el que el recuerdo del evento traumático se convierta en "arma arrojadiza vengativa"[57]. Y este mecanismo de tutela *iusdigital* no es otro que: "el derecho al olvido, como garantía de una "evitación" digital; este jugaría un papel importante no sólo en el restablecimiento del control de este colectivo sobre su propia información personal (de carácter íntimo, además) y como mecanismo de empoderamiento socio-digital, sino también como herramienta para el alivio del trauma constante que supone tener un rastro digital eterno e incesante de la red y para poder llegar más fácilmente a una recuperación psico-emocional, sin tener que tomar medidas tan drásticas como cambiarse su nombre, usuario, mudarse de ciudad o desaparecer de las redes sociales y servicios digitales".

Así, cabe recordar que, aunque las mujeres víctimas de violencia de género tampoco están expresamente mencionadas como grupo vulnerable en la normativa de protección de datos aplicable, la perspectiva de riesgo adoptada por esta, y la transversalidad de la igualdad y del género nos llevan a considerar que el tratamiento de datos de este colectivo debe gozar también de especial protección[58].

[56] R. MARTÍNEZ MARTÍNEZ, citado por L. J. SÁNCHEZ, *¿Cómo garantizar la seguridad de las víctimas de violencia de género desde la protección de datos?,* en *Confilegal*, abril 2017, https://confilegal.com/20170417-como-garantizar-la-seguridad-de-las-victimas-de-violencia-de-genero-desde-la-proteccion-de-datos/.

[57] E. ECHEBURÚA ODRIOZOLA, M.S. CRUZ-SÁEZ, *De ser víctimas a dejar de serlo. Un largo proceso,* en *Revista de Victimología*, 2015, n. 1, p. 93.

[58] En similar sentido, recordemos que los datos personales concernientes a una mujer víctima de violencia de género son calificados, tanto en el reglamento general de protección de datos como en la directiva policial, como categorías especiales de datos personales (o datos sensibles), no sólo porque la información concerniente puede con-

Recordemos que, hasta fechas bien recientes, a nivel europeo, contamos con dos instrumentos normativos en materia de protección de datos, que reconocen, en su concreto ámbito de su aplicación, un derecho al olvido: el reglamento general de protección de datos y la directiva policial. Ahora, además, debemos añadir las garantías que presenta la citada directiva (UE) 2024/1385, que enfatiza la necesidad de garantizar la protección de la privacidad y la información confidencial de las víctimas. En lo que se refiere específicamente al derecho al olvido, observamos que la normativa de protección de datos lo contempla en su faceta de derecho de supresión, para el que encontramos un par de supuestos habilitadores: cuando la supresión sea una obligación legal y cuando el tratamiento se haya realizado vulnerando cualquiera de los principios de protección de datos, siendo, por ende, ilícito[59]. Como apuntan algunos autores, el objetivo es evitar que se siga produciendo un daño a la víctima, agravando el ya TEPT digital, siendo ambas consecuencias lesivas y continuadas del delito[60].

En general, la falta de consentimiento constituye uno de los títulos habilitantes para ejercer el derecho al olvido, en cualquiera de sus facetas, pues el principio del consentimiento determina la licitud del tratamiento, por lo que la vulneración del mismo resultará en un tratamiento ilícito. El derecho al olvido, interrelacionado con el consentimiento, actúa como instrumento de empoderamiento y autodeterminación en el control de los datos de carácter personal, y como garantía para eliminar o impedir el acceso y utilización sucesiva de datos personales, precisamente cuando su tratamiento deja de estar (o, como en este caso, nunca estuvo[61]) autorizado por el interesado (art. 17.2 RGPD). Las víctimas de ciberviolencia sexual no tienen por qué so-

tener datos de salud (física/sexual o psicológica), sino porque los datos identificativos relativos al género en sí son datos de especial sensibilidad. Por ambas razones gozarían del mayor nivel de protección que dota la normativa de protección de datos en lo que a su tratamiento se refiere.

[59] Vid. art. 16.2 de la directiva policial.

[60] J.M. DE LA ROSA CORTINA, *Las medidas cautelares personales en el proceso penal*, Barcelona, 2015, pp.409-412.

[61] En el caso de las víctimas de pornografía vengativa, si bien el material audiovisual fue grabado y compartido mediando consentimiento, su distribución a terceros o su publicación en abierto en la red no lo fue.

portar la omnipresencia de sus datos personales (sea su imagen, su nombre, o cualesquiera otra información identificativa, sobre todo si encima es de carácter íntimo) en la Red, sobre todo cuando no existe interés alguno, o suficiente, que justifique su permanencia.

Así también parecen haberlo comprendido las agencias nacionales independientes de protección de datos para estos casos específicos de ciberviolencia sexual. De hecho, en muchas ocasiones han tenido que actuar y colaborar con las autoridades para evitar mayor disponibilidad y acceso a este tipo de contenidos. La Agencia Española de Protección de Datos, por ejemplo, lanzó el año pasado un sitio web de ayuda para proteger la privacidad de las víctimas de ciberviolencia de género en el contexto de acoso digital, sextorsión o pornografía vengativa. Esta plataforma digital incluye no solo información práctica para proteger su privacidad, los servicios a su disposición y cómo actuar, sino también, y en lo que respecta al tema en estudio, facilitar y acelerar los procedimientos de eliminación urgente de contenidos sexuales o violentos, distribuidos ilegalmente tras su difusión[62].

Con todo ello, podemos afirmar que el derecho al olvido deviene, en la práctica, no sólo como un simple derecho de eliminación de contenidos dañinos sino como una garantía para devolverle a la mujer víctima de ciberviolencia sexual un control y algo de dignidad, quebrantada en el mundo virtual por motivos perversos e injustificables por su agresor[63]. Este, sea en su faceta de supresión de datos personales o de re-contextualización digital[64], permite que las víctimas de violencia, atendiendo a los diferentes factores y elementos del caso particular, no queden atrapadas en un limbo de violencia multidimensional y continuada.

[62] A través del llamado "Canal específico para comunicar, con carácter prioritario, la difusión ilegítima de imágenes sensibles". https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/canalprioritario.jsf.

[63] Que, recordemos además, al igual que los ciberacosadores, son también responsables del tratamiento, según la jurisprudencia del Asunto *Lindqvist,* quedando expuestos a las sanciones pertinentes por el incumplimiento de la normativa de protección de datos.

[64] La tipología que proponemos en M. MARTÍNEZ LÓPEZ-SÁEZ, *El derecho al olvido como garantía,* cit.

4. *Reflexiones finales*

La revolución tecnológica y la transformación socio-digital han generado un nuevo mundo marcado por la continua y rápida creación, almacenamiento, tratamiento e intercambio masivo de información, que forman identidades y perfiles digitales de los que nos volvemos dependientes o que nos condicionan la vida. Rodotà, en esta línea, habla del desafío a la identidad, del empobrecimiento de la capacidad de decidir, de la inutilidad de suplicar mayor privacidad y de que se percibe como una auténtica pérdida del control sobre uno mismo[65].

Ya no sólo podemos hablar de la "colonización"[66] de los derechos personalísimos a través de medios tecnológicos, sino que debemos pasar a hablar de la demolición de dignidad y del surgimiento de hipotecas vitalicias, modelos y estructuras digitales de opresión y esclavitud por la omnipresencia y omnipotencia de las NTIC y el abuso que se hace de ellas. Necesitamos un marco integral para prevenir y combatir eficazmente la violencia contra las mujeres. En los últimos años, el marco europeo y español se ha enfocado precisamente en eso: en reforzar el marco jurídico con el fin de prevenir y combatir eficazmente la violencia contra las mujeres. El año pasado se adoptó un instrumento, en marco de un conjunto integral de normas, que justamente aborda de manera concreta el problema persistente de la violencia contra las mujeres, y sus nuevas manifestaciones en aras a la transformación digital, y establece medidas armonizadas para apoyar de manera efectiva a las que sufren nuevas formas de discriminación y violencia de género.

No obstante, observamos como esta, propio de su naturaleza en cuanto instrumento de armonización parcial, establece un marco mínimo (en cuanto a definiciones y derechos, por ejemplo), a la vez que contiene las denominadas "clausulas abiertas" o de "flexibilización", en las que se reconoce un cierto margen de apreciación nacional a los Estados miembros al permitir la especificación o desarrollo de su contenido a nivel nacional, propio de las dinámicas de integración euro-

[65] S. RODOTÀ, *El derecho a tener derechos,* cit., 309-310.

[66] A.E. PÉREZ LUÑO, *El posthumanismo no es un humanismo,* en *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos,* 2021, n. 44, pp. 17-40.

pea. Como se puede apreciar, no todas las disposiciones tienen el mismo nivel de flexibilidad: algunas disposiciones obligan o permiten desarrollar o ampliar su contenido en la normativa nacional, otras sugieren realizar adaptaciones, otras permiten fijar exenciones, derogaciones o condiciones específicas (la famosa coletilla de técnica jurídica "los Estados miembros podrán…"), por lo que todavía hay margen de mejora en aras a la armonización total y protección reforzada de las mujeres a nivel europeo. Esta directiva, además, se deberá interpretar de manera sistemática con el resto del ordenamiento jurídico europeo, incluido el marco general y especial de protección de datos, y todavía hay incógnitas en cuanto a qué acción o conjunto de acciones se deben y pueden ejercer simultáneamente en lo que se requiere a medidas de protección y eliminación de contenidos.

En cualquier caso, ante la pérdida de control o la anulación e indefensión en la capacidad de respuesta en entornos digitales, el derecho al olvido resulta ser, en definitiva, un recurso o garantía constitucional de naturaleza digital para protección de intimidad y la identidad, y en última instancia, la dignidad de las mujeres que han sufrido ciberviolencia sexualizada.

Abstract

El desarrollo de las NTIC no sólo ha comportado la aparición de nuevas formas de violencia, sino que también ha servido de cauce para la proliferación y agudización de sus formas más clásicas. La violencia ejercida en contra de la mujer, ahora trasladada y transmutada en los entornos digitales, ha generado un nuevo concepto de necesario estudio: "ciberviolencia contra la mujer". Este trabajo analiza la configuración jurídico-constitucional en España de dos derechos fundamentales en juego, con el fin de presentar los mecanismos de tutela y proponer nuevas garantías y recursos ante hipotecas personales vitalicias y nuevos modelos de opresión de la mujer en tiempos digitales.

PALABRAS CLAVE: Ciberviolencia contra la mujer – intimidad – protección de datos – brecha digital por razón de género – privacidad en entornos digitales

UNA (RE)VISIONE COSTITUZIONALE DEI DIRITTI CLASSICI ED EMERGENTI DI FRONTE ALLE NUOVE FORME DI CYBERVIOLENZA CONTRO LE DONNE

Lo sviluppo delle NICT non solo ha portato alla comparsa di nuove forme di violenza, ma è anche servito da canale per la proliferazione e l'aggravamento delle sue forme più classiche. La violenza contro le donne, ora trasferita e trasmessa negli ambienti digitali, ha generato un nuovo concetto che deve essere studiato: la "cyberviolenza contro le donne". Il presente lavoro analizza la configurazione giuridico-costituzionale in Spagna dei due diritti fondamentali in gioco, con l'obiettivo di presentare i meccanismi di protezione e proporre nuove garanzie e risorse di fronte alle ipoteche personali vitalizie e ai nuovi modelli di oppressione delle donne in epoca digitale.

KEYWORDS: Cyber-violenza contro le donne – privacy – protezione dei dati – divario digitale di genere – privacy negli ambienti digitali

CONVENZIONE DI ISTANBUL E CONVENZIONE DI BUDAPEST: UNA RISPOSTA COORDINATA AL FENOMENO DELLA CYBERVIOLENZA CONTRO LE DONNE

*Anna Iermano**

1. *Convenzione di Istanbul e dimensione digitale della violenza contro le donne: una lacuna apparente*

Sebbene la Convenzione di Istanbul[1] non affronti specificamente

* Professoressa associata di Diritto internazionale, Università degli Studi di Salerno. Email: aiermano@unisa.it.

[1] Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, adottata dal Comitato dei Ministri del Consiglio d'Europa il 7 aprile 2011, aperta alla firma l'11 maggio 2011 in occasione della 121a Sessione del Comitato dei Ministri a Istanbul ed entrata in vigore il 1° agosto 2014. Gli Stati che hanno finora ratificato la Convenzione sono 39. L'Italia l'ha ratificata con Legge 27 giugno 2013, n. 77, in GU Serie Generale n. 152 del 1 luglio 2023. Al riguardo giova ricordare che il primo paese che ha ratificato la Convenzione il 14 marzo 2011, la Turchia, con decreto firmato dal presidente Recep Tayyip Erdoan il 20 marzo 2021 ha, invece, manifestato la volontà di recedere dalla Convenzione ai sensi dell'art. 80, ritenendo che le leggi nazionali fossero sufficienti a garantire la protezione delle donne. La Convenzione è aperta all'adesione di qualsiasi paese disposto ad attuarne le disposizioni. V., *ex multis*, S. DE VIDO, M. FRULLI (eds.), *Preventing and combating violence against women and domestic violence. A Commentary on the Istanbul Conven-*

la dimensione digitale della violenza contro le donne e della violenza domestica, essa è tuttavia rilevante nel prevenire e combattere anche questa dimensione "distinta" ma non "separata" dalla violenza contro le donne[2], di cui è ulteriore manifestazione in un quadro unitario e complessivo violento.

Come precisa, infatti, il gruppo GREVIO[3] nella Raccomandazione n. 1 del 20 ottobre 2021[4] sulla dimensione digitale della violenza contro le donne[5], quest'ultima non è altro che un *continuum* della violenza offline di genere[6], ovvero un'estensione o prosecuzione della violenza psicologica, sessuale e fisica che le donne sperimentano nella realtà, in particolare in ambito domestico.

tion, Cheltenham-Northampton, 2023, p. 482 ss.; A. DI STEFANO, *La Convenzione di Istanbul del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica*, in www.dirittopenalecontemporaneo.it, 11 ottobre 2012; F. POGGI, *Violenza di genere e Convenzione di Istanbul: un'analisi concettuale*, in *Diritti umani e diritto internazionale*, 2017, n. 1, p. 51 ss.

[2] Così GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women*, 20 ottobre 2021.

[3] Il Gruppo di esperti sulla lotta contro la violenza nei confronti delle donne e la violenza domestica.

[4] GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women*, cit., che, in linea con l'art. 69 della Convenzione di Istanbul, chiarisce ulteriormente l'applicazione della Convenzione medesima in relazione alle espressioni digitali della violenza contro le donne. Offre un'interpretazione approfondita della Convenzione nel contesto della violenza online e facilitata dalla tecnologia e chiarisce, in termini pratici, gli obblighi degli Stati membri, fornendo a questo riguardo raccomandazioni concrete.

[5] L'espressione "dimensione digitale della violenza contro le donne" o "violenza contro le donne nella sua dimensione digitale" è sufficientemente ampia da comprendere sia gli atti di violenza online (condivisione di immagini umilianti, insulti, minacce di morte e di stupro,…) che quelli perpetrati attraverso l'uso di TIC [telefoni cellulari e smartphone, Internet, piattaforme di social media o e-mail, dispositivi di localizzazione, droni, dispositivi di registrazione non connessi a Internet e Intelligenza Artificiale (AI)], incluse le tecnologie ancora da sviluppare, il tutto in linea con il carattere evolutivo dello spazio digitale e degli atti violenti ivi commessi. Al riguardo mi si permetta di rinviare ad A. IERMANO, *Violenza digitale e Convenzione di Istanbul: una dimensione distinta ma non separata dalla violenza contro le donne*, in *Freedom, Security & Justice: European Legal Studies*, 2024, n. 1, p. 64 ss.

[6] GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women*, cit.

Non a caso, oggi, la distinzione tra "mondo fisico" e "mondo virtuale" tende ad essere superata dalla nuova realtà cosiddetta "*on-life*".

Tuttavia, allo stato, sussiste un apparente dualismo tra le questioni relative a tecnologie dell'informazione e della comunicazione, spesso non informate alla violenza di genere contro le donne, e risposte nazionali alla violenza di genere contro le donne, specie in ambito domestico, che raramente includono la dimensione digitale di siffatta violenza.

Tale dualismo sembra, altresì, riflettersi sul piano normativo laddove fonti, come la Convenzione sulla criminalità informatica del Consiglio d'Europa (Convenzione di Budapest)[7], regolano i diritti di accesso online, le Tecnologie dell'Informazione e della Comunicazione (TIC) e la sicurezza, senza contemplare la dimensione della violenza di genere; al contempo, – almeno fino all'entrata in vigore della direttiva

[7] Consiglio d'Europa, Convenzione sulla criminalità informatica, STE, n. 185, aperta alla firma il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004. Ad oggi conta 78 Stati parte. È stata ratificata in Italia con la Legge 18 marzo 2008, n. 48, in GU 4 aprile 2008, n. 80. La Convenzione è aperta agli Stati membri del Consiglio d'Europa e, su invito, ai paesi che non ne sono membri. Non prevede l'adesione dell'Unione europea che è, tuttavia, riconosciuta come organizzazione con lo *status* di osservatore presso il Comitato della Convenzione sulla criminalità informatica; inoltre, l'Unione offre un sostegno costante alla Convenzione anche nel quadro del finanziamento di programmi di sviluppo delle capacità. La Convenzione di Budapest è supportata dal Comitato della Convenzione sulla criminalità informatica che ne monitora l'attuazione e dall'Ufficio per il programma sulla criminalità informatica di Bucarest, Romania, che sostiene i paesi in tutto il mondo attraverso programmi di creazione di competenze come il progetto GLACY (*Global Action on Cybercrime*). Vedi, anche, Consiglio d'Europa, Raccomandazione del 9 settembre 1989 n. R (89)9 e Raccomandazione n. R (95)13 dell'11 settembre 1995 sui profili di procedura penale collegati alle tecnologie dell'informazione. In dottrina cfr., *inter alia*, N. RUSSO, *20° anniversario della Convenzione di Budapest*, in *Diritto penale e processo*, 2022, vol. 28, n. 8, p. 1020 ss.; J. CLOUGH, *A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation*, in *Monash University Law Review*, 2014, p. 701 ss.; F. CAJANI, *La convenzione di Budapest nell'insostenibile salto all'indietro del legislatore italiano, ovvero: quello che le norme non dicono …*, in *Ciberspazio e diritto*, 2010, vol. 11, n. 1, p. 185 ss.; E. COLOMBO, *La cooperazione internazionale nella prevenzione e lotta alla criminalità infomatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in *Ciberspazio e diritto*, 2009, vol. 10, fasc. 3/4, p. 285 ss.

2024/1385[8] – atti sui diritti delle donne, prima fra tutte la Convenzione di Istanbul, non affrontano specificamente la dimensione digitale della violenza contro le donne e della violenza domestica.

Dualismo, questo, riscontrato anche in sede giurisprudenziale, come nella sentenza *Buturugă c. Romania*[9], in cui la Corte europea dei diritti dell'uomo, nel primo caso di cyberviolenza ai danni di una donna sottoposto alla sua attenzione, ha riscontrato nella prassi un approccio "dualista" che tende a distinguere tra violenza domestica da un lato, e violenza digitale dall'altro, sia nella fase delle indagini che di merito[10].

[8] Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio, *sulla lotta alla violenza contro le donne e alla violenza domestica*, del 14 maggio 2024, in GUUE L del 24 maggio 2024 che, nel capo 2 *reati di sfruttamento sessuale femminile e minorile e criminalità informatica*, disciplina la condivisione non consensuale di materiale intimo o manipolato tramite Tecnologie dell'Informazione e della Comunicazione (TIC) *ex* art. 5, lo *stalking* online (art. 6), le molestie online (art. 7) e l'istigazione alla violenza o all'odio online (art. 8).

[9] Corte europea dei diritti dell'uomo, sentenza dell'11 febbraio 2020, ricorso n. 56867/15, *Buturugă c. Romania.* Per un commento v. C. CONTI, *Maltrattamenti in famiglia e violazione della riservatezza della corrispondenza*, in *Diritto penale e processo - Osservatorio Corte Europea dei Diritti dell'Uomo*, 2020, n. 5, p. 716 ss.; E. FALLETTI, *Corte Europea dei Diritti Umani. Assenza di indagini penali su violenze coniugali*, in *Osservatorio di diritto internazionale privato e comunitario*, in *Famiglia e diritto*, 2020, n. 5, p. 499 ss.; V. TEVERE, *Per la Corte europea dei diritti dell'uomo l'accesso, senza consenso, all'account personale del* partner *è violenza domestica: analisi del caso Buturugă c. Romania*, in *I diritti dell'uomo*, 2020, n. 1, p. 229 ss.; ID., *La giurisprudenza della Corte di Strasburgo in materia di violenza digitale/La jurisprudencia del tribunal de estrasburgo sobre violencia digital*, in questo Volume, pp. 257-272, con riferimento anche agli altri casi di violenza digitale contro le donne sottoposti all'attenzione della Corte europea dei diritti dell'uomo (sentenza del 9 luglio 2021, ricorso n. 40419/19, *Vodolina c. Russia* (No. 2) e sentenza del 3 dicembre 2024, ricorso n. 28935/21, *MSD c. Romania*).

[10] Il caso di specie origina dal ricorso presentato da una cittadina rumena, Aurelia Buturugă, che denunciava l'ex marito sia per i ripetuti episodi di violenza domestica (violenze fisiche e minacce di morte) che per violazione della segretezza della corrispondenza (utilizzo abusivo dei suoi account informatici, inclusa la pagina Facebook, acquisizione di conversazioni private, documenti e foto). La ricorrente fece dapprima richiesta di perquisizione elettronica del computer della famiglia per acquisire prove nell'ambito di un procedimento penale, ma la polizia di Tulcea respinse la richiesta ritenendo, le prove, non collegate ai reati di minaccia e violenza. A seguire presentò denuncia per violazione della riservatezza della corrispondenza ma il Pubblico Mini-

Al contrario, la Corte ha asserito, all'unanimità, che la cyberviolenza deve essere considerata, a tutti gli effetti, come violenza contro le donne e che, di conseguenza, le autorità nazionali non possono trattare episodi, quali l'utilizzo abusivo degli account di una donna da parte dell'ex marito o l'acquisizione di immagini e dati, alla stregua di casi di violenza ordinaria; esse devono piuttosto applicare le regole più stringenti fissate per i casi di violenza domestica, in linea con la citata Convenzione di Istanbul.

Di fatto, dunque, la cyberviolenza allude ad un'ampia gamma di comportamenti riconducibili alla definizione di "violenza nei confronti delle donne" ex art. 3, lett. a) della Convenzione di Istanbul, la quale, come noto, include "tutti gli atti di violenza fondati sul genere che provocano o sono suscettibili di provocare danni o sofferenze di natura fisica, sessuale, psicologica o economica, comprese le minacce di compiere tali atti, la coercizione o la privazione arbitraria della libertà, sia nella vita pubblica, che nella vita privata"; atti, questi, che richiedono specifiche azioni di contrasto fondate sui quattro pilastri (4P): prevenzione, protezione, perseguimento penale e politiche coordinate.

In definitiva, la Convenzione di Istanbul trova applicazione nel caso di violenza contro le donne, a prescindere dal fatto che essa sia online e/o offline, nell'ottica di un approccio globale al fenomeno, in tutte le sue dimensioni.

stero considerò tardiva la denuncia relativa alla violazione del segreto della corrispondenza. La Corte europea sostiene che le autorità inquirenti, dando prova di un formalismo eccessivo, nel respingere qualsiasi collegamento con gli episodi di violenza domestica già portati alla loro attenzione dalla ricorrente, non hanno risposto in un modo commisurato alla gravità dei fatti lamentati, in violazione degli artt. 3 e 8 della Convenzione. Cfr. S. CECCHINI, *La cyber-violenza di genere: un caso di omogeneizzazione giurisprudenziale tra ordinamenti statali*, in *Giurisprudenza italiana*, 2020, n. 3, p. 533. Secondo l'A. questa sentenza è di notevole interesse soprattutto per la parte motivazionale in cui il giudice europeo ha formulato delle raccomandazioni alle stesse autorità rumene su come condurre le indagini nei casi di violenza domestica.

2. La complementarità tra Convenzione di Istanbul e Convenzione di Budapest nell'azione di contrasto alla cyberviolenza contro le donne

La Convenzione di Istanbul ancorché, come sopra riscontrato, fornisca un rilevante quadro giuridico per prevenire e combattere la dimensione digitale della violenza contro le donne e della violenza domestica, "si completa" con altri strumenti normativi pertinenti, quali, anzitutto, la Convenzione sulla criminalità informatica del Consiglio d'Europa che fornisce una serie di standard giuridicamente vincolanti per criminalizzare gli aspetti della violenza informatica, garantire le prove elettroniche e stabilire, altresì, una cooperazione transfrontaliera e internazionale per indagare e perseguire la violenza online contro le donne[11].

Tali fonti, come vedremo di qui a poco, possono integrarsi a vicenda in modo dinamico, nell'interesse superiore della vittima[12]: da un lato la Convenzione di Istanbul, il più ambizioso trattato sui diritti umani giuridicamente vincolante in tema di violenza contro le donne, alla cui stregua si riconosce la natura di "genere" della violenza anche nella sua dimensione digitale e online; dall'altro, la Convenzione di Budapest, il primo e più rilevante trattato internazionale giuridicamen-

[11] Cfr. uno studio realizzato nell'ambito del Consiglio d'Europa da Adriane van der Wilk, *Protecting women and girls from violence in the digital age - The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women*, dicembre 2021.

[12] La relazione esplicativa alla Convenzione sottolinea che quest'ultima coesiste armoniosamente con altri trattati, siano essi multilaterali o bilaterali. L'obiettivo principale della Convenzione è rafforzare la protezione delle vittime garantendo loro il più alto livello di protezione. Al riguardo, l'art. 71 sottolinea che la Convenzione non pregiudica "gli obblighi derivanti dalle disposizioni di altri strumenti internazionali" ratificati o da ratificare dalle parti "che contengono disposizioni relative a materie disciplinate dalla presente Convenzione" e l'art. 73 aggiunge che la Convenzione non pregiudica "le disposizioni di diritto interno e di altri strumenti internazionali vincolanti già in vigore o che possono entrare in vigore, in base ai quali sono o sarebbero riconosciuti dei diritti più favorevoli per la prevenzione e la lotta contro violenza sulle donne e la violenza domestica". Inoltre, l'art. 71, par. 2, prevede che "Le Parti alla presente Convenzione possono concludere tra loro accordi bilaterali o multilaterali relativi alle questioni disciplinate dalla presente Convenzione, al fine di integrarne o rafforzarne le disposizioni o di facilitare l'applicazione dei principi in essa sanciti".

te vincolante nell'ambito della criminalità informatica e delle prove elettroniche[13], il quale offre il potenziale per esercitare l'azione penale nei casi di violenza contro le donne[14].

Per di più la Convenzione di Budapest, attraverso una serie di disposizioni di diritto penale, affronta direttamente e indirettamente anche alcuni tipi di violenza online e agevolata dalla tecnologia: essa impone alle Parti di criminalizzare condotte che spaziano dall'accesso illegale, all'interferenza nei dati e nei sistemi, alla frode informatica, sino alla diffusione di materiale pedopornografico.

[13] La Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica è volta ad agevolare la lotta contro i reati compiuti avvalendosi di reti informatiche. Essa: 1) contiene disposizioni che armonizzano gli elementi del diritto penale sostanziale interno e le disposizioni collegate nel settore della criminalità informatica; 2) fornisce le competenze di diritto procedurale penale a livello interno necessarie per le indagini e l'esercizio dell'azione penale in relazione a tali reati, così come in relazione ad altri reati commessi per mezzo di un sistema informatico o laddove le prove siano in formato elettronico; 3) è volta a istituire un rapido ed efficiente regime di cooperazione internazionale.

[14] Il 24 dicembre 2024, l'Assemblea generale delle Nazioni Unite ha adottato la Convenzione sulla criminalità informatica (*Cybercrime Convention*), dopo cinque anni di negoziati da parte di un Comitato *ad hoc* istituito nel 2019 (*Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*; vedi Risoluzione 74/247 dell'Assemblea generale delle Nazioni Unite, del 27 dicembre 2019, sul contrasto all'uso di tecnologie dell'informazione e della comunicazione a scopi criminali). Promuovendo una più forte collaborazione internazionale, il trattato mira a combattere la criminalità informatica nel mondo digitale e fisico. Riconosce il grave danno che i reati informatici arrecano agli Stati, alle imprese, agli individui e alla società, e si concentra sulla loro salvaguardia da reati come il terrorismo, la tratta di persone, il traffico di droga e i reati finanziari online; sottolinea la necessità fondamentale di una maggiore cooperazione internazionale nella lotta alla criminalità informatica. Ciò include: facilitare l'assistenza tecnica, promuovere programmi di formazione e lo scambio di prove tra gli Stati per indagare e perseguire efficacemente i reati informatici. Inoltre, la Convenzione è il primo trattato globale che affronta specificamente la violenza sessuale contro i minori commessa attraverso le TIC. Infine, per affrontare in modo efficace la criminalità informatica e promuovere uno spazio digitale più sicuro per tutti, il trattato chiede agli Stati di sviluppare strategie e misure di prevenzione globali, che includano programmi educativi, riabilitazione dei rei, supporto alle vittime e misure per mitigare i rischi. Sarà aperto alla firma in una cerimonia formale ad Hanoi, Vietnam, nel 2025 ed entrerà in vigore 90 giorni dopo la ratifica da parte del 40° firmatario.

Ciononostante, resta il fatto che il campo della criminalità informatica[15] è, ad oggi, ancora in gran parte neutrale rispetto al genere, motivo per cui l'ampia portata e l'approccio globale della Convenzione di Istanbul potrebbero fungere da strumento vitale per un riconoscimento sistematico dell'esposizione delle donne alla violenza in tale campo.

Al riguardo, l'art. 49 della Convenzione di Istanbul sottolinea l'importanza di garantire che le indagini e i procedimenti giudiziari relativi a tutte le forme di violenza contro le donne siano svolti senza indebito ritardo nel rispetto dei diritti della vittima durante l'intero *iter* procedimentale penale[16], per raccogliere prove, aumentare i casi di condanna e porre fine alle impunità, il che rileva indubbiamente pure a fronte della cyberviolenza; inoltre, al paragrafo 2, prevede che siano adottate misure legislative o di altro tipo, in conformità ai principi fondamentali in materia di diritti umani e tenendo conto della violenza di genere per garantire indagini e procedimenti efficaci.

Ebbene tale disposizione indurrebbe ad una rinnovata lettura e ad un'applicazione "di genere" del testo della Convenzione di Budapest nella direzione di indagare e perseguire penalmente, nello specifico, la cyberviolenza contro le donne.

Inoltre, per quanto qui rileva, di indubbio rilievo è, altresì, il secondo Protocollo addizionale alla Convenzione di Budapest[17], non an-

[15] Il Consiglio d'Europa si occupa anche di altre minacce associate alla Rete: la Convenzione sulla prevenzione del terrorismo (2005) contiene disposizioni che trasformano in reato il reclutamento e l'addestramento di terroristi tramite Internet; la Convenzione di Lanzarote (2007) affronta lo sfruttamento sessuale e l'abuso di minori, anche in relazione all'ambiente online; la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale sulla protezione dei dati fornisce garanzie contro la raccolta e l'utilizzo illecito di dati personali (1981).

[16] Come si sottolinea nella Relazione esplicativa (par. 255) gli estensori hanno voluto evitare che agli incidenti di violenza contro le donne e di violenza domestica venga assegnata una bassa priorità nelle indagini e nei procedimenti giudiziari, circostanza che contribuisce notevolmente ad un senso di impunità tra gli autori di questi atti e ha contribuito a perpetuare alti livelli di accettazione di tali violenze.

[17] La Convenzione di Budapest è corredata dal primo Protocollo n. 189 relativo all'incriminazione di atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici del 28 gennaio 2003, in vigore dal 1° marzo 2006 e dal secondo Protocollo n. 224, adottato il 12 maggio 2022, ma non ancora in vigore.

cora in vigore, il quale intende fornire norme comuni a livello internazionale per rafforzare la cooperazione in materia di criminalità informatica e la raccolta delle prove in formato elettronico[18] ai fini delle indagini o procedimenti penali specifici[19].

[18] In particolare, il secondo Protocollo, definito dal Consiglio d'Europa uno strumento finalizzato a potenziare "*its legal arsenal*", in materia di contrasto alla criminalità informatica (Comunicato del 17 novembre 2021, Ref. DC 207(2021)), propone di affrontare alcune sfide nell'accesso alle prove elettroniche e nella cooperazione internazionale in conformità con lo stato di diritto e gli standard sui diritti umani, assicurando che i governi rispettino il loro obbligo di proteggere gli individui e i loro diritti nel cyberspazio. Propone di accelerare le procedure di mutua assistenza giudiziaria (MLA) che attualmente possono richiedere fino a 18 mesi, consentendo un accesso più efficiente da parte delle forze dell'ordine alle prove elettroniche archiviate in un'altra parte, compresi i mezzi per la cooperazione in situazioni di emergenza e per la cooperazione diretta tra una parte e un fornitore di servizi Internet situato in un'altra parte. Il secondo Protocollo faciliterebbe anche la divulgazione delle informazioni sulla registrazione del nome di dominio (a volte cruciali per identificare gli autori e chiarire la responsabilità) e risolverebbe alcune delle sfide poste dalla giurisdizione e dalla territorialità. In particolare, sul rapporto tra le previsioni del secondo Protocollo e la disciplina dell'Unione europea in materia di protezione dei dati personali, cfr. M. BUCCARELLA, *Digitalizzazione della cooperazione giudiziaria internazionale in materia penale e tutela dei dati personali nel diritto dell'UE: alla ricerca di una compatibilità (im)possibile*, in *Freedom, Security and Justice: European Legal Studies*, 2023, n. 2, p. 216 ss.

[19] Il secondo Protocollo contempla, oltre a previsioni di carattere più generale, specifiche disposizioni a carattere tecnico. In particolare, riconosce la necessità di una cooperazione rafforzata e più efficace tra gli Stati e con il settore privato, nonché di una maggiore chiarezza e certezza del diritto per i prestatori di servizi e altri soggetti per quanto riguarda le circostanze in cui possono rispondere alle richieste di divulgazione di prove elettroniche presentate dalle autorità giudiziarie penali di altre Parti. Previsioni in materia di indagini digitali interessano, pertanto, non solo le competenti autorità dei paesi, bensì anche prestatori di servizio privati, come i gestori dei *provider* o le società fornitrici dei servizi di telecomunicazione. L'applicabilità di alcune previsioni del secondo Protocollo anche nei confronti di tali soggetti si spiega in ragione della tipologia dei servizi erogati dai privati, consistenti per lo più in piattaforme digitali ove possono transitare (ed essere conservate) tracce o elementi determinanti ai fini della ricostruzione dei fatti di reato. Il Protocollo riconosce, inoltre, che un'efficace cooperazione transfrontaliera ai fini della giustizia penale, anche tra autorità del settore pubblico e soggetti del settore privato, richiede condizioni efficaci e solide garanzie per la tutela dei diritti fondamentali. A tal fine, segue un approccio basato sui diritti e prevede condizioni e garanzie in linea con gli strumenti internazionali in materia di

In tale contesto è, pertanto, ravvisabile, come vedremo, una proficua complementarità, sia sotto il profilo procedurale che sostanziale, tra disposizioni della Convenzione di Istanbul e disposizioni della Convenzione di Budapest ove applicabili, in merito alla tutela delle donne vittime di violenza online e facilitata dalla tecnologia.

3. *L'interazione tra le due Convenzioni in punto di indagini e misure procedurali*

Come anticipato, disposizioni della Convenzione di Budapest in materia di indagine e misure procedurali integrano disposizioni della Convenzione di Istanbul quando si tratta di perseguire la cyberviolenza contro le donne.

Per quanto concerne le misure procedurali si richiamano anzitutto gli artt. 16 (conservazione rapida di dati informatici immagazzinati) e 17 (conservazione e divulgazione rapide di dati relativi al traffico) di cui al titolo II della Convenzione[20], ovvero misure coattive per la conservazione rapida – per un periodo di tempo non superiore a 90 giorni, ma prorogabile, ed in regime di segretezza – di specifici dati elettronici immagazzinati per mezzo di un sistema informatico (art. 16)[21] e,

diritti umani, compresa la Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (1950). Poiché le prove elettroniche riguardano spesso dati personali, il Protocollo prevede, altresì, solide garanzie per la protezione della vita privata e dei dati personali. Per approfondimenti si rinvia a G.M. RUOTOLO, *Il Secondo Protocollo alla Convenzione cybercrime sulle prove elettroniche tra diritto internazionale e relazioni esterne dell'Unione europea*, in *Diritto Penale e Processo*, 2022, n. 8, p. 1022 ss.

[20] Titolo II *conservazione rapida di dati informatici immagazzinati*.

[21] Art. 16 *conservazione rapida di dati informatici immagazzinati*: "1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle competenti autorità di ordinare o ottenere in altro modo la protezione rapida di specifici dati informatici, inclusi i dati sul traffico, che sono stati conservati attraverso un sistema informatico, in particolare quando vi è motivo di ritenere che i dati informatici siano particolarmente vulnerabili e soggetti a cancellazione o modificazione. 2. Quando una Parte rende effettive le previsioni di cui al precedente paragrafo 1 attraverso l'ordine ad un soggetto di conservare specifici dati informatici immagazzinati che siano in suo possesso o sotto il suo controllo, la Parte deve adottare

misure ad esse strumentali (art. 17)[22]. Si tratta, in sostanza, di disposizioni sulla conservazione di dati informatici, inclusi quelli relativi al traffico già raccolti e archiviati dai titolari dei dati, come i fornitori di servizi, di cui è necessaria la conservazione a causa della propria volatilità.

Le prove di un reato possono, infatti, essere facilmente perse attraverso pratiche di gestione e archiviazione negligenti, manipolazione o cancellazione intenzionale o programmata di dati che non è più necessario conservare. Si consideri poi che i reati informatici o ad essi correlati vengono commessi in larga misura proprio a seguito della trasmissione di comunicazioni attraverso il sistema informatico. L'acquisizione di dati di traffico archiviati associati a comunicazioni passate può essere, quindi, fondamentale per determinare la fonte o la destinazione di una comunicazione risalente e identificare così i colpevoli. Oltretutto, anche se nessun singolo fornitore di servizi possiede dati di traffico sufficienti per poter determinare l'effettiva origine o destinazione della comunicazione, ciascuno di essi può essere in possesso di una parte rilevante che deve essere esaminata nell'insieme per identificare l'origine o la destinazione. A tal uopo l'art. 17 garantisce che, lad-

le misure legislative e di altra natura che siano necessarie per obbligare tale soggetto a proteggere e mantenere l'integrità di quei dati informatici per il periodo di tempo necessario, per un massimo di novanta giorni, per consentire alle autorità competenti di ottenere la loro divulgazione. Una Parte può prevedere che tale ordine possa essere successivamente rinnovato. 3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per obbligare il custode o la persona incaricata di conservare i dati informatici di mantenere il segreto sulla procedura intrapresa per il periodo di tempo previsto dal proprio diritto interno. 4. I poteri e le procedure di cui al presente articolo devono essere soggetti agli articoli 14 e 15".

[22] Art. 17 *conservazione e divulgazione rapide di dati relativi al traffico*: "1. Al fine di assicurare la conservazione dei dati relativi al traffico in applicazione di quanto previsto all'articolo 16 ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per: a. assicurare che la conservazione dei dati relativi al traffico sia disponibile nonostante uno o più fornitori di servizi siano stati coinvolti nella trasmissione di tale comunicazione; e b. assicurare la rapida trasmissione all'autorità competente della Parte, o al soggetto designato da tale autorità, di una quantità di dati relativi al traffico sufficiente per consentire alla Parte di identificare il fornitore di servizi e la via attraverso la quale la comunicazione fu trasmessa. 2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 1".

dove uno o più fornitori di servizi siano stati coinvolti nella trasmissione di una comunicazione, la rapida conservazione dei dati di traffico può avvenire tra tutti i fornitori di servizi.

In tale contesto vengono, altresì, in rilievo l'art. 18[23] relativo a misure coattive che consentano di acquisire la cognizione sia di specifici dati informatici, che siano in possesso o sotto il controllo di qualunque persona, immagazzinati in un sistema informatico o su un supporto informatico (art. 18.1a), sia di dati relativi agli abbonati[24], che siano in

[23] Art. 18 *ingiunzione di produrre*: "1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle autorità competenti di ordinare: a. ad un soggetto nel proprio territorio di trasmettere specifici dati informatici nella propria disponibilità o controllo, che siano immagazzinati in un sistema informatico in un supporto informatico per la conservazione di dati; e b. a un fornitore di servizi che offre le proprie prestazioni nel territorio della Parte di fornire i dati in proprio possesso o sotto il suo controllo relativi ai propri abbonati e concernenti tali servizi. 2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15. 3. Ai fini del presente articolo, l'espressione "informazioni relative agli abbonati" designa ogni informazione detenuta in forma di dato informatico o sotto altra forma da un fornitore di servizi e relativa agli abbonati ad un proprio servizio e diversa dai dati relativi al traffico o al contenuto e attraverso la quale è possibile stabilire: a. il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche prese a tale riguardo e il periodo del servizio; b. l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio; c. ogni altra informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio".

[24] Per "dati relativi agli abbonati" si intende ogni tipo di informazione, anche non in forma di dati informatici, riferita agli abbonati e diversa dai dati relativi al traffico o al contenuto, che permetta di accertare una serie di ulteriori dati. Nel corso di un'indagine penale, le informazioni dell'abbonato possono essere necessarie principalmente in due situazioni specifiche. In primo luogo, le informazioni dell'abbonato sono necessarie per identificare quali servizi e misure tecniche correlate sono stati utilizzati o sono utilizzati da un abbonato, come il tipo di servizio telefonico utilizzato (ad esempio, cellulare), il tipo di altri servizi associati utilizzati (ad esempio, inoltro di chiamata, posta vocale, ecc.), il numero di telefono o altro indirizzo tecnico (ad esempio, indirizzo e-mail). In secondo luogo, quando è noto un indirizzo tecnico, le informazioni dell'abbonato sono necessarie per aiutare a stabilire l'identità della persona interessata. Altre informazioni dell'abbonato, come le informazioni commerciali sui registri di fatturazione e pagamento dell'abbonato possono anche essere rilevanti per

possesso o sotto il controllo di un fornitore di servizi (art. 18.1b), i quali possono risultare fondamentali e contenere, tra le altre informazioni, l'indirizzo IP del presunto autore del reato; nonché l'art. 19[25] di cui al titolo IV sulla perquisizione e il sequestro di dati informatici archiviati, allo scopo di ottenere prove in relazione a specifiche indagini o procedimenti penali[26].

le indagini penali, in particolare quando il reato in esame riguarda frodi informatiche o altri reati economici.

[25] Art. 19 *perquisizione e sequestro dati informatici immagazzinati*: "1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di perquisire o accedere in modo simile: a. a un sistema informatico o parte di esso e ai dati informatici ivi immagazzinati; e b. a supporto per la conservazione di dati informatici nel quale i dati stessi possono essere immagazzinati nel proprio territorio. 2. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire che, qualora le proprie autorità perquisiscano o accedano in modo simile a specifici sistemi informatici o parte di essi, in conformità al paragrafo 1.a, e abbiano ragione di ritenere che i dati ricercati si trovino presso un altro sistema informatico o parte di esso nel proprio territorio, e a tali dati sia possibile legalmente l'accesso dal sistema iniziale, le stesse autorità possano estendere rapidamente la perquisizione o l'accesso all'altro sistema. 3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di sequestrare o acquisire in modo simile i dati informatici per i quali si è proceduto all'accesso in conformità ai paragrafi 1 o 2. Tali misure devono includere il potere di: a. sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici; b. fare e trattenere una copia di quei dati informatici; c. mantenere l'integrità dei relativi dati informatici immagazzinati; d. rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato. 4. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie per consentire l'applicazione delle misure di cui ai paragrafi 1. e 2. 5. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15".

[26] Il 17 gennaio 2025 è stato pubblicato il rapporto del Comitato per la Convenzione sulla criminalità informatica (T-CY). Nel documento, il Comitato ha fatto il punto sulle modalità con le quali gli Stati parte hanno attuato l'art. 19 della Convenzione. La lotta alla criminalità richiede interventi delle autorità inquirenti sui dati informatici archiviati, ma è necessario che le perquisizioni e la successiva confisca avvengano nel rispetto degli standard internazionali come affermati nella Convenzione

Infine, degne di nota sono le disposizioni di cui al titolo V: l'art. 20, relativo a misure che consentono la raccolta o la registrazione in tempo reale, in regime di segretezza, di dati relativi al traffico concernenti specifiche comunicazioni effettuate attraverso un sistema informatico, ovvero di dati sul traffico rilevanti ai fini delle indagini che indicano il numero di visitatori di un sito web, o quando i presunti sospettati si collegano e/o comunicano e tramite quale fornitore di servizi (*host* di posta elettronica, data, ora,…); e, altresì, l'art. 21[27] concernente misure che permettono, invece, in relazione a gravi reati, la raccolta o la registrazione in tempo reale, in regime di segretezza, di dati relativi al contenuto di comunicazioni avvenute tramite un sistema in-

di Budapest. Questo perché – precisa il Comitato nel rapporto del 12 dicembre 2024 – è indispensabile garantire la protezione dei diritti delle persone e, al tempo stesso, svolgere indagini adeguate. Le autorità, in particolare nei casi di criminalità informatica, "devono affrontare scenari complessi, come la perquisizione di sistemi connessi, copie dei dati anziché la confisca di interi sistemi o la rimozione di contenuti nocivi accessibili, ad esempio materiale contenente abusi sessuali sui minori". Malgrado le regole fissate nella Convenzione, gli Stati hanno diverse modalità di intervento e, quindi, il Comitato ha voluto catalogare le pratiche seguite nei diversi paesi per poi formulare raccomandazioni al fine di garantire un'uniformità negli interventi. In particolare, il quadro 4.2 raccoglie i diversi interventi legislativi, inclusi quelli dell'Italia, relativi all'attuazione nell'ordinamento interno dell'art. 19.

[27] Art. 21 *intercettazione di dati relativi al contenuto*: "1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie, in relazione ad una serie di gravi infrazioni che devono essere definite dal diritto nazionale, per consentire alle proprie competenti autorità di: a. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, e b. obbligare un fornitori di servizi, nell'ambito delle sue capacità tecniche a: i. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, o in tempo reale di dati relativi al contenuto di comunicazioni specifiche eseguite nel proprio territorio attraverso un sistema informatico. 2. Qualora una Parte, a causa dei principi del proprio ordinamento giuridico, non è in grado di applicare le misure previste al paragrafo 1.a, può invece adottare misure legislative e di altra natura che dovessero essere necessarie per assicurare la raccolta o la registrazione in tempo reale dei dati relativi al contenuto di comunicazioni specifiche eseguite sul proprio territorio, attraverso l'utilizzo di strumenti tecnici in quel territorio. 3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare un fornitore di servizi a mantenere segreto il fatto che un qualsiasi potere previsto nel presente articolo sia stato sia stato esercitato e ogni informazione relativa. 4. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15".

formatico. Trattasi di dati sensibili che contengono informazioni quali testi, immagini, foto, video, suoni, ecc., soggetti a norme di protezione dei dati più severe rispetto ad altre.

Ebbene, siffatti artt. da 16 a 21 della Convenzione di Budapest possono ritenersi complementari all'art. 50 della Convenzione di Istanbul che impone una risposta immediata nel contesto del perseguimento della violenza online e agevolata dalla tecnologia contro le donne, fornendo alle parti indicazioni più precise sulle misure da intraprendere per garantire le prove elettroniche nei procedimenti penali nei territori degli Stati parte. Articolo questo che, come puntualizza la relazione esplicativa della Convenzione di Istanbul, richiede misure legislative e di altro tipo necessarie per garantire alle autorità una reazione tempestiva e appropriata contro tutte le forme di violenza che rientrano nel campo di applicazione della Convenzione medesima, offrendo protezione idonea e immediata alle vittime (art. 50, par. 1), anche in termini di prevenzione, ivi compresa la raccolta di prove, oltre che misure operative di prevenzione (art. 50, par. 2)[28].

4. *Violenza digitale e online contro le donne tra cooperazione internazionale, mutua assistenza giudiziaria e accesso alle prove elettroniche in contesti transfrontalieri*

Altre disposizioni della Convenzione di Budapest vengono in rilievo per quanto concerne la cooperazione internazionale, la mutua assistenza giudiziaria e l'accesso alle prove elettroniche in contesti transfrontalieri, quali: l'art. 23 sui principi generali relativi alla cooperazio-

[28] Come precisa la relazione esplicativa della Convenzione di Istanbul (Istanbul, 11 maggio 2011), la conformità con l'obbligo di cui all'art. 50 comprende, ad esempio, quanto segue: il diritto delle autorità responsabili incaricate dell'applicazione della legge di entrare nel luogo ove si trovi una persona in pericolo; la cura e la consulenza alle vittime da parte delle autorità incaricate dell'applicazione della legge secondo opportune modalità; colloquio tempestivo con le vittime condotto da personale qualificato, ove opportuno femminile, in strutture atte a stabilire un rapporto di fiducia tra la vittima e il personale delle forze dell'ordine; garantire la presenza di un numero adeguato di funzionari donne delle forze dell'ordine, anche ad alti livelli di responsabilità.

ne internazionale, l'art. 25 sui principi generali relativi alla mutua assistenza[29] e gli artt. da 29 a 34 della Convenzione di Budapest.

Questi, come avremo modo di constatare, possono ritenersi complementari all'art. 62 della Convenzione di Istanbul, il quale stabilisce che le parti cooperano "nella misura più ampia possibile" quando si tratta di prevenzione, protezione e assistenza alle vittime e di indagini o di procedimenti relativi ai reati elencati nella Convenzione, nonché dell'esecuzione delle sentenze penali, compresi gli ordini di protezione. In sostanza, come si evidenzia nella relazione esplicativa della Convenzione di Istanbul, l'art. 62 obbliga le parti a ridurre, per quanto possibile, gli ostacoli ad una rapida circolazione delle informazioni e degli elementi di prova.

In tale ambito la cooperazione assume indubbia rilevanza specie quando una vittima sotto la giurisdizione di uno Stato parte inoltra una denuncia per un reato perpetrato in un altro Stato parte. La vitti-

[29] Art. 25: "1. Le Parti devono concedersi reciprocamente la più ampia mutua assistenza al fine delle indagini o dei procedimenti relativi ai reati relativi a sistemi e dati informatici o per la raccolta di prove in formato elettronico di reati. 2. Ogni Parte deve anche adottare le misure legislative e di altra natura che dovessero essere necessarie per l'adempimento degli obblighi assunti in base agli articoli da 27 al 35. 3. Ogni Parte può, in casi d'urgenza, fare richieste di mutua assistenza o comunicazioni ad essa relative attraverso strumenti rapidi di comunicazione, come il fax o la posta elettronica, a condizione che tali strumenti diano appropriate garanzie di sicurezza e autenticazione (inclusa la criptazione, se necessaria), seguite da conferma ufficiale ulteriore se lo Stato richiesto lo esige. Lo Stato richiesto deve accettare la domanda e rispondere alla richiesta con uno qualsiasi di tali mezzi rapidi di comunicazione. 4. Salva contraria disposizione espressamente prevista negli articoli del presente capitolo, la mutua assistenza è soggetta alle condizioni previste dalla legislazione della Parte richiesta o dai trattati di mutua assistenza applicabili, inclusi i motivi sulla base dei quali la Parte richiesta può rifiutare la cooperazione. La Parte richiesta non può esercitare il diritto di rifiutare la mutua assistenza in relazione ai reati menzionati negli articoli da 2 a 11 per il solo motivo che la richiesta riguarda un reato che essa reputa di natura fiscale. 5. Qualora, in conformità alle previsioni del presente capitolo, la Parte richiesta è autorizzata a subordinare la mutua assistenza ad una doppia incriminazione, questa condizione sarà considerata come soddisfatta, se il comportamento considerato reato per il quale la mutua assistenza è stata richiesta costituisca reato in base al proprio diritto interno, a prescindere dal fatto che la propria legislazione classifichi o meno il reato nella stessa categoria o lo denomini con la stessa terminologia della legislazione della Parte richiedente".

ma può, infatti, presentare denuncia, depositandola presso le autorità competenti dello Stato di residenza[30] e quest'ultime possono o avviare il procedimento se consentito dalla loro legislazione, o trasmettere la denuncia alle autorità dello Stato in cui è stato commesso il reato, in conformità alle disposizioni pertinenti degli strumenti di cooperazione applicabili ai paesi in questione[31].

In generale, ai fini della cooperazione internazionale, l'art. 23 della Convenzione di Budapest fissa tre principi fondamentali: in primo luogo, le parti devono cooperare le une con le altre nella misura più larga possibile; in secondo luogo la cooperazione deve estendersi a tutte le infrazioni penali legate a sistemi o dati informatici, così come alla raccolta delle prove sotto forma elettronica; in terzo luogo la cooperazione deve tener conto dell'applicazione degli strumenti internazionali pertinenti relativi alla cooperazione internazionale in materia penale e agli accordi fondati su legislazioni uniformi o reciproche e, altresì, del loro diritto nazionale.

Nello specifico, quanto disposto dalla Convenzione di Budapest contribuisce di fatto ad ampliare la capacità di accedere e preservare le prove elettroniche ed espandere i poteri investigativi nel contesto della mutua assistenza e della cooperazione internazionale.

Circa la mutua assistenza relativa a misure provvisorie, rileva l'art. 29 sulla conservazione rapida dei dati informatici, ai sensi del quale una parte può richiedere ad un'altra di ordinare od ottenere in altro modo la conservazione rapida di dati immagazzinati attraverso un sistema informatico, situato nel territorio di quest'altra parte e nei confronti della quale la parte richiedente intende avanzare una richiesta di mutua assistenza per la perquisizione, il sequestro o la divulgazione dei dati[32]. Ad esso si collega l'art. 30 sulla divulgazione rapida dei dati, il

[30] Il par. 2 dell'art. 62 si basa sull'articolo 11, parr. 2 e 3, della decisione quadro del Consiglio dell'Unione europea del 15 marzo 2001 sulla posizione delle vittime nei procedimenti penali.

[31] Così la relazione esplicativa della Convenzione di Istanbul con riferimento all'art. 62.

[32] Come si legge al punto 189 del Rapporto esplicativo alla Raccomandazione n. 13 del 1995 del Consiglio d'Europa, avente a oggetto "Problemi di diritto penale processuale connessi all'informazione tecnologica" (Raccomandazione R(95)13 adottata dal Consiglio dei Ministri degli Sati membri del consiglio d'Europa l'11 settembre

quale dispone che, se nel corso dell'esecuzione di una richiesta effettuata sulla base dell'art. 29, la parte richiesta scopra che un *service provider* di un altro Stato sia coinvolto nella trasmissione della comunicazione, la parte richiesta deve rapidamente trasmettere alla parte richiedente una quantità sufficiente di dati concernenti il traffico che consenta di identificare il *service provider* e la via attraverso la quale la comunicazione è stata effettuata.

Gli artt. da 31 a 34, inseriti nel titolo II *mutua assistenza relativa ai poteri d'indagine*, riguardano, invece, la cooperazione internazionale in materia di poteri investigativi e, rispettivamente, in tema di: divulgazione accelerata dei dati di traffico conservati quando vi è motivo di ritenere che questi siano particolarmente a rischio di perdita o modificazioni (art. 31)[33]; di accesso transfrontaliero da parte delle forze dell'ordine a dati informatici immagazzinati quando questi sono accessibili al pubblico, oppure con il consenso della persona legalmente autorizzata a divulgarli (che potrebbe essere il presunto sospettato) ex art. 32[34]; di mutua assistenza nella raccolta in tempo reale di dati rela-

1995), la maggioranza degli Stati mostrava grande diffidenza verso modelli di ricerca a livello di network effettuata nello Stato dove i dati fossero accessibili o conservati, intendendola come una violazione di sovranità dello Stato, nonché un'evidente deviazione dai passaggi obbligati della mutua assistenza convenzionale che sarebbe stata, così, aggirata.

[33] Art. 31 *mutua assistenza concernente l'accesso a dati informatici immagazzinati*: "1. Una Parte può richiedere ad un'altra Parte la perquisizione o altro simile mezzo di accesso, il sequestro o altro strumento simile, o la divulgazione dei dati immagazzinati attraverso un sistema informatico situato nel territorio della Parte richiesta, inclusi i dati che sono stati conservati in base all'articolo 29. 2. La Parte richiesta soddisfa la richiesta attraverso gli strumenti internazionali, gli accordi e le legislazioni alle quali si fa riferimento all'articolo 23, e conformandosi alle disposizioni del presente capitolo. 3. La richiesta deve essere soddisfatta al più presto possibile quando: a. vi è motivo di ritenere che i dati relativi siano particolarmente a rischio di perdita o modificazioni; o b. gli strumenti, gli accordi e le legislazione di cui al paragrafo 2 prevedano una cooperazione rapida".

[34] Art. 32 *accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili*: "Una Parte può, senza l'autorizzazione di un'altra Parte: a. accedere ai dati informatici immagazzinati disponibili al pubblico (fonti aperte), senza avere riguardo al luogo geografico in cui si trovano tali dati; o b. accedere o ricevere, attraverso un sistema informatico nel proprio territorio, dati informatici immagazzinati situati in un altro Stato, se la Parte ottiene il consenso legale e volontario

tivi al traffico, almeno per quanto concerne i reati per i quali tale raccolta sarebbe disponibile in un caso nazionale simile, per evitare che dati importanti vengano cancellati o eliminati dai fornitori di servizi (art. 33)[35], nonché, in materia di intercettazione di dati relativi al contenuto, ovvero di dati più sensibili, soggetti a privacy[36], che potrebbero costituire prove chiave in diverse indagini penali, compresi i casi di violenza contro le donne (art. 34)[37].

della persona legalmente autorizzata a divulgare i dati allo Stato attraverso tale sistema informatico". Si tratta di eccezioni al principio di territorialità, perché si consente, senza necessità di mutua assistenza, l'accesso a dati conservati all'estero.

[35] Art. 33 *mutua assistenza nella raccolta in tempo reale di dati sul traffico*: "1. Le Parti devono fornire mutua assistenza tra loro nella raccolta in tempo reale di dati sul traffico, associati a specifiche comunicazioni nel proprio territorio, trasmessi attraverso l'uso di un sistema informatico. Questa assistenza, soggetta alle disposizioni del paragrafo 2, è regolata dalle condizioni e dalle procedure previste dal diritto interno. 2. Tutte le Parti devono fornire questa assistenza almeno rispetto ai reati per i quali la raccolta in tempo reale dei dati sul traffico sarebbe possibile, in ambito interno, in una situazione analoga".

[36] In tale ambito viene in rilievo, altresì, la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, nota come "Convenzione 108+", che garantisce a ciascun individuo, nel territorio delle Parti che hanno ratificato la Convenzione, indipendentemente dalla nazionalità o residenza, il rispetto di diritti e libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento automatizzato di dati personali, nonché dei dati sensibili come quelli genetici e biometrici e prevede, altresì, il "diritto alla cancellazione". Trattato aperto alla firma degli Stati membri e all'adesione degli Stati non membri a Strasburgo il 28 gennaio 1981 ed entrato in vigore dal 1° ottobre 1985, e aggiornato nel 2018. Tale Convenzione rappresenta il primo strumento internazionale obbligatorio che ha per scopo la protezione delle persone contro l'uso abusivo del trattamento automatizzato dei dati di carattere personale, e che disciplina il flusso transfrontaliero dei dati. Oltre le garanzie previste per il trattamento automatizzato dei dati di carattere personale, essa bandisce il trattamento dei dati "delicati" sull'origine razziale, sulle opinioni politiche, la salute, la religione, la vita sessuale, le condanne penali, in assenza di garanzie previste dal diritto interno. La Convenzione garantisce anche il diritto delle persone di conoscere le informazioni catalogate su di loro e ad esigere, se del caso, delle rettifiche. Unica restrizione a tale diritto può aversi solo nel caso in cui sia presente un interesse maggiore (sicurezza pubblica, difesa, ecc.). La Convenzione impone anche delle limitazioni ai flussi transfrontalieri di dati negli stati in cui non esiste alcuna protezione equivalente.

[37] Art. 34 *mutua assistenza in materia di intercettazione di dati relativi al contenuto*: "Le Parti devono fornirsi mutua assistenza nella raccolta o registrazione in tempo reale

Infine, tornando alla Convenzione di Istanbul, valga evidenziare che l'art. 62 prevede che la mutua assistenza giudiziaria possa trovare una base giuridica pure nella stessa Convenzione, anche se gli Stati interessati non hanno concluso un altro trattato specificamente incentrato sulla mutua assistenza giudiziaria[38], incoraggiando in tal modo la cooperazione giudiziaria tra le Parti della Convenzione.

In sintesi, dunque, a livello di Consiglio d'Europa, la sinergia tra le due convenzioni offre il potenziale per sviluppare risposte coordinate al fenomeno della cyberviolenza contro le donne[39], anche sotto il

di dati relativi al contenuto di specificate comunicazioni trasmesse attraverso l'uso di un sistema informatico nella misura consentita dai trattati applicabili fra le stesse e dalle leggi interne".

[38] V. Convenzioni europee di estradizione e assistenza giudiziaria in materia penale, rispettivamente del 1957 e 1959, con i protocolli aggiuntivi.

[39] In tema, ai fini del contrasto alla cyberviolenza contro le donne, rilevano, altresì, atti di *soft law* come la Raccomandazione CM/Rec(2019)1 del Comitato dei Ministri agli Stati membri sulla prevenzione e la lotta contro il sessismo, adottata dal Comitato dei Ministri il 27 marzo 2019, in occasione della 1342esima riunione dei Delegati dei Ministri, che prevede una sezione specifica sull'incitamento all'odio sessista online. Tale raccomandazione contiene la prima definizione di sessismo concordata a livello internazionale, anche online e attraverso le nuove tecnologie. Ai fini della raccomandazione, si definisce sessismo: ogni atto, gesto, rappresentazione visiva, proposta orale o scritta, pratica o comportamento, fondato sull'idea che una persona o un gruppo di persone siano inferiori per via del loro genere, che si verificano nella sfera pubblica o privata, in Rete o fuori dalla Rete, aventi per oggetto o effetto: i. di violare la dignità o i diritti fondamentali di una persona o di un gruppo di persone; o ii. di provocare ad una persona o gruppo di persone danni o sofferenze di natura fisica, sessuale, psicologica o socio-economica; o iii. di creare un ambiente intimidatorio, ostile, mortificante, umiliante o offensivo; o iv. di ostacolare l'autonomia e la piena realizzazione dei diritti umani di una persona o gruppo di persone; o v. di mantenere e rafforzare gli stereotipi di genere. Inoltre, l'Assemblea parlamentare del Consiglio d'Europa ha adottato due risoluzioni sulla discriminazione informatica e l'odio online (Council of Europe (2017a), Parliamentary Assembly, *Resolution on ending cyberdiscrimination and online hate*, 25 gennaio 2017, disponibile su https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23456) e sulla fine della violenza sessuale e delle molestie contro le donne negli spazi pubblici (Council of Europe (2017b), Parliamentary Assembly, *Resolution on putting an end to sexual violence and harassment of women in public space*, del 27 giugno 2017, disponibile su http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23977&lang=en). Allo stesso modo, la Strategia per l'uguaglianza di genere 2018-2023 del Consi-

profilo della cooperazione internazionale, della mutua assistenza giudiziaria e dell'accesso alle prove elettroniche in contesti transfrontalieri, completandosi a vicenda, nell'ottica di una tutela effettiva.

5. *La rilevanza penale di forme di violenza digitale contro le donne ai sensi della Convenzione di Istanbul coordinate con disposizioni della Convenzione di Budapest*

La Convenzione di Istanbul rileva, altresì, sotto il profilo penalistico, atteso che molte delle forme di violenza contro le donne perpetrate attraverso mezzi digitali sono riconducibili alle condotte intenzionali che gli Stati parte della Convenzione sono già tenuti a criminalizzare, come la violenza psicologica (art. 33), lo *stalking* (art. 34) e le molestie sessuali (art. 40).

Anzitutto l'art. 33 della Convenzione di Istanbul descrive la violenza psicologica come "comportamento intenzionale che mira a compromettere seriamente l'integrità psicologica di una persona con la coercizione o le minacce".

Ebbene, a tal proposito, valga rilevare come tutte le forme di violenza contro le donne perpetrate nella sfera digitale hanno un simile impatto, talora anche in termini più significativi e, pertanto, sono qualificabili come "violenza psicologica". Oltretutto, forme di violenza psicologica già perpetrate nel contesto della violenza domestica finiscono per aggravarsi se combinate con le nuove tecnologie: ad esempio, partner attuali o precedenti possono abusare di quest'ultime per rintracciare dove si trovano le loro vittime.

Nell'articolo citato – giova poi osservare – si parla di "comportamento" piuttosto che di una singola condotta, volendo sottolineare la rilevanza penale di atti abusivi protrattisi nel tempo, all'interno della famiglia o al di fuori di essa. Ciononostante, atti di violenza individua-

glio d'Europa (Council of Europe, *Gender Equality Strategy 2018-2023*, March 2018, disponibile su https://rm.coe.int/prems-093618-gbr-gender-equality-strategy-2023-web-a5/16808b47e1) ha sottolineato la necessità di combattere la violenza contro le donne sia online che offline, affrontando gli stereotipi di genere e il sessismo, compresi l'incitamento all'odio sessista e le minacce sessuali online, in particolare sulle piattaforme dei social media.

li, che non sono punibili penalmente, possono comunque varcare la soglia della violenza psicologica se correlati, ad esempio, alla ripetizione facilitata da Internet: un commento provocatorio può diventare bullismo a sfondo sessuale se ripetuto o proveniente da un gran numero di persone[40].

E ancora, la violenza psicologica online può assumere anche la forma di intimidazione, minacce alla vittima o alla sua famiglia, insulti, diffamazione, incitamento al suicidio o all'autolesionismo, spesso rafforzati da meccanismi della mentalità mafiosa e dall'anonimato.

Un'ulteriore forma di violenza psicologica è, altresì, l'abuso economico, inteso come il controllo della capacità di una donna di acquisire, utilizzare e mantenere risorse. Esso si verifica solitamente nel contesto della violenza da parte del partner e ha un indubbio impatto negativo sulla salute delle vittime, come il rischio di povertà e un ridotto accesso all'assistenza sanitaria, oltre a costituire una minaccia al benessere finanziario e all'indipendenza della vittima, con gravi ripercussioni sulla sua integrità psicologica.

Sul piano digitale tale tipo di abuso può assumere la forma del controllo dei conti bancari e delle attività finanziarie della vittima attraverso l'Internet *banking*, come pure del danneggiamento del suo *rating* creditizio mediante l'utilizzo delle sue carte di credito senza autorizzazione o la firma di contratti finanziari a nome della vittima (locazioni, prestiti, ecc.).

In secondo luogo, la Convenzione di Istanbul all'art. 34 disciplina lo *stalking*, definendolo come "comportamento intenzionalmente e ripetutamente minaccioso nei confronti di un'altra persona, portandola a temere per la propria incolumità"[41]. E qui l'estensione della sua por-

[40] Ai sensi dell'art. 78, par. 3, della presente Convenzione, i singoli Stati o l'Unione europea al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, mediante dichiarazione inviata al Segretario generale del Consiglio d'Europa, possono precisare che si riservano il diritto di prevedere sanzioni non penali (es. ordinanza di restrizione), invece di imporre sanzioni penali, in caso di violenza psicologica (art. 33), oltre che in caso di *stalking* (art. 34), purché siano efficaci, proporzionali e dissuasive.

[41] Nell'ordinamento italiano il delitto di atti persecutori (c.d. *stalking*) è stato introdotto dal Decreto-legge n. 11 del 2009 che ha inserito l'art. 612-*bis* nel codice penale. Con il Decreto-legge n. 93 del 2013 è stata parzialmente ritoccata la disciplina della

tata alla sfera digitale è asserita proprio nella relazione esplicativa alla Convenzione medesima[42].

Al riguardo, il comportamento minaccioso può consistere nel seguire ripetutamente un'altra persona, ricercare una comunicazione indesiderata con la stessa o farle sapere che viene osservata. Ciò può tradursi sia nel seguire fisicamente la vittima, presentandosi sul posto di lavoro o negli altri contesti di riferimento (palestra, supermercato, scuola, …), sia nel seguirla nel mondo virtuale (*chatroom*, siti di social network, ecc.)[43], spiando la vittima sui vari social media[44] o su piattaforme di messaggistica, e-mail e telefono, rubando password, violando o hackerando i suoi dispositivi per accedere a spazi privati, installando *spyware* o applicazioni di geolocalizzazione, o monitorandola attraverso dispositivi tecnologici connessi tramite l'Internet delle cose (IoT), come gli elettrodomestici intelligenti. In tal caso le pratiche di *stalking* digitale possono includere minacce (di natura sessuale, economica, fisica o psicologica), danni alla reputazione, monitoraggio e raccolta di informazioni riservate sulla vittima, furto di identità, adescamento sessuale, impersonificazione della donna e molestie con complici per isolare la vittima.

In sostanza il *cyberstalking* perpetrato da un partner o un ex partner segue gli stessi modelli dello *stalking* offline e, pertanto, non è altro che una violenza facilitata dalla tecnologia.

fattispecie penale proprio in attuazione della Convenzione di Istanbul.

[42] Relazione esplicativa della Convenzione di Istanbul, cit., al punto 182 e 183 con riferimento all'art. 34: "Inoltre, un comportamento minaccioso include atti vandalici nei confronti di un'altra persona, tracce sottili di contatto con i beni personali della vittima lasciati dallo stalker, atti rivolti contro un animale domestico della vittima, l'uso di false identità o la diffusione online di false informazioni".

[43] Così al punto 182 della Relazione esplicativa della Convenzione di Istanbul, cit., ove, tra l'altro, si precisa che, il ricercare una comunicazione indesiderata con la vittima implica la volontà di un contatto diretto con essa attraverso qualsiasi mezzo di comunicazione, inclusi quelli informatici e, comunque attraverso le più recenti tecnologie.

[44] A. SCHIAVON, *La cyber-violenza maschile contro le donne: una nuova sfida per il diritto penale*, in *Studi sulla questione criminale*, 2019, n. 1-2, pp. 207-222. Secondo l'A. è indubbia la portata rivoluzionaria dei social media, tuttavia, essi manifestano un'evidente natura di Giano Bifronte: alle innumerevoli opportunità che lo spazio digitale offre si contrappongono altrettanti rischi e pericoli.

Infine, l'art. 40 della Convenzione di Istanbul disciplina le molestie sessuali, intendendo per tali "qualsiasi forma di comportamento indesiderato, verbale, non verbale o fisico, di natura sessuale, con lo scopo o l'effetto di violare la dignità di una persona, segnatamente quando tale comportamento crea un clima intimidatorio, ostile, degradante, umiliante o offensivo".

Anche in tale definizione sono riconducibili comportamenti online o digitali[45], come la condivisione pubblica non consensuale di foto/video di nudo o di natura sessuale di una persona, o minacce in tal senso, con scopo vendicativo, noti anche come pornografia vendicativa o *revenge porn*[46]; l'acquisizione, produzione o reperimento non consensuale di immagini o video intimi, compresi atti di *upskirting*[47] e *creepshots*[48]; la produzione di immagini alterate digitalmente in cui il volto o il corpo di una persona è sovrapposto o "cucito" a una foto pornografica o video, noti come "falsa pornografia"[49]; lo sfruttamento, la coercizione e le minacce, che includono forme di violenza come *sexting*[50], ricatti sessuali, minacce di stu-

[45] V. TEVERE, *Article 40 Sexual Harassment*, in S. DE VIDO, M. FRULLI (eds.), *Preventing and combating violence against women and domestic violence*, cit., p. 482 ss., in part. pp. 487-488.

[46] Tale termine destinato ad avere una valenza tecnica dal punto di vista della disciplina giuspenalistica, si deve alla definizione contenuta nell'*Urban Dictionary*, un dizionario online dedicato ai neologismi e alle espressioni *slang* della lingua inglese. Stando a tale fonte costituirebbe "*revenge porn*" "*l'homemade porn uploaded by ex girlfiend or (usually) ex boyfriend after particulary vicious breakup as a means of humiliating the ex or just for own amusment*".

[47] Dall'inglese *up*: su e *skirt*: gonna, è una forma di molestia sessuale che consiste nel riprendere, tramite una fotocamera o una telecamera posizionata sotto la gonna, la parte inferiore della figura femminile mettendone in evidenza la biancheria intima o la nudità. Tali immagini poi spesso vengono diffuse online senza il consenso dell'interessata.

[48] Fotografia di parti intime o di corpi in posizioni sessualmente allusive che vengono scattate in pubblico senza che la persona interessata ne sia a conoscenza.

[49] Vedi i "*deepfake*" che sono foto, video e audio creati grazie a *software* di Intelligenza Artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

[50] Dalla crasi dei termini inglesi *sex* e *texting*, pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o

pro, *doxing*[51] sessualizzato/di genere, furto d'identità e *outing*[52]; il bullismo a sfondo sessuale[53]; il *cyberflashing*[54].

Ancora una volta gli articoli della Convenzione di Istanbul citati possono essere arricchiti da una serie di disposizioni sostanziali della Convenzione di Budapest, alcune delle quali hanno una connessione diretta con la violenza contro le donne online e facilitata dalla tecnologia, specie con il *cyberstalking*, mentre altre criminalizzano atti che potrebbero facilitarla.

A tal uopo viene, innanzitutto, in evidenza l'art. 2 *accesso illegale ad un sistema informatico* che prevede l'adozione di misure legislative e di altro tipo necessarie per sanzionare come reato, in base alla propria legge nazionale, l'accesso all'intero sistema informatico o a parte di esso (*hardware*, dati memorizzati del sistema installato, *directory*, dati relativi al traffico e al contenuto) senza autorizzazione. Al riguardo, uno Stato parte può richiedere che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro.

Ebbene, l'accesso agli strumenti digitali di una vittima (computer, tablet, telefono o strumenti connessi) tramite *stalkerware* o *hacking* è senz'altro comune alle citate forme di violenza informatica (art. 33),

tramite Internet, app e/o social network.

[51] Il termine *doxing, o doxxing*, si riferisce alla pratica di cercare e diffondere pubblicamente online informazioni personali e private (come ad es. nome e cognome, indirizzo, numero di telefono ecc.) o altri dati riguardanti una persona, di solito con intento malevolo.

[52] La parola inglese *outing* indica la pratica di rendere pubblico l'orientamento sessuale o l'identità di genere di una persona in assenza del suo consenso.

[53] Il bullismo sessuale include comportamenti, quali diffusione di pettegolezzi o voci sul presunto comportamento sessuale di una vittima, pubblicazione di commenti a sfondo sessuale sotto i post o le foto della vittima, o esporre allo scoperto qualcuno senza il suo consenso allo scopo di spaventare, minacciare e fare *body-shaming* (derisione del corpo è l'atto di deridere e/o discriminare una persona per il suo aspetto fisico).

[54] Il *cyberflashing* consiste nell'invio di immagini di natura sessuale non richieste tramite applicazioni di appuntamenti o di messaggistica, messaggi di testo o utilizzando tecnologie *airdrop* o *Bluetooth*.

stalking online (art. 34) e a minacce informatiche (art. 40), alla stregua dell'interpretazione estensiva fornitane.

A seguire valga poi citare l'art. 3 sull'intercettazione abusiva di dati personali (non pubblici) di una vittima, sia installando un *software* sui suoi dispositivi per intercettare tali dati, sia introducendosi nei suoi dispositivi con mezzi tecnici (es. ascolto, monitoraggio, sorveglianza del contenuto delle comunicazioni, acquisizione del contenuto dei dati direttamente tramite l'accesso e l'uso del sistema informatico, o indirettamente tramite l'uso di dispositivi elettronici di intercettazione)[55].

Tale articolo presenta senza dubbio un collegamento con il *cyberstalking*, poiché criminalizza atti che potrebbero rientrare in questo tipo di violenza facilitandola, così come il traffico dei dati può preludere a violazioni della privacy, quali abusi e molestie sessuali basati sulle immagini.

E ancora, vengono, altresì, in rilievo l'art. 4 attentato all'integrità dei dati e l'art. 5 attentato all'integrità di un sistema che hanno una connessione facilitante e diretta con la cyberviolenza.

L'art. 4 impone, a livello nazionale, di configurare quale reato il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione, eventualmente prevedendo, ai fini della punibilità, che la condotta provochi un danno grave.

Nel contesto della violenza domestica, tale reato potrebbe imputarsi ad un partner o ex partner violento che distrugge o elimina gli strumenti, i dispositivi o i contenuti della vittima per una questione di controllo o vendetta, come pure la nozione di "danno grave" potrebbe intendersi quale circostanza aggravante, in termini di impatto sulla vittima.

Parimenti rileva l'art. 5 relativo al serio impedimento, senza alcun

[55] Art. 3 *intercettazione abusiva*: "Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici. Una Parte può richiedere che il reato venga commesso con intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico".

diritto, del funzionamento di un sistema informatico tramite l'introduzione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici intenzionalmente.

Di interesse è pure l'art. 6 sull'abuso di apparecchiature, ovvero sull'uso improprio di dispositivi o di password per computer, codici di accesso o dati simili tramite i quali è possibile accedere a tutto o a una parte di un sistema informatico, con l'intento di utilizzarlo allo scopo di commettere uno qualsiasi dei reati di cui sopra ex artt. 2-5; disposizione, questa, particolarmente rilevante nel contesto dello *stalkerware* per il tracciamento delle attività[56].

Infine, valga richiamare l'art. 8 della Convenzione di Budapest sulle frodi informatiche, che intenzionalmente e senza diritto causano un pregiudizio patrimoniale ad altri, mediante introduzione, alterazione, cancellazione o soppressione di dati informatici; oppure tramite qualsiasi interferenza nel funzionamento di un sistema informatico, con l'intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per sé stesso o altri.

A tal proposito si osserva che alcune forme di *sextortion*[57] ex art. 40 della Convenzione di Istanbul possono essere considerate frodi informatiche, in quanto i colpevoli estorcono immagini private o minacciano di farlo per esigere denaro dalle vittime, talvolta utilizzando strategie di *hacking*.

Ne emerge, dunque, sia pure alla stregua di una sommaria analisi, come la rilevanza penale di forme di cyberviolenza contro le donne ne esca "rafforzata" dal coordinamento tra disposizioni delle due Con-

[56] Come si legge nel glossario di cui allo studio realizzato nell'ambito del Consiglio d'Europa da Adriane van der Wilk, cit., lo *spyware* è un *software*, solitamente sotto forma di app scaricata sul telefono o dispositivo di qualcuno, utilizzato per tracciare le attività di quel dispositivo. Lo *spyware* è considerato *stalkerware* nel contesto della violenza domestica.

[57] Il termine *sextortion*, nato dalla combinazione dei termini *sex* ovvero sesso ed *extortion* cioè estorsione, letteralmente tradotto in italiano come estorsione sessuale o minaccia sessuale, indica una forma di ricatto, estorsione o alle volte truffa perpetuata su Internet utilizzando materiale multimediale sessualmente esplicito come forma di coercizione psicologica e non fisica per estorcere o barattare favori sessuali o denaro alla vittima.

venzioni, ai fini di un suo più efficace perseguimento in sede giurisdizionale.

6. *Considerazioni finali*

Come è emerso dalla presente disamina, sia sul piano procedurale che sostanziale, la lettura coordinata della Convenzione di Istanbul e della Convenzione di Budapest può contribuire all'efficace perseguimento della violenza online e facilitata dalla tecnologia ai danni delle donne che, allo stato, incontra numerose sfide.

Talune difficoltà derivano, senza dubbio, dall'assenza di un quadro giuridico nazionale adeguato a questa nuova dimensione della violenza di genere, quantomeno nell'attesa di recepire la direttiva 2024/1385, come pure da una giurisprudenza ancora poco incline ad una interpretazione *gender sensitive* delle leggi esistenti relative ai reati informatici o ai reati in materia di protezione dei dati personali.

Altre risiedono nella mancanza di formazione del settore della giustizia penale, nella tendenza alla minimizzazione o al trattamento individuale di ciascun tipo di aggressione in Rete, piuttosto che ad una valutazione dell'impatto cumulativo degli abusi subiti, sia online che offline.

Altre ancora derivano dalla conformazione stessa del cyberspazio, dalla natura elettronica delle prove che possono essere copiate o diffuse oppure, al contrario, cancellate o modificate con un semplice clic. E sul punto, oltre alla questione dell'ammissibilità delle prove elettroniche in tribunale, emerge l'estrema difficoltà, per le autorità di polizia, di ottenere prove cruciali da un altro paese o da un fornitore di servizi. Tra l'altro, siffatte prove possono anche essere archiviate nel *cloud*, causando problemi di giurisdizione.

Queste e altre sfide saranno, altresì, affrontate anche con il significativo apporto della *Cybercrime Convention* adottata il 24 dicembre 2024 dall'Assemblea generale delle Nazioni Unite, una volta ratificata[58].

Ad ogni modo, oggi, come sopra riscontrato, la dinamica intera-

[58] Si rinvia alla nota 14.

zione tra Convenzione di Istanbul e Convenzione di Budapest offre un interessante ed efficace quadro ai fini del contrasto alla violenza online e facilitata dalla tecnologia contro le donne, pur non menzionandola, sia dal punto di vista procedurale che sostanziale, oltre che sul piano della cooperazione internazionale, specie in punto di indagini che per la messa in sicurezza delle prove elettroniche.

Abstract

Sebbene la Convenzione di Istanbul non affronti specificamente la cyberviolenza, è tuttavia rilevante nel prevenire e combattere questa dimensione distinta ma non separata dalla violenza contro le donne, insieme ad altri strumenti normativi pertinenti, come la Convenzione sulla criminalità informatica del Consiglio d'Europa (Convenzione di Budapest). Quest'ultima, come noto, fornisce una serie di standard giuridicamente vincolanti per criminalizzare gli aspetti della violenza informatica, garantire le prove elettroniche e stabilire una cooperazione transfrontaliera e internazionale per indagare e perseguire, altresì, la violenza online e digitale ai danni delle donne.

KEYWORDS: Dimensione digitale della violenza contro le donne – violenza online – cyberviolenza – Convenzione di Istanbul – Convenzione di Budapest

CONVENIO DE ESTAMBUL Y CONVENIO DE BUDAPEST: UNA RESPUESTA COORDINADA AL FENÓMENO DE LA CIBERVIOLENCIA CONTRA LAS MUJERES

Aunque el Convenio de Estambul no se refiere específicamente a la ciberviolencia, es, sin embargo, relevante para prevenir y combatir esta dimensión distinta pero no separada de la violencia contra las mujeres, junto con otros instrumentos normativos pertinentes, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest). Este último, como es sabido, proporciona un conjunto de normas jurídicamente vinculantes para penalizar aspectos de la ciberviolencia, asegurar las pruebas electrónicas y establecer una cooperación transfronteriza e internacional para investigar y perseguir la violencia en línea y digital contra las mujeres.

PALABRAS CLAVE: Dimensión digital de la violencia contra las mujeres – violencia en línea – ciberviolencia – Convenio de Estambul – Convenio de Budapest

CIBERVIOLENCIA MACHISTA EN EL MARCO DE LA DIRECTIVA (UE) 2024/1385 Y CONVENIO DE ESTAMBUL: PERSPECTIVA DE GÉNERO Y OBLIGACIONES DEL ESTADO

Elena Martínez García [*]

SUMARIO: 1. Nuevo marco delictivo inabarcable dentro de las fronteras y soberanía de un estado. – 2. Planteamiento de las dificultades procesales a las que se enfrenta una víctima de ciberviolencia machista. – 3. La importancia de aplicar la perspectiva de género en la aplicación de normas relativas a la prevención y erradicación de la ciberviolencia ejercida contra una mujer. – 3.1. ¿Cuál es el objetivo o el *para qué* la perspectiva de género? – 3.2. ¿Qué no constituye la perspectiva de género? – 4. Consecuencias de no aplicar la perspectiva de género. – 4.1. Violencia institucional y perspectiva de género. – 4.2. Responsabilidad del Estado por falta de diligencia debida según el Convenio de Estambul. Caso *Buturugă contra Rumanía*. – 5. Contenidos concretos del deber de diligencia debida del Estado en materia de violencia contra las mujeres en la directiva, Convenio de Estambul y Convenio de Budapest. – 5.1. Normas con perspectiva de género. – 5.2. Prevención, sensibilización frente a las formas de violencia contra la mujer. – 5.3. Protección social. – 5.4. Protección y acción judicial. – 6. Breve reflexión sobre el daño para entender el momento de nacimiento de la falta de diligencia debida del Estado en esta materia. – 6.1. Incumplimiento de las obligaciones de respeto y obligaciones de no hacer. – 6.2. Incumplimiento de las obligaciones de hacer. – 6.2.1. Obligaciones de regulación, monitoreo y fiscalización. – 6.2.2. Obligaciones para garantizar la información y el acceso a la información. – 6.2.3. Obligación de declarar la alerta. – 6.2.4. Obligaciones integradas en el principio de precaución. – 6.2.5. Obligaciones de mitigar la situación que genera daños. – 6.3. El carácter inmediato de estas obligaciones y la obligación de progresividad y prohibición de regresividad. – 7. Conclusiones.

[*] Catedrática de Derecho procesal, Universitat de València. Correo-e: Elena.Martinez@uv.es. Este capítulo ha sido realizado en el marco del Proyecto I+D CIPROM 2023 64 (GV)

1. *Nuevo marco delictivo inabarcable dentro de las fronteras y soberanía de un estado*

En el momento actual es preciso revisar nuestra forma de afrontar el proceso penal y la función jurisdiccional, para preguntarnos si las normas existentes son suficientes para otorgar una tutela eficaz y garantista para los derechos de las víctimas de la ciberdelincuencia[1] y para la presunción de inocencia los agresores. ¿Es viable el paradigma clásico de tutela o nos adentramos en cambios profundos que afectan a ciertos elementos de la tutela procesal clásica, dada la especialidad de las agresiones online? ¿La perspectiva de género en este tipo de violencia machista debe ser una herramienta de interpretación de la realidad procesal para entender y reinterpretar la tutela de sus derechos cuando se produce en línea y con tecnología? Para contestar estas preguntas lo primero que debemos abordar es el marco normativo existente en la actualidad, un entramado complejo que con toda certeza requiere que el elemento tecnológico se adapte a la realidad de la violencia machista. A priori tenemos estas normas:

1) Convenio del Consejo de Europa sobre ciberdelincuencia (Convenio de Budapest 2001) jurídicamente vinculante complementado con Protocolos adicionales y por un Comité que vela por el cumplimiento del Convenio (T-CY).

2) Convenio de Estambul (2011)[2] y para el ámbito de la Unión europea disponemos de la directiva de violencia doméstica y de género (2024)[3]. Ambos deben de cohonestarse con el citado Convenio de Bu-

[1] Consejo de Derechos Humanos, Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos, A/HRC/38/47, 18 de junio de 2018. El informe revela el incremento que esta ciberviolencia machista ha tenido en los últimos años y, por tanto, la urgencia en afrontar su prevención y erradicación.

[2] Convenio del Consejo de Europa *sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, Estambul,* 11.V.2011, firmado por España el 1 de agosto de 2014.

[3] Directiva (UE) 2024/1385 del Parlamento europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica,* de 14 de mayo de 2024, en DOUE 1385 de 24 de mayo 2024, pp. 1-36.

dapest para abordar de forma eficaz la ciberdelincuencia machista, siempre aplicando la perspectiva de género como forma de remover obstáculos que, de aplicarse de forma neutra, impedirían otorgar la tutela judicial efectiva.

3) A su vez, directiva sobre violencia de género remite al reglamento de servicios digitales[4] (para plataformas de gran tamaño) (art. 2), básico para la retirada de contenidos digitales dañinos, y .al reglamento de inteligencia artificial[5], y podría ser de aplicación en determinados casos la directiva (UE) 2011/92 del Parlamento y del Consejo de 13 diciembre de 2011 relativa a los abusos sexuales y explotación sexual de los menores, pornografía infantil[6].

4) Igualmente, el reglamento (UE) 2023/1543 sobre las órdenes europeas de producción y conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales[7], así como la directiva (UE) 2023/1544 por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales[8].

5) Recomendación general núm. 35 del Comité CEDAW de 26 de

[4] Reglamento (UE) 2022/2065 del Parlamento europeo y del Consejo, *relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)*, de 19 de octubre de 2022, en DOUE 277 de 27 de octubre de 2022.

[5] Reglamento (UE) 2024/1689 del Parlamento europeo y del Consejo, *por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial),* de 13 de junio de 2024, en DOUE 1689, de 12 de julio de 2024, pp. 1-144.

[6] Directiva (UE) 2011/92 del Parlamento europeo y del Consejo, *relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, de 13 de diciembre de 2011,* en DOUE 335 de 17 de diciembre de 2011, pp. 1-14.

[7] Reglamento (UE) 2023/1543 del Parlamento europeo y del Consejo, *sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales,* de 12 de julio de 2023, en DOUE 191 de 28 de julio de 2023, pp. 118-180.

[8] *Ibidem.*

julio 2017, reconoce la violencia contra las mujeres a través de la tecnología, de manera transfronteriza, como acto de violencia agravada, dirigida a la mujer por el hecho de ser mujer, aunque sea por plataformas tecnológicas, redes sociales, móviles etc. Estructuralmente dicha violencia es la misma.

6) Recomendación del Consejo de Europa sobre la prevención y lucha contra el sexismo (27 de marzo 2019), reconociendo estos discursos de odio en el ciberespacio como forma de expresión y transmisión del sexismo en cualquiera de sus facetas.

7) Estrategia de la igualdad de género 2018-2023 y 2020-2025 del Consejo de Europa reconoce la discriminación y violencia contra las mujeres en línea, igualmente, a través de contenidos digitales, como fuente que alienta los estereotipos e incita al odio, que exige un marco de cooperación entre plataformas y otras partes interesadas para luchar contra la violencia de género en línea.

8) Propuesta de directiva de víctimas se encuentra en reelaboración e igualmente reconoce la especialidad de las víctimas en línea (COM 2023- 0424).

9) Código de conducta para la UE para la lucha contra la incitación ilegal al odio en internet, firmado el 22 de junio 2020 por Facebook, Instagram, TikTok, YouTube, Twitter, Microsot…*soft law* que debería ayudar, pero en la práctica parece que no se cumple.

En definitiva, se trata de un entramado complejo que arroja muchos vacíos por legislar[9], en un mundo tecnológico veloz que augura cierta anomia para la persecución de los delitos. Las pruebas electrónicas, así como los instrumentos europeos de la orden investigación y la orden de protección, aunque recién nacidos, parecen ya insuficientes[10].

¿Hasta qué punto le corresponde al Estado legislar adecuadamente para prevenir y erradicar esta violencia contra la mujer que se gene-

[9] Informe disponible en: https://violenciagenero.igualdad.gob.es/wp-content/uploads/GREVIO202411_First-thematic-evaluation-report_Spain_ES.pdf (fecha de consulta: 9 de enero de 2025).

[10] O. FUENTES SORIANO, *Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías*, en *Revista General de Derecho de Derecho Procesal*, 2018, n. 44, p. 3, disponible en Base de Datos Iustel: https://www.iustel.com/ (fecha de consulta: 9 de enero de 2025).

ra en el espacio virtual, sin fronteras, con una magnitud de daños inimaginable, una vulnerabilidad extrema para la mujer y los menores, especialmente? ¿Existe un deber de diligencia para los Estados de la UE destinado a hacerle responder, en caso de daño, si no ha actuado dentro de los estándares establecidos en el marco legal internacional y nacional? ¿Puede constituir una suerte de violencia institucional no cambiar las condiciones que alimentan esta violencia? ¿Existen obligaciones primarias y secundarias para el Estados recogidas en los acuerdos internacionales? En este concreto sentido, *La Sentencia del Tribunal Europeo del Caso Buturugă v. Romania* nos recuerda que, el alcance de la diligencia debida de los Estados, representa una nueva etapa para las administraciones públicas. Sobre estas cuestiones vamos a reflexionar en las líneas siguientes.

2. *Planteamiento de las dificultades procesales a las que se enfrenta una víctima de ciberviolencia machista*

La victimización que se produce de las mujeres y menores a través de la violencia en línea y facilitada por la tecnología tiene características muy específicas. Éstas impregnan todo el proceso de forma tal que, sin una perspectiva de género, es difícil asegurar el derecho de acceso a la justicia de estas víctimas y su tutela judicial efectiva de forma eficaz.

1. La primera característica es la muy posible ausencia de relación entre víctima y agresor, así como el tipo de relación, no necesariamente compatible con una relación común o habitual de la vida real.

2. El número de plataformas existente hace inabarcable la regulación de una vía única o común de intervención.

3. El perfil de los agresores, muy diverso y que normalmente se multiplica en el número de personas que se adhieren a la agresión, sin conexión a veces entre ellos para generar la intimidación sexual o los ataques en línea, agresores primarios y secundarios que responden a diferentes motivaciones incluso en la consciencia y determinación sobre el ejercicio del daño.

4. El grado de incidencia del daño es altísima, con reiteraciones y

permanencia irreparable en la red, que le va a marcar de por vida a esa persona, su entorno, su trabajo, salud mental, etc.

5. La identificación de la violencia que se sufre no es fácil. Las plataformas suelen dar información, pero poco clara y muy limitada, lo que desincentiva para denunciar o para responder la empresa.

6. Documentar la violencia es crucial, conservar el contenido ofensivo de los mensajes, fotografías, etc. La prueba va a ser uno de los elementos más complejos, teniendo que recurrir a la prueba indiciaria en muchas ocasiones, según planteará en este monográfico la profesora María José Jordán.

7. La denuncia se convierte en un acto complejo porque, en primer lugar, debe encontrarse la autoridad con sensibilidad para entender lo ocurrido, cuando muchas veces hay un aparente consentimiento de la víctima, requiere tener línea para poder presentar los materiales probatorios, lo que no siempre ocurre en zonas rurales remotas. Los estereotipos jugarán un importante papel a la hora de tramitar la denuncia correctamente para que dé lugar a una buena investigación del crimen.

8. La investigación tecnológica requiere mucha formación de los agentes de la autoridad y el poder judicial, así como mucha cooperación judicial y policial transfronteriza al encontrarse la información en nubes pertenecientes a muy diferentes jurisdicciones.

9. La cobertura legal de estas situaciones es determinante para el éxito de la tutela y reparación. Pero la transnacionalidad de las acciones, falta de jurisdicción supranacional, lentitud, hace que no se acaben denunciado muchos de estos delitos y ello deriva en una normalización de este tipo de crímenes, sin una beligerancia cultural mediática, y de las administraciones públicas, lo que los hace pensar en la responsabilidad del Estado por falta de diligencia debida al no remover los obstáculos que impiden la igualdad y la tutela de los derechos fundamentales.

10. Junto a la intimidación personal existe una intimidación ambiental. Este ciberespacio de interacción social fragiliza los marcos de protección de la intimidad, convirtiendo en víctimas vulnerables a las personas cuando, por accesos indebidos a datos personales, pierden de manera, casi siempre irreversible y frente a centenares o miles de personas, el control de la vida privada. Pero no solo. Cuando tales datos

se relacionan con la sexualidad, junto a la divulgación indiscriminada, y en especial si la víctima es mujer y a consecuencia de constructos sociales marcados muchas veces por hondas raíces ideológicas patriarcales y machistas, se activan mecanismos de red de criminalización, humillación y desprecio.

11. En especial, la dificultad probatoria por el especial marco del crimen por todo lo expuesto con anterioridad, acrecentado por el anonimato en red y la dificultad pericial de averiguar quién está detrás del crimen, manipulación de pruebas, la cantidad de elementos tecnológicos que impiden una accesibilidad sencilla a las fuentes de prueba veraces y a la protección real de la víctima y su reparación presente y futura[11].

12. Son delitos transfronterizos, que conllevan fuertes dificultades de prevención y sanción del crimen, unido a la temporalidad de los datos, desubicados en plataformas en países de difícil cooperación judicial en esta materia.

13. Derechos fundamentales en juego, puestos en peligro en las investigaciones transfronterizas y con una dificultosa falta de efectividad de medidas cautelares. Pensemos que estas fuentes de prueba se obtienen en países cuya regulación a la hora de obtenerlas, puede chocar frontalmente con nuestro nivel de legalidad constitucional, generando ilicitud de la prueba: secreto de las comunicaciones e intimidad de las personas (18.3 Constitución española), haciendo falta una autorización judicial, un reconocimiento judicial, aseguramiento de prueba, documental, acta notarial… Cuestiones de diferente tratamiento según ordenamientos jurídicos de corte anglosajón o europeo.

14. La prueba de WhatsApp, por ejemplo, supone que el servidor de mensajería instantánea no guarda información sino simplemente trafico.

15. El testimonio de la víctima será importante para coligar todos los elementos de prueba directa e indiciaria, sin merma de credibilidad de la relación entre víctima y agresor, siempre que se acrediten que no hay fines espurios ni secundarios.

16. Los testigos online validados por ministerio como prueba preconstituida.

[11] B. ROMO SABANDO, *La prueba digital en violencia de género*, en E. CERRATO GURI (dir.) *La prueba de la violencia de género y su problemática judicial*, Madrid, 2022, p. 286.

17. La doctrina en la STS núm. 744/2022, de 21 de julio (RJ\2022\4193), estableció que el acusado, al impugnar las conversaciones tanto de WhatsApp como de SMS que sirvieron de prueba de cargo para condenarle por un delito de amenazas a su expareja, debió acreditar él que, efectivamente, estábamos ante una prueba falsa a través de la correspondiente pericial, es decir, hay una inversión de la carga de la prueba en estos casos, no debiendo recaer en la parte acusadora sino en la parte impugnante de los mensajes.

Estas dificultades requieren de una interpretación con perspectiva de género, no genérica como si de cualquier delito se tratara. Su ausencia en la aplicación será fruto, en su caso, de la existencia de estereotipos y puede llegar a producir violencia institucional, porque el Estado, a través de sus poderes públicos y de las administraciones públicas, no ha cumplido con sus obligaciones de hacer, derivadas de los marcos internacionales de derechos humanos y normativa nacional que le obliga a remover todas las cusas que impiden a la mujer vivir en condiciones de igualdad y a no sufrir violencia por el hecho de ser mujer.

3. *La importancia de aplicar la perspectiva de género en la aplicación de normas relativas a la prevención y erradicación de la ciberviolencia ejercida contra una mujer*

Si ha hecho falta esta ingente cantidad de normativa internacional, europea y nacional para luchar contra la discriminación y violencia machista, es innegable que existe un reconocimiento global de la presente desigualdad estructural, que genera violencia hacia las mujeres ¿Cuál es el papel de las instituciones públicas del Estado y del poder judicial en esta lucha por la igualdad de la mujer? Como afirma Fiscalía General del Estado, la perspectiva de género "es un instrumento o metodología que permite identificar, cuestionar y valorar la discriminación y la desigualdad en el trato entre hombre y mujeres derivado de los roles sociales. La perspectiva de género permite una justicia libre de estereotipos y garantiza un adecuado derecho constitucional a la tutela judicial efectiva y a la igualdad efectiva"[12].

[12] *Guía de actuación con perspectiva de género en la investigación y enjuiciamiento*

En conclusión, la labor del poder judicial es clara y exige de este canon reforzado de investigación y enjuiciamiento (art. 49.2 Convenio de Estambul). Las sentencias modifican la realidad social, por eso, como afirma el magistrado Subijana Zunzunegui, "la perspectiva de género equivale a una protección reforzada de las mujeres en el orden penal, tanto sustantivo como procesal, a partir del especial desvalor predicable de una violencia del hombre que ratifica un modelo social de discriminación de la mujer"[13]. *Ello obliga* a la persona titular del orden jurisdiccional a que interprete y aplique las leyes penales con esta perspectiva de poder, tanto en la *investigación de los hechos* (delimitación de los mismos, la fijación de la significación jurídica del hecho, la determinación de sus efectos anudados o consecuencias jurídicas de protección), *en materia probatoria* (el objeto de la prueba y su valoración), así como en *el procedimiento* (averiguación de los hechos delictivos y enjuiciamiento, sentencia y ejecución de sentencia). Si a ello unimos las dificultades que trae consigo la tecnología y violencia en la red, esta protección reforzada exige aplica parámetros que entiendan y reflejen este tipo de violencia individual, alimentada por la cultura y en el espacio virtual. De hecho nuestro Tribunal Supremo, ya ha anulado sentencias absolutorias por delitos relacionados con la violencia de género, si la valoración de la prueba que condujo al órgano enjuiciador a la absolución, no se ha llevado a cabo con perspectiva de género[14].

3.1. *¿Cuál es el objetivo o el para qué la perspectiva de género?*

La prohibición de discriminar a las mujeres exige acciones afirmativas para desenmascarar una neutralidad axiológica establecida desde los inicios de la historia del proceso penal y la historia en general. "Interpretar y aplicar la norma con perspectiva de género es, por lo tanto, reconocer la plenitud de los derechos de las mujeres a desarrollar su personalidad de forma autónoma, en libertad, exenta de violencia.

de los delitos de violencia de género, Fiscalía General del Estado Español, 2020.

[13] I. J. SUBIJANA ZUNZUNEGUI, *La perspectiva de género en la interpretación de las leyes penales, sustantivas y procesales,* en *Revista del Parlamento Vasco,* 2024, n. 4, p. 114.

[14] *Tribunal Supremo, sentencia núm. 852/2021, de 4 de noviembre, Rec. 4725/2019, RJ\2021\5054.*

Desde este enfoque metodológico, la respuesta de un tribunal debería ser diferente", rompiendo esa falsa neutralidad (STC 48/2024, de 8 de abril Ponente Inmaculada Montalbán)[15]. Se trata, por tanto, *no de una opción sino de una obligación para el órgano jurisdiccional a la hora de resolver.*

"Juzgar con perspectiva de género no es más que hacer realidad en el quehacer jurisdiccional el derecho a la igualdad. Para llevar a cabo adecuadamente esta tarea, es necesario asumir, por lo menos, tres premisas básicas:

1. El fin del derecho es combatir las relaciones asimétricas de poder y los esquemas de desigualdad que determinan el diseño y ejecución del proyecto de vida de las personas.

2. El quehacer jurisdiccional tiene un invaluable potencial para la transformación de la desigualdad formal, material y estructural. Quienes juzgan, son agentes de cambio en el diseño y ejecución del proyecto de vida de las personas.

3. El mandato de la igualdad requiere eventualmente de quienes imparten justicia un ejercicio de deconstrucción de la forma en que se ha interpretado y aplicado el derecho"[16].

Es decir, no se trata de afectar la naturaleza del proceso y sus garantías procesales; sino de desmontar una falsa neutralidad de la norma que afecta negativamente a un colectivo, si no se introduce una perspectiva diferente, que acabe con los posibles sesgos que tiene la norma y/o la función jurisdiccional destinada a aplicarla. *No se trata de legislar para las mujeres, sino de romper la estructura legal y social que*

[15] Son numerosos los pronunciamientos de nuestro Tribunal Constitucional español, donde ha afirmado que el "obligatorio tratamiento diverso de situaciones distintas en un Estado social y democrático de derecho, para la efectividad de los valores que la Constitución consagra con el carácter de superiores del ordenamiento, como son la justicia y la igualdad" (Tribunal Constitucional, sentencia núm. 31/2018, de 10 de abril entre otras muchas), por lo que da sentido al art. 9.2 CE, cuando impone a los poderes públicos la obligación de remover los obstáculos que impiden la igualdad. En tal sentido se pronuncia la Recomendación 33 de CEDAW sobre el acceso de las mujeres a la Justicia.

[16] Protocolo para Juzgar con Perspectiva de Género, Haciendo Realidad el Derecho a la Igualdad, México, 2013, p.81.

hilvana una sociedad que las ha excluido siempre[17]. Introducir la perspectiva de género en un proceso no atenta contra la presunción de inocencia, como garantía jurisdiccional de protección del acusado[18]. Y por supuesto, el instrumento a través del que se ejerce la violencia, la red y la tecnología, tampoco afecta a las garantías procesales del acusado, pero sí a determinados aspectos procesales cuyas dificultades probatorias pueden perjudicar precisamente a las víctimas.

3.2. *¿Qué no constituye la perspectiva de género?*

Tal vez es más sencillo comenzar explicando lo que no es perspectiva de género, a tal fin, me parece muy certeras las palabras del Protocolo para Juzgar con Perspectiva de Género creado por la Corte Suprema de México[19]:

[17] E. BODELÓN GONZÁLEZ, *Feminismo y Derecho: mujeres que van más allá de lo jurídico* en *Género y Dominación*, 2009, pp. 95-116.

[18] I. J. SUBIJANA ZUNZUNEGUI, *op. cit.,* p. 6. En ningún caso podemos anudar estas ideas, porque conllevaría la negación de la idea de Justicia, remoción de la discriminación, la imparcialidad objetiva y subjetiva y las bases del proceso penal. Según Subijana, ambos -la protección de la víctima y la defensa del imputado- son instrumentos del proceso penal, que constituyen "estatutos jurídicos que integran el estándar del juicio justo (Tribunal europeo de derechos humanos, sentencia de 5 de octubre de 2006, *Marcello Viola c. Italia* y Tribunal de Justicia de la Unión europea, sentencia de 29 de julio asunto C-38/2018)". Ambos conllevan obligaciones para el Estado –a través de sus representantes en el Poder Judicial- en favor de las dos partes del proceso. "Esta exigencia obliga a implementar un proceso de comunicación que se adapte a las circunstancias y condiciones personales de la mujer víctima de violencia de género, así como la naturaleza concreta del delito sufrido por ella (arts. 5.1 y 20 LEVD)" (p.6). Ello tiene que hacer entender al órgano jurisdiccional que el contacto visual con el sospechoso puede ser un impedimento para hablar – como lo ha sido durante años hasta denunciarle –, o razón suficiente para admitir la prueba preconstituída, para necesitar del acompañamiento de una psicóloga, modificando las formas en las que se le interpela en su declaración, entendiendo las dificultades en declarar contra quien ha sido tu amor o el padre de tus hijos,…etc. evitando la victimización secundaria, porque ésta es violencia institucional que le impide ejercer su derecho a la tutela judicial efectiva (art. 24.2 CE y 2 y 3 del CEDH), porque en puridad no son mecanismos de tutela "efectiva" (Tribunal europeo de derechos humanos, sentencia de 2 de marzo de 2017, *Caso Tapis c. Italia*).

[19] C. PALOMO CAUDILLO, *Juzgar con perspectiva de género: de la teoría a la práctica*,

"a.- Juzgar con perspectiva de género no implica darles la razón a las mujeres siempre y bajo cualquier circunstancia, sino que implica identificar los factores estructurales que generan desventajas políticas, económicas, sociales y estructurales para las mujeres, impidiéndoles alcanzar una igualdad sustantiva de derechos.

b.- La perspectiva de género no es sólo un instrumento para las mujeres, no solo es pertinente en casos relacionados con mujeres. Lo que determina si en un proceso se debe aplicar o no es la existencia de situaciones asimétricas de poder, o bien de contextos de desigualdad estructural basados en el sexo, el género, las preferencias u orientaciones sexuales, entre otros".

c.- Y personalmente añado que, no constituye la aplicación correcta de la perspectiva de género, la afectación del estatuto de garantías del imputado, es decir, en la mayoría de las ocasiones, la aplicación de la perspectiva de género es la forma de solución a un sesgo, cuyo origen puede estar en el propio actuar del propio Estado, estereotipado y poco formado, con un desgaste del sistema con la consecuente defraudación de las expectativas que la intervención penal crea en la mujer (victimización secundaria) (Tribunal Constitucional, sentencia núm. 87/202, de 20 de julio de 2020)[20].

En conclusión, la perspectiva de género no sólo es afectar al proceso penal y la prueba, sino – sobre todo – es revisar la función jurisdiccional y sus sesgos posibles, la falta de medios que aboca a la judicatura hacia el desbordamiento y, por tanto, a la posible victimización secundaria, a la ausencia de apoyos intraprocesales para las víctimas que requerirían declarar con asistencia de personas expertas…Es decir, entendemos que esta idea no siempre es sencilla en su aplicación práctica. Por ejemplo, una cosa es que el sistema no deba cuestionar la veracidad del relato de la mujer con el fin de evitar que prejuicios (de género), puedan conducir a una cierta pobreza en la recepción y trámite de las denuncias, o en una investigación inadecuada que aporte escasa fuente de prueba, etc., y, otra bien distinta es que deba presumirse siempre y con un sentido acrítico que lo que se manifiesta la víctima

en *Revista Saber y Justicia*, 2021, n. 1(19), pp. 37-52.

[20] Sobre el derecho a obtener una investigación suficiente y con perspectiva de género, donde se ve la aplicación de esta herramienta de manera extensa y adecuada.

(mayor de edad o menor de edad) o la documentación que presenta sea siempre verdadera. Esto no es perspectiva de género y anula el sentido de la función jurisdiccional. Se puede concluir, por tanto, que desde el derecho y a través de su aplicación, se puede coadyuvar al mantenimiento de esta discriminación[21], sin una consciencia de la existencia de prejuicios y estereotipos. Por tanto, no se trata de legislar para las mujeres, sino para lograr la igualdad efectiva entre las mujeres y los hombres, removiendo los obstáculos que impiden dicha igualdad[22]. El denominado "poder transformador de las sentencias" es la forma de *deconstruir* la realidad de la norma jurídica y su hermenéutica en torno a lo masculino singular, olvidando las singularidades de las mujeres en sus derechos materiales y procesales. Analizado el contexto de posibles prejuicios, el proceso penal tiene sus reglas y garantías, sin las cuales no existe el mismo. En definitiva, en última instancia para ser eficaces en la aplicación de la perspectiva de género, se requiere, como afirma la profesora Mónica Martínez López en esta obra en el capítulo "Una (re)visión constitucional de los derechos clásicos y emergentes ante nuevas formas de ciberviolencia contra la mujer".

4. *Consecuencias de no aplicar la perspectiva de género*

El art. 49.2 del Convenio de Estambul establece un canon reforzado de investigación de delitos contra las mujeres[23], de otra forma éste no cumple con lo que le es exigible para otorgar la tutela judicial efectiva. Para lograr este objetivo debemos librarnos de los estereotipos de género en el ejercicio de la función jurisdiccional y policial, porque su existencia puede constituir violencia institucional y victimización secundaria inapropiada e intolerable.

[21] J. A. GARCÍA AMADO, *¿Tienen sexo las normas? Temas y problemas de la teoría feminista del Derecho,* en *Anuario de Filosofía del derecho IX*, 1992, p. 14.

[21] E. BODELÓN GONZÁLEZ, *op. cit.* pp. 95-116.

[22] *Ibidem.*

[23] Muy interesante los principios que debe regir al Fiscal en materia de investigación en violencia machista (p.14).

4.1. *Violencia institucional y perspectiva de género*

Existen las obligaciones judiciales de proteger a la víctima y facilitar su relato para que sea compatible con un juicio justo y aquí es donde la perspectiva de género puede tener cabida. Es decir, actuar de forma generalista en la toma de declaración, obtención de fuentes de prueba o práctica de la misma, puede dejar al proceso sin prueba y dañar, por tanto, a la víctima. Aquellas acciones judiciales que pueden generar duda, siguiendo los estándares clásicos procesales, pueden llegar a suponer una falta de comprensión de esta necesidad de protección reforzada de la víctima, "por venir su ambigüedad del especial desvalor predicable en la sociedad de este tipo de personas" (Subijana Zunzunegui). Y ello ocurre porque no tenemos consciencia de los numerosos estereotipos que día a día forman parte de nuestras creencias más arraigadas y que expresamos de forma sutil. Es decir, el daño producido a una víctima fruto de una falta de "contextualización" de los hechos, debido a una valoración *neutra* de las fuentes de prueba, podrían llevar a una denegación de "protección" adecuada, por no apercibirse el órgano jurisdiccional "del especial desvalor predicable de una violencia del hombre que ratifica un modelo social de discriminación de la mujer", o de las dificultades que una víctima tiene a la hora de declarar hechos violentos de esta naturaleza; nunca olvidemos que es una testigo, pero además una víctima y esta doble condición transforma la forma de vivir y narrar los hechos y los mecanismos íntimos de interpretación judicial de la prueba.

Esta es una obligación judicial, de fiscalía y de las fuerzas y cuerpos de seguridad del Estado. Y no solo alcanza a los estereotipos, también la falta de sensibilidad, el propio desbordamiento que el personal de justicia tiene si hay falta de medios personales o materiales, la dilación injustificada…todo ello puede hacer sentir la victimización secundaria de la mujer y su arrepentimiento de estar metida en el proceso judicial, incluso llegando a retirar la denuncia, dando una versión afectada, de poca calidad, etc. si no se compensa con un apoyo comprensivo de su específica situación. Pero nunca olvidemos que cierta victimización en el proceso penal siempre se da, para cualquier tipo de delitos. Es una suerte de mal necesario llegar a la verdad formal o procesal en juicio. No por ello es inexigible al Estado una mayor diligen-

cia en su actuación para no dañar –también – institucionalmente a las personas. La falta de perspectiva de género – dado que su aplicación es obligatoria – puede conllevar responsabilidad para el Estado por no remover los obstáculos desde una perspectiva estructural o sistémica, es decir, por no formar y sensibilizar a la judicatura para abordar los cambios que exigen remover de forma efectiva la discriminación y la desigualdad[24]. Se ha de interpretar los deberes de la administración pública, así como los del Poder judicial en prevenir, reparar y castigar con una perspectiva que le dote de verdadera "efectividad" a sus derechos y a los riesgos que se pretende evitar (arts. 13, 544-*bis*, 544-*ter*, 282, 449-*bis*, y *ter*, 703-*bis*, 730.2, 416 Ley de enjuiciamiento Criminal Española). Porque habrá un daño causado a partir de la no diferenciación por causas de género, porque había obligación de actuar de forma diferente a lo ordinario y no se hizo. Se puede llegar a tratar como supuestos de violencia institucional.

Todo ello nos lleva a entender qué si lográramos detectar los estereotipos de género, podríamos modificarlos de antemano y cambiar así las decisiones irracionales y con posibles sesgos, eliminando finalmente la discriminación. Ello nos debe hacer ver que, a mayor prevención en estereotipos, menor intervención en el derecho procesal y el proceso penal.

4.2. *Responsabilidad del Estado por falta de diligencia debida según el Convenio de Estambul. Caso* Buturugă contra Rumanía

Sabemos que la perspectiva de género viene establecida en el Convenio de Estambul y la directiva para la erradicación de la violencia doméstica y de género citadas. Dicha perspectiva es un instrumento de interpretación de la realidad, también la normativa y la procesal, para desenmascarar una falta de neutralidad si se aplican las normas de forma lineal, sin contemplar las especificidades de determinadas personas vulnerables hacia el sistema preestablecido hegemónicamen-

[24] Tribunal Supremo, sentencia n. 1263/2018, del 17 de julio 2018, reconoce la vulneración de derechos fundamentales de la madre. Vía de aplicación de las resoluciones del Comité de la CEDAW de la ONU.

te[25]. Por tanto, es una obligación su uso tanto para los diferentes poderes públicos, administraciones públicas y la judicatura. A través de su aplicación se remueven los obstáculos que impiden la igualdad, tanto desde una perspectiva estructural o sistémica, como respecto de la tutela individual de los derechos. Esto que decimos entronca directamente con el deber de diligencia que tienen los Estados para actuar garantizando los derechos de las mujeres a vivir una vida libre de violencia. Y esto es aplicable a la normativa reguladora de la prevención de la violencia online que sufren en las relaciones de pareja o ex pareja, entre otras muchas.

Centrándonos ahora en el Convenio de Estambul, del análisis de los arts. 4 y 5 podemos comprobar que se reconoce esta doble estructura para la prevención y erradicación de la violencia machista. No olvidemos que el derecho internacional de los derechos humanos forma parte del sistema de fuentes a aplicar por nuestra jurisprudencia, así como por el poder ejecutivo y legislativo a la hora de generar leyes y políticas públicas.

Procedo a realizar el análisis de estos dos artículos del Convenio de Estambul que recogen esta triple relación Estado-Sociedad-Ciudadano[26].

El art. 4, bajo el enunciado derechos humanos, igualdad y no discriminacion se establecen las *Obligaciones de hacer* de naturaleza "legislativa", o "de cualquier otro tipo", llegando a "de prohibir e, incluso, sancionar" o "de derogar leyes y prácticas", "que impidan vivir a mujer a salvo de la violencia en el ámbito público y privado".

[25] E. MARTÍNEZ GARCÍA, *Juzgar en el siglo XXI*, Valencia, 2024.

[26] L. FERRAJOLI, *Poderes salvajes. La crisis de la democracia constitucional*, 2013, p. 29. Estas garantías de un derecho fundamental son complejas y variadas. Ferrajoli las define en dos grupos y ambos integran siempre el derecho fundamental. En primer lugar, existen las *garantías primarias* de los derechos fundamentales que consisten en las prohibiciones de hacer (en *los derechos de libertad o status libertatis*), por lo que actúan a modo de *garantías negativas* para que los derechos no sean lesionados por otros; junto a ellas, existen *garantías positivas* que exigen prestaciones activas de otros para no ser lesionados dichos derechos. En segundo lugar, este autor citado denomina *garantías secundarias* a *las garantías de proteccionabilidad o justiciabilidad*, es decir, el derecho a la tutela judicial efectiva de nuestro art. 24 CE (lo que constituyen los derechos derivados de su *status activus procesualis*).

Por su lado, el art. 5 párrafo 1, bajo el titulo obligaciones del estado y diligencia debida, regula la *Obligación de abstenerse de hacer* por poderes públicos "Cualquier acto de violencia por autoridades, agentes e instituciones estatales, así como demás actores en nombre del Estado". Con ello, se limita la libertad de los poderes públicos, onde un "hacer" que viole los derechos de las mujeres, constituiría una transgresión de este derecho humano, una violación de carácter institucional por parte de los poderes públicos. De esta forma, no solo debemos pensar en, por ejemplo, un daño físico o sexual a una mujer por parte de un agente de policía, sino que estaríamos ante un plano más institucional y de incumplimiento de garantías objetivas, cuando las administraciones públicas dan un mal servicio, no derogan prácticas discriminatorias, no forman a los aplicadores de las normas con perspectiva de género, etc.

Por último, este mismo art. 5 párrafo 2, establece un nuevo mandato hacia los poderes públicos de los que se predica que "Actuarán con diligencia debida para prevenir, investigar, castigar e indemnizar por los actos de violencia, tanto los cometidos por agentes públicos como los realizados por actores no estatales". Extiende, por tanto, la obligación del Estado de ser diligente (y responsable) por los daños producidos -ahora sí- a sujetos (mujeres) concretos, cuando en el ejercicio de su derecho a la integridad física o de su familia, al restablecimiento de su derecho por la Judicatura, no se haya prevenido, investigado, castigado e indemnizado correctamente. Y esa hora donde surge un elemento trascendental, a saber, no solo por los actos de los poderes públicos que traen causa directa en su daño, sino por el daño que trae causa directa en la acción de sujetos no estatales[27]. Este derecho

[27] Estos sujetos no estatales deben ser objeto de estudio; si bien al principio me planté la posibilidad de que la norma se refiriera a empresas que gestionan aspectos de la violencia de género por encomienda de las administraciones públicas (puntos de encuentro, hospitales privados, empresas que gestionan sistemas de protección…), he acabado concluyendo que en este apartado debe integrarse la responsabilidad por los daños y la falta de reparación de la persona maltratadora. A ello apunta también la nueva propuesta de directiva de víctimas (Propuesta de directiva por la que se modifica la directiva (UE) 2012/29, por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y por la que se sustituye la decisión marco 2001/220/JAI del Consejo, *relativa al estatuto de la víctima en el proce-*

humano llega al punto de hacer responsable a la Administración por la falta de reparación a una víctima. Es el principio "Solve et repete".

Esto que decimos lo veremos al analizar el caso *Ángela González Carreño*[28] y más someramente en el Caso *Buturugă contra Rumanía*[29], donde por unanimidad se reconoce la violación de los derechos de la víctima por no aplicar dicha perspectiva de género.

"El alto Tribunal se refiere a la existencia de obligaciones positivas de hacer, tales como la investigación efectiva de los hechos. Y para ello, no basta con una investigación neutral, sino que exige el uso de la perspectiva de género para entender verdaderamente lo ocurrido y lo que debe de hacer las fuerzas y cuerpos de seguridad, la judicatura (art. 3 CEDH). Igualmente, se incumplió el artículo 8 CEDH sobre el respeto de la correspondencia, que no se conjugo con el Convenio de

so penal, de 15 de marzo de 2001, en DOCE 82 de 22 de marzo de 2001, pp. 1-4 (COM(2023)0424 – C9-0303/2023 – 2023/0250(COD). Vid. Considerando 9).

[28] La sentencia reconoce la condena y reparación en dos niveles que son coincidentes con la estructura defendida en este trabajo.

"a) Desde un plano de protección *individual* de la víctima de violencia machista y de la violencia institucional: i) Otorgar a la autora una reparación adecuada y una indemnización integral y proporcional a la gravedad de la conculcación de sus derechos; 600.000 eur; ii) Llevar a cabo una investigación exhaustiva e imparcial con miras a determinar la existencia de fallos en las estructuras y prácticas estatales que hayan ocasionado una falta de protección de la autora y su hija, debiendo comunicárselo a ella como parte de la reparación.

b) Desde un plano general o *sistémico*: i) Tomar medidas adecuadas y efectivas para que los antecedentes de violencia doméstica sean tenidos en cuenta en el momento de estipular los derechos de custodia y visita relativos a los hijos, y los derechos de visita o custodia no ponga en peligro la seguridad de las víctimas de la violencia, incluidos los hijos. El interés superior del niño y el derecho del niño a ser escuchado deberán prevalecer en todas las decisiones que se tomen en la materia; ii) Reforzar la aplicación del marco legal con miras a asegurar que las autoridades competentes ejerzan la debida diligencia para responder adecuadamente a situaciones de violencia doméstica; iii) Proporcionar formación obligatoria a los jueces y personal administrativo y sobre los estereotipos de género, así como una formación apropiada con respecto a la Convención, su Protocolo Facultativo y las recomendaciones generales del Comité, en particular la recomendación general núm. 19". Derecho internacional de los drechos humanos.

[29] Tribunal Europeo de Derechos Humanos, sentencia del 11 de febrero de 2020, *Buturugă contra Rumanía,* n. 56867/15.

Estambul y reconoce el tribunal que falta de examen por los tribunales del fondo de una denuncia de ciberacoso estrechamente vinculada a una denuncia de violencia doméstica[30]:

(a) La investigación de los malos tratos – las autoridades no abordaron los hechos impugnados desde el ángulo de la violencia doméstica. De hecho, la investigación no tuvo en cuenta las características específicas de la violencia doméstica reconocidas por el Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica.

El tribunal no estaba convencido "de que las conclusiones del tribunal nacional en el presente caso hubieran tenido un efecto suficientemente disuasorio para prevenir un problema tan grave como la violencia doméstica" (deber de precaución). Además, aunque ninguna de las autoridades nacionales había negado la realidad y la gravedad de las lesiones sufridas por la demandante (daño acreditado), de la investigación no había surgido ninguna prueba capaz de identificar a la persona responsable (práctica de la prueba con perspectiva de género). Así, las autoridades investigadoras se habían limitado a interrogar a los familiares de la demandante como testigos, sin recabar ningún otro ti-

[30] "Hechos – Basándose en un certificado médico forense, la demandante denunció a las autoridades el comportamiento violento de su ex marido. Solicitó un registro electrónico del ordenador familiar para utilizarlo como prueba en el proceso penal, alegando que su ex marido había consultado indebidamente sus cuentas electrónicas, incluida su cuenta de Facebook, y que había hecho copias de sus conversaciones privadas, documentos y fotografías. Dicha solicitud fue desestimada por considerar que cualquier prueba que pudiera obtenerse de este modo no guardaría relación con las supuestas amenazas y actos violentos cometidos por su ex marido. Posteriormente, la demandante presentó otra denuncia contra su ex marido por violación del secreto de su correspondencia, que fue desestimada por extemporánea. La fiscalía impuso una multa administrativa a su ex marido y archivó el caso, basándose en las disposiciones del código penal que regulan la violencia entre particulares y no en las relativas a la violencia doméstica. El tribunal confirmó las conclusiones de la fiscalía en el sentido de que las amenazas a la demandante no habían sido lo suficientemente graves como para ser calificadas de infracciones penales, y que no se había presentado ninguna prueba directa que demostrara que las lesiones sufridas por la demandante hubieran sido causadas por su ex marido. En cuanto a la supuesta violación de la confidencialidad de su correspondencia, el tribunal dictaminó que esa cuestión no guardaba relación con el objeto del caso, y que los datos publicados en las redes sociales eran públicos.

po de prueba para averiguar el origen de las lesiones de la demandante y, posiblemente, los responsables de infligirlas. En un caso de presuntos actos de violencia doméstica, las autoridades investigadoras deberían haber tomado las medidas necesarias para dilucidar las circunstancias del caso. Por consiguiente, aunque el marco jurídico establecido por el Estado demandado había proporcionado a la demandante algún tipo de protección, ésta había surtido efecto con posterioridad a los actos de violencia impugnados y no había subsanado las deficiencias de la investigación.

(b) La investigación sobre la violación de la confidencialidad de la correspondencia de la demandante.

Tanto en el derecho nacional como en el internacional, se considera que el fenómeno de la violencia doméstica no se limita a la violencia física, sino que también incluye la violencia psicológica o el acoso. Además, el ciberacoso se reconoce actualmente como un aspecto de la violencia contra las mujeres y las niñas y puede adoptar diversas formas, como la violación cibernética de la intimidad, el pirateo del ordenador de la víctima y el robo, intercambio y manipulación de datos e imágenes, incluidos detalles íntimos. En el contexto de la violencia doméstica, la cibervigilancia es a menudo rastreable hasta la pareja de la persona. Por lo tanto, el tribunal aceptó que actos como vigilar, acceder y guardar indebidamente la correspondencia del cónyuge o pareja podrían ser tenidos en cuenta por las autoridades nacionales al investigar casos de violencia doméstica. Tales alegaciones de violación de la confidencialidad de la correspondencia requerían que las autoridades llevaran a cabo un examen sobre el fondo para obtener una comprensión exhaustiva del fenómeno de todas las formas posibles de violencia doméstica (perspectiva de género).

No se había realizado ningún examen sobre el fondo del presente caso. Las autoridades nacionales no habían adoptado las medidas procesales para recabar pruebas con el fin de establecer la realidad o la calificación jurídica de los hechos. Habían sido excesivamente formalistas al descartar cualquier posible conexión con la violencia doméstica que la demandante ya había puesto en su conocimiento, y habían ignorado así las diversas formas posibles que adopta la violencia doméstica" (ausencia de aplicación de la perspectiva de género).

"Por lo tanto, el Estado había incumplido sus obligaciones positi-

vas en virtud de los artículos 3 y 8 del Convenio. Se condena por unanimidad a la indemnización de 10.000 euros a cargo del Estado".

Se trata de un ejemplo de lo que supone la no formación y sensibilización policial y judicial en un Estado en materia de perspectiva de género, donde ese elemento estereotípico no erradicado por el Estado, le hace incumplir el Convenio de Estambul o la directiva citada, contribuyendo a generar daño por los propios órganos jurisdiccionales, cuando la víctima ejerció su derecho a la tutela judicial efectiva o garantía de jurisdiccionalidad de su derecho a la intimidad a través de una investigación profunda y eficaz de los malos tratos sufridos, así como de la confidencialidad de la correspondencia y comunicaciones de la demandante. Es decir, la ausencia de cambios estructurales supone una falta de remoción de los obstáculos que impiden la igualdad de la mujer, provocan daños a la misma y representan una ausencia de la diligencia debida, según los estándares internacionales de los acuerdos de los que España forma parte, así como de su derecho nacional. Corresponde a los jueces y magistrados resolver estas antinomias con el derecho[31]. De otra forma, se puede entender que hay violencia institucional.

En España – y entorno de la UE – la influencia del convenio de Budapest en el proceso español ha traído como consecuencia la modificación de la LECRIM a través de la LO 13/2015 para el fortalecimiento de las garantías procesales y las medidas de investigación tecnológica (arts. 588-*bis* a 588-*octies*)[32], donde se regulan la pruebas elec-

[31] L. FERRAJOLI, *op. cit*. Sin embargo, cuando éste mismo juzgador aborde la inexistencia de una regulación de éstos derechos o sus garantías se genera lo que se denomina una *anomia*, por encontrar contenidos y límites difusos, no recogidos por las normas (*laguna*); dado que la tutela judicial debe cumplir la obligación del *non liquet,* la persona juzgadora debe de abordar que se revise, remueva y proteja de la manera que considere más acorde a su protección. Estas lagunas deben ser señaladas por la judicatura, que deberá indicar a la Administración y al Poder legislativo, los objetivos a cumplir con sus obligaciones de hacer, con el fin de que se supla ese déficit (por eso este autor les denomina derechos y garantías débiles, aunque no por ello dejan de tener la consideración de derecho fundamental y de ser parte de la democracia, se refiere a la educación, asistencia sanitaria, seguridad social y otros semejantes).

[32] Reglamento (UE) 2023/1543 del Parlamento europeo y del Consejo, *sobre las órdenes europeas de producción y conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penale*s, de

trónicas y la obligación de colaboración de las empresas prestadoras de servicios de la sociedad de la información y de comercio electrónico, así como de la conservación de datos, pudiendo incurrir en delito de desobediencia en caso de no respetar el deber de secreto y de colaboración. (en relación con arts. 16 y 18 Convenio de Budapest). Lo que normativamente hace pensar que la investigación, así como la actividad probatoria quedan garantizadas, no sin cuestionar la necesidad de aplicar la perspectiva de género en el caso concreto que se dé.

5. *Contenidos concretos del deber de diligencia debida del Estado en materia de violencia contra las mujeres en la Directiva, Convenio de Estambul y Convenio de Budapest*

Vista la doble estructura integradora de los derechos de las mujeres a una vida libre de violencia machista (diligencia debida por falta de cambios sistémicos que trae como consecuencia daños individuales para ellas)[33], propongo centrarme en revisar esos mínimos innegocia-

12 de julio de 2023, en DOUE 191 de 28 de julio de 2023, pp. 118-180; así como la (UE) Directiva 2023/1544 del Parlamento europeo y del Consejo, *por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales*, de 12 de julio de 2023, en DOUE 191 de 28 de julio de 2023, pp. 181-190. Con ello se permite a las autoridades judiciales nacionales implicadas en procedimientos penales remitir órdenes a los prestadores de servicios que ofrezcan servicios en la Unión Europea (UE) para que produzcan o conserven las pruebas electrónicas donde puedan encontrarse los datos; también facilitar y acelerar el acceso transfronterizo a los datos electrónicos e impedir su supresión, garantizando al mismo tiempo salvaguardias jurídicas para las personas cuyos datos se buscan. La directiva (UE) 2023/1544 exige que determinados prestadores de servicios que ofrecen servicios en la UE hayan designado establecimientos o representantes legales en la UE para que puedan recibir y cumplir con las órdenes de las autoridades nacionales a efectos de recabar pruebas electrónicas en procesos penales.

[33] Como afirma Román, se ha creado una doble dimensión del deber de diligencia debida de los Estados en materia de igualdad de la mujer: *una dimensión objetiva o sistémica y una dimensión individual*: "La primera, más genérica, reclama una intervención estatal tendente a garantizar un modelo de regulación integral y sostenida de la violencia contra la mujer que, además, persiga una transformación global de la sociedad que supere la desigualdad de género estructural". Por su lado, la responsabili-

bles para los Estados en la directiva, el Convenio de Estambul y el Convenio de Budapest, que tienden a consolidar los valores de la Unión y los derechos de su ciudadanía, en este caso el derecho a la igualdad de mujeres y hombres.

La directiva dedica el grueso de su articulado y Exposición de Motivos a reconocer que nos encontramos ante un problema de modelo cultural, ante una estructura de sociedad y de administración pública, que debe cambiar con el fin de poder evitar daños a las mujeres. Al igual que la Ley Orgánica de Violencia de Género española que dedica el Título Preliminar, I, II y III a transformar los elementos que en la sociedad contribuyen a perpetuar un sistema de subordinación sistémica; estos artículos lo que hacen es "contextualizar" todo aquello que parecía aparentemente neutro[34]. Hay, por tanto, insistimos en que se percibe un *cambio de paradigma*. A tal fin la directiva exige resultados y deja libertad en la forma y medios de conseguirlos (FJ 15). Esta idea es importante porque, si bien entra dentro de la potestad discrecional de la Administración el decidir *cómo* conseguir los objetivos de la directiva, *con qué medios* y *plazos* temporales, queda fuera de su alcance negociar las *finalidades* a alcanzar según la Unión, tan claramente delimitadas por la directiva.

Ejemplo de lo que decimos podemos encontrarlo recientemente en el *Informe de la Relatora Especial de Naciones Unidas sobre la violencia contra las mujeres y las niñas, sus causas y consecuencias*[35] por-

dad del Estado en su *dimensión individual*, exige que se deriven obligaciones para éste, destinadas a proporcionar a las víctimas concretas que sufren violencia, a través de la creación de medidas eficaces de protección, sanción y reparación, exigiendo ello un alto grado de acomodación y flexibilidad, vid. L. ROMÁN, *La protección jurisdiccional de las víctimas desde la perspectiva constitucional*, Tesis inédita defendida en la Universitat Rovira y Virgili, 2016, p.33 y 39-45.

[34] Ley Orgánica 1/2004, *de Medidas de Protección Integral contra la Violencia de Género,* de 28 de diciembre, en BOE 313 de 29 de diciembre de 2004.

[35] Consejo de derechos humanos, Informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, sus causas y consecuencias, REEM ALSALEM, *en custodia, violencia contra las mujeres y violencia contra los niños,* A/HRC/53/36, 13 de abril de 2023, donde explica el impacto de los estereotipos en la creación normativa así como en la función jurisdiccional y en servicios sociales en relación a la custodia y los menores. Así se citan varios apartados: a) La desigualdad de género en las leyes y ordenamientos jurídicos; b) el papel evaluador en los tribunales de familia y el negocio

menoriza los "problemas sistémicos" que dan cobertura a esta realidad violenta y discriminatoria que, junto a la directiva objeto de estudio, puede darnos mucha luz sobre cómo integrar este nivel de exigibilidad en los cuerpos legislativos de los Estados miembro y cuáles son las transformaciones internas eficientes para cumplir con los estándares de diligencia debida de la Unión [36]. Sobre estas bases, la nueva directiva regula para los Estados miembro esta misma doble estructura de la que venimos hablando: obligaciones de llevar a cabo cambios naturaleza sistémica con el fin de garantizar, en segundo término, los derechos individuales de las mujeres a prevenir, reparar y erradicar la violencia machista.

Procedemos a enumerar las condiciones estructurales que deben cambiarse en aras de remover los obstáculos que impiden la igualdad – objetivo de la directiva – y qué derechos se otorga a la ciudadanía en la directiva para conseguir tal fin, entendiendo que la realización de la ciberviolencia machista se encuadra en esta misma doble estructura que se debe remover para alcanzar la igualdad.

5.1 *Normas con perspectiva de género*

Se tiene el derecho a una *legislación civil, penal, administrativa y laboral que recoja las bases para la transformación de nuestra sociedad*[37] y eleve a la mujer a una protección digna y segura y que conlleve sanciones eficaces para el abusador (fundamento jurídico 28 de la directi-

existente en los informes psicológicos en la materia; c) Conducta de la judicatura y de los profesionales del derecho; d) La falta de asistencia jurídica gratuita y costes de los litigios de derecho de familia (pp. 15-20).

[36] Muy interesante el artículo: G. DOMÉNECH PASCUAL, *Repensar la responsabilidad patrimonial del Estado por normas contrarias a Derecho,* en *Indret,* 2022, n. 4. Nos explica con extrema claridad la responsabilidad del Estado en su *hacer bien* las normas, pormenorizando en los niveles de diligencia exigible en estos casos y reconociendo que si hay daño, puede haber responsabilidad, existiendo una norma (también de derecho internacional) que individualice la infracción y una relación de causalidad directa, puede darse este caso de responsabilidad.

[37] Sobre la obligación del Estado de proteger penalmente los derechos fundamentales vid. G. DOMÉNECH PASCUAL, *Los derechos fundamentales a la protección penal,* en *Revista Española de Derecho Constitucional*, 2006, n. 78, pp. 333-372.

va). La directiva exige eficacia, perspectiva de género[38], excluyendo la aceptación de normas que no garanticen la transformación de la sociedad y una forma legal eficaz de abordar la violencia machista. Para la consecución de tal fin se exige formación incluso al propio legislador.

La directiva, a tal fin, regula para todos los Estados las violencias más reprochables que sufren las mujeres en la Unión, según la Encuesta del Fundamental Rights Agency[39], a saber, las ejercidas por sus parejas o ex parejas, por su entorno familiar, por terceros con carácter sexual, las ejercidas dentro del ámbito de los delitos de honor, y las que se usan las TIC para el sometimiento, todas ellas ejercidas por el simple hecho de ser mujer. También extiende este ámbito a otras personas pertenecientes a colectivos discriminados y a una perspectiva interseccional, que agrava cualquier violencia especialmente en su abordaje y tutela. Ejemplo de la obligación de legislar con dicha perspectiva son la regulación de delitos (arts. 3-8), la limitación a su prescripción (art. 13), las penas (ar. 10) y agravantes (art. 11), inducción complicidad y tentativa (art. 9), la obligación de regular el delito de quebrantamiento de medida cautelar, etc.

En materia de ciberviolencia es obligatorio tener un marco normativo penal, derivado tanto de la directiva como del Convenio de Estambul. La directiva ya en su art. 1 reconoce la obligación de regular y sanciones la violencia que se realiza por medios informáticos, en el art. 5 regula en qué consiste la difusión de material íntimo o manipulado, el art. 6 reconoce el ciberacecho, el art. 7 el ciberacoso, art. 8 regula como delito la incitación al odio por medios cibernéticos, art. 23 reconoce las medidas para eliminar materiales en línea, art. 42 obliga a la cooperación entre prestadores de servicios intermediarios. Por su lado, el Convenio de Estambul exige tener regulada la violencia digital y a través de medios tecnológicos contra la mujer (art. 40 sobre acoso sexual online sexual, art. 34 sobre la violencia online y el acoso tecnológico o el art. 33 sobre dimensión digital de la violencia psicológica), así

[38] *Supra.*

[39] Agencia Europea de los Derechos Fundamentales (FRA), *Violencia de genero contra las mujeres: Una encuesta a escala UE*, 2014. Disponible en: https://fra.europa.eu/es/publication/2020/violencia-de-genero-contra-las-mujeres-una-encuesta-escala-de-la-ue-resumen-de-las.

como a tener en general políticas globales para erradicar este tipo de violencia contra la mujer (art. 7 Convenio de Estambul).

Dentro de estas obligaciones de legislar, encontramos la cita expresa entorno a la creación "directrices" para asegurar la actuación de la policía y demás autoridades con dicha perspectiva de género (art. 21 directiva), legislación que debe contar con una evaluación del impacto de género (art. 45 directiva), seguida de una comunicación o traslado de los datos resultantes de esta implementación al Instituto Europeo para la Igualdad de Género (EIGE). Para ello exige la creación de organismos de igualdad en cada país (art. 22). Por último, el alcance normativo debe de llegar a regular la coordinación de todos los servicios, dado el carácter integral y transversal que exigen estas normas y sus resultados (fundamento jurídico 83 y art. 25 y Capítulo IV de la directiva). También, el art. 16 del Convenio de Budapest (Conservación rápida de datos informáticos almacenados), la respuesta inmediata, prevención y protección (art. 50 Convenio de Estambul), incluidas las medidas operativas preventivas y la recogida de pruebas, entre otras muchas regulaciones exigibles a los Estados en la materia.

En conclusión, se tratan de dos marcos normativos vinculantes que nos obligan a todos los Estados de la UE yd e Convenio a tener una regulación adecuada en la materia objeto de estudio. A lo dicho en el capítulo de derecho penal español nos remitimos. Políticas globales y coordinadas art. 7 Convenio de Estambul, lo que conlleva la previsión de recursos financieros (art. 8 Convenio de Estambul), que alcancen no solo a los órganos del estado en cargados de la materia sino también a las organizaciones no gubernamentales (art. 9 Convenio de Estambul) y los órganos de coordinación de la efectividad de estas leyes en un plano ejecutivo (art. 10 Convenio de Estambul).

5.2. *Prevención, sensibilización frente a las formas de violencia contra la mujer*

Las obligaciones generales en prevención también son objeto de tutela por parte de los Estados (art.12 Convenio de Estambul): Sensibilización (art. 13 Convenio de Estambul), Educación (art. 14 Convenio de Estambul), Formación de profesionales (art. 15 Convenio de Estambul), Programas preventivos de intervención y tratamiento (art.

16 Convenio de Estambul) y Participación del sector privado y medios de comunicación (art. 17 Convenio de Estambul). También la directiva parte de la idea relativa a la necesidad de desmontar un modelo cultural para entender y prevenir las violencias contra la mujer, de manera absoluta y de forma también interseccional.

Se tiene derecho a que esta legislación atienda a crear un modelo de *publicidad, comunicación, educación y sanidad* respetuoso con la especial situación de la mujer en nuestra sociedad, que transforma valores, estereotipos, prejuicios sobre la mujer (fundamento jurídico 74, 75, 77 y art. 36 de la directiva y art. 17 Convenio de Estambul). Es una obligación para los Estados la formación y sensibilización de profesionales que intervienen ante un caso de violencia machista con el fin de entender esta realidad tan específica (prevención secundaria). La formación obligatoria de las personas profesionales, en especial "la judicatura y otros profesionales del sistema judicial en materia de sesgo de género, la dinámica de la violencia doméstica, las denuncias del maltrato y la alienación parental, etc., debiéndose asegurar que la ciudadanía tiene acceso a materiales y un teléfono de información (fundamento jurídico 75 y 77 y art. 29 y 36 de la drectiva)[40].

La directiva recoge *programas de atención* temprana a niños y jóvenes para evitar que sean maltratadores (art. 34 directiva), medidas específicas para prevenir la cultura de la violación (art. 35 directiva) o la mutilación genital o los ciberdelitos sexuales (art. 34 directiva), incluso en los colegios (art. 35 directiva). Los estados miembros adoptarán las medidas necesarias para tener programas de intervención que evite la comisión de estos delitos y la reincidencia (art. 37 directiva).

[40] Ejemplo de lo que decimos viene desarrollado por el Informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, cuando se "prohíbe" la invocación de los conceptos como alienación parental o pseudoconceptos parecidos en litigios de derecho de familia, porque violan la norma del interés superior del menor, poniendo de manifiesto que el marco normativo de todavía muchos Estados ahonda en desigualdad, cuando regula estas normas en estos casos (Conclusión 74 del Consejo de derechos humanos, Informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, sus causas y consecuencias, REEM ALSALEM, *en custodia, violencia contra las mujeres y violencia contra los niños,* A/HRC/53/36, 13 de abril de 2023, *op. cit.).*

5.3. *Protección social*

La atención social preventiva es básica tal y como asume la directiva en su articulado al reconocer la prevención primaria, secundaria y terciaria (FJ 73). Allí se habla del derecho a servicios de apoyo a las víctimas (arts. 18 y 25 directiva) y a su recuperación, con especial incidencia en los casos de violencia sexual (art. 26) y para los casos de mutilación genital femenina (art. 27) y acoso sexual en el trabajo (art. 28); derecho al servicio de salud (art. 25 directiva), existencia de líneas telefónicas de ayuda a las víctimas accesibles y garantizadoras de una comunicación efectiva (art.29), prestaciones de apoyo específicas a las necesidades interseccionales de víctimas y grupos de riesgo (art. 33). En general, se diseña todo un entramado de normas que apuntan en la dirección de unos servicios sociales óptimos para prevenir y reparar daños, con la exigencia de coordinación efectiva (arts. 39 y 40 directiva). Nada se dice sobre el derecho a la autonomía económica de la víctima en dicha directiva, quedará a decisión de cada Estado, lo que se presenta como una debilidad de esta directiva.

5.4 *Protección y acción judicial*

Dentro de los cambios estructurales que requiere el Estado para ser diligente, entraría toda la estructura de la justicia y del proceso, donde sin una interpretación de todo este entramos jurídico sin perspectiva de género, hace muy difícil entender la realidad en la que acontece este tipo de delitos, también cuando se comenten en la red.

Procedemos a enumerar las garantías necesarias para garantizar a las mujeres y niñas, así como otras víctimas, el derecho a la tutela judicial efectiva en este concreto derecho humano:

1.- La recogida de datos de la investigación (art. 11 Convenio Estambul), asegurando su permanencia como fuente de prueba, las obligaciones generales y específicas de protección a víctimas de la ciberdelincuencia (art. 18 Convenio Estambul); el cumplimiento de la obligación de información y transparencia (art. 19 Convenio de Estambul); la existencia de una red de servicios de apoyo a las víctimas (arts. 20 y 22 Convenio de Estambul) con especial hincapié en las necesidades requeridas para denunciar (art. 21 Convenio de Estambul), con inde-

pendencia de sus especiales necesidades (art. 22 Convenio de Estambul); que incluyan un teléfono de 24 horas con guardias telefónicas (art. 24 Convenio de Estambul); con servicios especiales de apoyo a víctimas de violencia sexual (art. 25 Convenio de Estambul), así como para menores y testigos (art. 26 Convenio de Estambul) que faciliten la denuncia (arts. 27 y 28 Convenio de Estambul).

2.- Se tiene derecho a la *asistencia jurídica y defensa* para que el sistema de justicia sea económicamente accesible para las víctimas, tanto en la fase de asesoramiento, representación y defensa procesal (art. 32 de la directiva y arts. 19, 22 y 57 Convenio de Estambul). El art. 14 asegura el derecho a realizar denuncias telemáticas y que permita cargar el material prueba del delito (pantallazos, etc.).

3.- Se tiene derecho a la *regulación de programas de apoyo legal y social* a las víctimas (art. 25 y 26 directiva y arts. 16, 20, 56 Convenio de Estambul), tanto para las mujeres como para los niños y niñas víctimas con especial incidencia en la seguridad en materia de derecho de custodia y visitas (art. 70 directiva y art. 31 Convenio de Estambul), incluso llegando a la pérdida de la patria potestad (art. 45 de Convenio de Estambul) y obligando por que sea financiado este apoyo a cargo del Estado (vid. también la Conclusión 74 del informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, de 13 de abril de 2023, A/HRC/56/36), así como para las mujeres extranjeras. Aquí podemos integrar entre otros muchos, a la existencia de casas de acogidas (art. 33 directiva y 23 Convenio de Estambul).

4.- Se tiene derecho a la *tutela judicial efectiva* frente a la violencia de género a través de la correcta *investigación y obtención y aseguramiento de fuentes de prueba, así como la protección, reparación y especialización del juzgador* en su fase investigadora como de enjuiciamiento, garantizando el derecho al *recurso civil y penal adecuado* (arts. 20, 30 y 34 directiva y arts. 29, 44 y 54 Convenio de Estambul). En el ámbito de la prueba la directiva reconoce que los reconocimientos médicos y análisis forenses *deben de ser financiados por el Estado*, asegurando que las personas que los realicen sean verdaderamente expertas (art.26 directiva y Conclusión 74 del informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, de 13 de abril de 2023, A/HRC/56/36Relatora A/HRC/56/36). En violencia sexual, tanto la prueba tecnológica

como el uso de las imágenes deben ser garantizado y custodiado sin victimización secundaria (art. 15 directiva).

Es decir, se tiene el derecho a *un juicio justo y sin dilaciones indebidas* no solo para saber qué ocurrió, sino para averiguar las *circunstancias o "contexto"* en el que ocurrió. Averiguar este contexto es *profundizar en los elementos fácticos reales que explican los comportamientos de víctima y agresor* y, por tanto, dejar a un lado la aparente neutralidad de la norma. Esto requiere una alta formación de los y las operadores jurídicos que realmente aseguren los diversos contenidos del derecho al proceso justo y el acceso a la justicia de la mujer víctima (fundamento jurídico 77 y ss. y art. 36 directiva y arts. 8, 11, 15 Convenio de Estambul). La motivación de la sentencia constituye garantía de *la valoración de la prueba y la convicción judicial* en relación a dicho "*contexto particular en el que ha ocurrido el hecho*" que permitan explicar racionalmente lo ocurrido, no pudiendo derivarse prejuicios o valoraciones (fundamento jurídico 48 directiva)[41].

Se tiene derecho a ser evaluada en *el riesgo* existente de forma individualizada y eficaz por profesionales formados y sin sesgos (art. 16). Ello deberá dar lugar a una resolución judicial adecuada que puede incluir, a tenor de la directiva, las órdenes de alejamiento, de prohibición o de protección (art. 19) para evitar el peligro inmediato y posible reiteración delictiva, sin que dependan del hecho de que la víctima denuncie, pudiendo ser dictadas de oficio o a instancia de parte, alcanzando la obligación de las autoridades a informar a la víctima sobre ellas tanto en el ámbito nacional como transfronterizo (art. 19). Y, por último, reconoce el *delito de quebrantamiento de medida cautelar* y, si se da, existe el derecho a que se revise la resolución que legitimaba la medida sobre la base de un riesgo y la obligación de revisarlo periódicamente (art. 19).

5.- Se tiene derecho a que haya una *coordinación integral* eficaz (Cap. VI y art. 25 de la directiva) y que, ante un *fallo del sistema,* deba estudiarse lo ocurrido y la posible responsabilidad del Estado por no

[41] L. CLÉRICO, *Hacia un análisis integral de estereotipos: desafiando la garantía estándar de imparcialidad,* en *Revista Derecho del Estado,* 2018, n. 41; M. LORENTE ACOSTA, *Justicia, Género y Estereotipos*, en E. MARTÍNEZ GARCÍA (ed.), *Análisis de la Administración de Justicia desde la perspectiva de género*, Valencia, 2018.

regular el marco legal de protección policial y jurisdiccional eficaz (art. 21 directiva). El derecho a una reparación o indemnización de la víctima está regulado solo a cargo del abusador, algo que debe simultanearse con nuestra aspiración de cambiar estructuralmente las necesidades de estas personas en la sociedad (FJ 56 y 57 directiva, art. 30 Convenio de Estambul y Conclusión 74 del informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, de 13 de abril de 2023, A/HRC/56/36).

6.- Es importante recordar que ninguna víctima de este tipo de violencia puede ser sometida obligatoriamente a un *modo alternativo de resolución de conflictos* (art. 48 Convenio de Estambul). La directiva guarda silencio, pero la complementación con la directiva 2012/29/UE, de víctimas[42] deja la puerta abierta bajo determinadas circunstancias y siempre que no esté prohibido. Así ocurre en la legislación española, pero este silencio puede dejar espacio a estas opciones en países más reactivos a los presentes cambios, por ejemplo.

7.- Derecho a que se observe exigencias legales que *eviten la victimización secundaria de la mujer y de los niños y niñas ante la Administración de Justicia* (Art. 21, 25 y 36 directiva y la Conclusión 74 del informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, de 13 de abril de 2023, A/HRC/56/36).

8.- Se tiene derecho a que el Estado tenga *refugios* o centros de acogida (fundamento jurídico 67 y ss, art. 30 de la directiva y Conclusión 74 del informe de la Relatora Especial sobre la violencia contra las mujeres y las niñas, de 13 de abril de 2023, A/HRC/56/36) para víctimas nacionales o extranjeras, dejando la puerta abierta esta directiva a una suerte de copago, lo cual entorpece la salida del domicilio como medida policial o judicial preventiva.

9.- Junto al *derecho a la reparación del daño* a cargo del agresor (fundamento jurídico 50 y 56 y art. 24 directiva y, en su defecto, a cargo del Estado *solve et repete* ex art.5 Convenio de Estambul), se debe de regular *garantías de no repetición*, estas últimas tan importantes co-

[42] Directiva 2012/29/UE Del Parlamento europeo y del Consejo, *por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y por la que se sustituye la Decisión marco 2001/220/JAI del Consejo*, de 25 de octubre de 2012, en DOUE 315 de 14 de noviembre de 2012, pp. 57 y ss.

mo las otras. A tal fin, debe considerarse la *preceptividad de la intervención en programas realistas de reeducación* del maltratador condenado (art. 37 directiva). También regula la directiva el derecho a que se garantice el olvido (real y virtual) de las víctimas, como parte de la reparación (art. 23 directiva).

10.- Se reconoce el derecho a recibir *una respuesta inmediata, prevención y protección* ante la denuncia de los hechos violentos (art. 50 Convenio de Estambul), incluidas las medidas operativas art. y la recogida de pruebas por las fuerzas y cuerpos de seguridad. Por lo que se refiere a las formas de violencia en línea y facilitadas por la tecnología, el reconocimiento temprano y rápido de ese tipo de violencia por parte de las fuerzas del orden contribuye al establecimiento de procesos óptimos para la recogida de pruebas. A este respecto, los arts. 16 a 21 del Convenio de Budapest podrían complementar el art. 50 del Convenio de Estambul en lo que se refiere al enjuiciamiento de la violencia contra las mujeres en línea y facilitada por la tecnología. Asimismo, esos arts. darían a las Partes una orientación más precisa sobre las medidas que deben adoptarse para obtener las pruebas electrónicas en los procedimientos penales en los territorios de las Partes.

11.- A tenor del art. 16 del Convenio de Budapest se reconoce el derecho a la *conservación rápida de datos informáticos almacenados*. El Informe explicativo del Convenio de Budapest destaca que: "Las medidas contenidas en los Artículos 16 y 17 se aplican a los datos almacenados ya obtenidos y conservados por los titulares de los datos, como, por ej., los proveedores de servicios, debido a la volatilidad de los datos informáticos, que son fácilmente objeto de manipulaciones y modificaciones. Por lo tanto, las pruebas de un delito pueden desaparecer fácilmente debido a negligencias en el manejo o las prácticas de almacenamiento; a la manipulación o borrado deliberados de los datos con el fin de destruir las pruebas, o a la eliminación sistemática de datos cuya conservación no se requiere por más tiempo". El art. 21 del Convenio de Budapest, por su lado, reconoce el derecho a que se produzca por las autoridades la interceptación de datos relativos al contenido, porque éstos incluyen información como texto, imágenes, fotos, vídeos, sonido, etc. Los arts. 16 a 21 del Convenio de Budapest son complementarios del art. 50 del Convenio de Estambul.

12.- Igualmente, es resaltable el art. 51 del Convenio de Estambul

que se refiere a la *valoración y gestión de riesgos para la víctima, exigiendo la coordinación de la seguridad y el apoyo de la misma*. De hecho, muchas formas de violencia contra las mujeres en línea y facilitada por la tecnología podrían precipitar situaciones potencialmente mortales. Por lo tanto, las víctimas de violencia doméstica ejercida por parejas o ex parejas deben disponer de mecanismos coordinados que les brinden apoyo y seguridad, incluso en los casos de abuso perpetrado en línea o facilitado por las nuevas tecnologías.

13.- Igualmente el art. 52 del Convenio de Estambul (*Órdenes urgentes de prohibición*) y art. 53 (*Mandamientos u órdenes de protección*) buscan prevenir a la víctima frente a nuevas agresiones, tanto frente a las formas de violencia doméstica perpetrada en línea y facilitada por las nuevas tecnologías. De hecho, en la práctica, las órdenes de prohibición o de protección en muchos casos no mencionan la comunicación electrónica debido a la falta de comprensión por parte de las fuerzas del orden de las numerosas formas de violencia mediadas por las nuevas tecnologías. Además, como los medios de comunicación electrónica se han ampliado y son ahora más variados y menos claros y directos, algunas características de las redes sociales tienen que ver ahora menos con la comunicación (intercambio de mensajes o de contenidos) que con la visualización (ver de forma pasiva el contenido producido por alguien, sin interacción), o incluso a veces con el acoso, por ejemplo, el visualizar las "historias" de alguien en línea o el "orbitar", comportamiento que consiste en no responder a los mensajes de alguien pero seguir observando visiblemente sus contenidos en línea.

14.- El art. 56 es crucial ya que enumera las *necesidades de las víctimas en todas las fases del proceso judicial*. El tomar en cuenta las necesidades especiales de las víctimas cuando son testigos, y el brindar protección a sus familias y testigos contra la revictimización y las represalias en línea y facilitadas por la tecnología puede eliminar gran número de amenazas vehiculadas por esos medios.

En conclusión, en este cruce de normas especializadas en género y normas neutras (aplicables a cualquier tipología delictiva), como las arrojadas por la regulación de la tecnología y redes, es imprescindible aplicar la perspectiva de género para que sean verdaderamente protectoras de las realidades de la violencia de género, especialmente la de naturaleza o componentes sexuales y relativos a la intimidad.

6. *Breve reflexión sobre el daño para entender el momento de nacimiento de la falta de diligencia debida del Estado en esta materia*

¿A partir de qué momento se le puede hacer responder al Estado por un daño producido a una víctima en las redes? La obligación de precaución del Estado contiene numerosas facetas que van desde el deber de legislar para conocer los límites de lo que se puede hacer o no, hasta la evitación del daño, algo que siempre está en evolución. Se trata de un deber de precaución y progresión en el daño que debe de desarrollarse doctrinal y jurisprudencialmente en materia de ciberviolencia, dado que el daño puede ser exponencialmente masivo y/o irreparable. En estas líneas realizamos una breve aproximación a este análisis, a partir de los datos que se están desarrollando en materia medioambiental[43].

6.1. *Incumplimiento de las obligaciones de respeto y obligaciones de no hacer*

Los Estados deben de *abstenerse* de dañar la igualdad de la mujer, su integridad física y moral, la de su familia y entorno. Ello se puede hacer por acciones y omisiones de los propios órganos del Estado o de entidades de gestión estatal, también por la omisión de legislar correctamente y hacer planes adecuados o, a continuación, no proceder a la ejecución de los mismos puede constituir omisiones que producen daño[44]. La anomia en materia de avances tecnológicos y digitales es presumible que se dé en el futuro, dada la velocidad a la que avanza la In-

[43] E. MARTÍNEZ GARCÍA, *La diligencia debida de los Estados en materia medioambiental en el marco europeo de justicia global,* en *Revista de Derecho Europeo,* 2024, n. 63; y E. MARTÍNEZ GARCÍA, *La función Jurisdiccional en tiempos de interdependencia y ecodependencia,* Valencia, 2024.

[44] El Estado puede dañar por permitir dejar hacer a las empresas públicas o privadas. Conviene saber en estos supuestos si la aquiescencia del Estado es meramente pasiva o, por el contrario, es activa, por ejemplo, postergando o modificando los parámetros regulatorios, demorando en la adopción de medidas urgentes de mitigación o negando importancia a la contaminación realizada, C. COURTIS, *La "debida diligencia" de la empresa como medio para el respeto de los derechos humanos. ¿Herramienta útil o vía para postergar obligaciones legales?,* en *Revista de Derecho Laboral,* 2022, n. 65, p.6.

teligencia Artificial; el daño puede ser individual y masivo, si el legislador no da cobertura a estos avances.

6.2. *Incumplimiento de las obligaciones de hacer*

Por su lado, los Estados deben de *adoptar garantías y hacer real este derecho de las mujeres y los niños y niñas en un entorno digital,* debe de hacer cosas para evitar esos daños, para prevenir violaciones de derechos de ámbito individual (derecho a la salud, a la vida privada, a tener una infancia saludable, etc.) o de ámbito colectivo o público (imagen de la mujer, estereotipos u odio). Algunas de estas obligaciones recaen directamente en falta de cumplimiento por parte de los poderes del Estado, que producen daño, y otras veces afectarán al "hacer" de las empresas que gestionan servicios públicos, en ambos casos se responde por no evitar activamente que se le haga daño a la víctima por cualquier actor (arts. 4 y 5 Convenio de Estambul). Ello significa que el Estado debe vigilar, prevenir, regular, castigar, reparar, es decir, hay obligaciones de simple comportamiento de la Administración para prevenir y, en segundo lugar, hay obligaciones de garantizar activamente y hacer cumplir las normas nacionales e internacionales. Por ambas obligaciones de hacer va a poder responder el Estado. Son títulos jurídicos diferentes por los que pedir la acción ante la justicia. Todo lo que afirmo, a continuación, es predicable de un deber de precaución constante y exigente para el Estado en materia de violencia digital, a los fines de eludir sus responsabilidades.

6.2.1. Obligaciones de regulación, monitoreo y fiscalización

El comportamiento del Estado puede contribuir a no prevenir o no ejercer su deber de precaución y que se produzcan dando dentro o fuera del territorio. Hay un umbral de riesgo no cubierto por el Estado, porque hay indicadores legales que apuntan ya cómo deben ser las acciones del Estado para prevenir un daño, sobre todo, lo encontramos en materia medioambiental. Estas obligaciones de prevención alcanzan a (a) la prevención del daño en sí mismo, (b) a la evitación del agravamiento de la situación, (c) a la mitigación del daño y (d) a la restauración del mismo. Son las fases de consolidación del daño donde el

deber de precaución del Estado se manifiesta una y otra vez. Van en paralelo en su objetivación y progresión del mismo.

Cuando el legislador regula en materia digital debe tener en consideración el alcance de su *deber de precaución*; es decir, esta progresión de evitación de males mayores le interpela como Estado directamente, aunque la persona actora inmediata de la acción que genera el daño sea un sujeto o una empresa, pensemos por ejemplo un maltratado o la empresa que gestiona una casa de acogida o una plataforma de contenidos de Internet. Para hacer efectiva la reparación del daño, es necesario que el Estado esté no solo *regulando*, sino también *supervisando* el avance del daño evidenciado, la actitud del sujeto que genera el riesgo, la entidad pública o privada, las medidas estatales y empresariales adoptadas a cada momento, la reparación del mismo. La dejación del *Estado de este deber de supervisión le puede hacer corresponsable. El deber de diligencia no se agota con la obligación de regular normativamente, sino que la actitud de precaución del Estado sigue vigente y progresiva durante todo el incidente y daño a través de la red. Van en paralelo.*

La *calidad de la norma reguladora y calidad de la supervisión* de la progresión del riesgo y daño. Regular requiere trabajar con la *ciencia*, con los datos que tenemos, apuntan daños de salud mental graves por el uso y abuso de la tecnología y lo digital. Todo ello, puede justificar la limitación de la libertad de la empresa en favor de la igualdad de las personas, sus derechos fundamentales y su salud mental; tal vez el caso de menores es más visual todavía. Para que no haya perjuicios de ningún tipo corresponde a la administración articular medidas que hagan compatibles los numerosos intereses en juego, libertad de mercado vs. Protección de la mujer y víctimas vulnerables. Libertad en las redes vs. derechos de las personas.

La evaluación de impacto de género en la creación de legislaciones en la materia está para esto: prevenir, profundizar en la actividad riesgosas, permitir al estado adoptar ese deber de precaución de forma realista, adelantarse en caso de que exista riesgo y daño tangibles de derechos humanos. Téngase en cuenta que el Estado va a ser víctima incluso de su propia inoperancia, porque junto a las personas dañadas, junto a la sociedad en general, el propio Estado es el que es dañado en su patrimonio al tener que reparar o indemnizar, y no olvidemos que el estado somos todos y todas.

Por tanto, importa la calidad de la norma, la diligencia temporal y material en su aplicación, su *inmediatez* en la aplicación de la misma, su carácter *progresivo* (con supervisión y medios de fiscalización gradual y acorde al avance del daño) *y no regresivo* (retroceso en materia de derechos sociales). Cuestiones a probar por el Estado porque se invierta la carga de la prueba en un proceso. Regulación, supervisión y fiscalización con elemento correlativos a probar. Hay un riesgo y un daño en movimiento cuando hay medios tecnológicos y transnacionales de por medio y, por tanto, la acción del Estado no puede ser estática y, además, ha de ser inmediata, dentro de los parámetros vistos. Esto es enteramente aplicable a la ciberviolencia.

6.2.2. Obligaciones para garantizar la información y el acceso a la información

El Tribunal Europeo de derechos humanos (TEDH) tiene reiterada jurisprudencia sobre el deber de información y acceso real de la ciudadanía a la misma, que recae sobre el Estado. Esto se ve en el Caso comentado *Buturugă vs Romania*[45]. Para evaluar riesgos y adoptar decisiones en el ámbito de la vida privada es necesaria la transparencia de las empresas que ofertan servicios que pueden entrañar riesgos para los bienes jurídicos de las personas y, por tanto, el responsable último es el Estado, que debe supervisar a las mismas, como forma de proteger a la ciudadanía y sus derechos. La transparencia exige una actualización de conocimiento por parte del Estado de la progresión de la actividad o de los riesgos que ella conlleva la actividad empresarial a través de la que se puede delinquir, algo complejo cuando hay una acción que es de naturaleza transnacional, como la de las plataformas digitales.

6.2.3. Obligación de declarar la alerta

Llega un punto en la realización del daño que – su evidencia objetiva – puede conllevar la declaración de alerta, esto se puede ver especialmente al tratar con menores, dado que la sensibilidad es mayor ha-

[45] Tribunal europeo de derechos humanos, sentencia de 19 de febrero de 1998, caso *Guerra vs. Italia*, p.60 y ss.

cia estas víctimas. Es un grado más en el curso de evidencias del daño, de deber de transparencia del Estado y de la obligación de actuación del mismo: debe haber un pronunciamiento de alerta por parte del Estado que no puede postergarse injustificadamente. De no hacerlo, se podría contemplar tolerancia con el daño. Es un delicado equilibrio de precaución.

6.2.4. Obligaciones integradas en el principio de precaución

Este principio está muy desarrollado en materia medioambiental[46]. Pero en daños individuales y masivos por razones de salud mental puede ser igualmente aplicable.

6.2.5. Obligaciones de mitigar la situación que genera daños

El daño debe ser mitigado tan pronto se perciba, con la finalidad de que no siga aumentando y se convierta en irreversible. La desaparición del material de la red y restauración del daño, la contención del ámbito geográfico, la obtención de la información necesaria sobre lo ocurrido y su contraste científico, la actuación inmediata y/o urgente. Su diligencia en este preciso momento incrementará o aminorará la diligencia exigible a un Estado. Corresponde al Estado probar que hizo todo lo posible para dicha mitigación ser lograda.

[46] El principio 15 de la declaración de Río (1992) aporta una dimensión muy importante al principio de precaución cuando afirma que, "La falta de certeza científica absoluta no deberá utilizarse como razón para postergar la adopción de medidas eficaces en función de los costos para impedir la degradación del medio ambiente". La ciencia debe de estar en la configuración de la norma, pero también en la supervisión; sin embargo, la falta objetiva de datos irrefutables no debe menguar el principio de precaución del Estado, sino que en un momento de construcción de los datos científicos que afectan a la salud y al medio ambiente, debemos utilizar la duda en favor de las personas. La carga de la prueba corresponde al Estado o persona que tenga las evidencias en su poder: si hay evidencias científicas se les debe de escuchar, aunque no sean irrefutables, porque también la ciencia es una construcción evolutiva de conocimiento; simplemente cuando los datos apuntan una posible inercia o tendencia compatible con un posible daño, debemos de respetarlos.

6.3. *El carácter inmediato de estas obligaciones y la obligación de progresividad y prohibición de regresividad*

Inmediatez y progresividad en materia digital son dos elementos propios de la diligencia debida del Estado. Ambos elementos son de aplicación a lo que estamos diciendo. Los que van a permitir el ejercicio de los derechos sociales, económicos y culturales. Los derechos de las personas deben de ser tutelados de forma *inmediata*, porque los daños pueden graduarse, porque pueden evolucionar en una mayor degradación si no se actúa rápidamente. Por esta razón la diligencia exigible será una protección gradual en el tiempo, acorde con los riesgos de las actividades en cuestión; por eso la *progresividad* en su protección significa, acorde con estas premisas, adecuación de las acciones y medidas adoptadas a la evolución de los riesgos generados y, por último, *prohibición de regresión* significa no dar un paso atrás, como decíamos, en la consolidación de estos derechos. Es decir, las obligaciones negativas de respeto y las positivas de garantía (regulación, supervisión y fiscalización) del Estado, son inmediatas por la razón de que no requieren de grandes inversiones, sino de un trabajo bien y diligentemente hecho por la administración pública, lo mismo ocurre con la sanción, en caso de incumplimiento por una empresa; consideramos que tampoco requiere grandes esfuerzos del Estado sino eficacia y acción. Inmediatez, progresividad y prohibición de regresividad se complementan.

7. *Conclusiones*

Podemos concluir en que la directiva y el Convenio de Estambul son un gran avance para las mujeres de la Unión europea, así como para los derechos de los niñas y niños y para la violencia doméstica que se sufre en familia, con una especial transcendencia para las acciones delictivas cometidas a través de medios digitales. Estas obligaciones sistémicas del Estado relatadas van a constituir grandes cambios para algunos países, mejoras en otros y consolidaciones en países como España, que cuenta con una experiencia valiente y determinante en esta trayectoria, aunque todavía lejos de conseguir los resultados necesarios

para poder entender que esta violencia ya no tiene un alcance desproporcionado y que vivimos en tiempo de igualdad y derechos de la mujer en las mismas condiciones que los hombres. En definitiva, estos cambios son los que garantizan que, dañada una víctima por la violencia machista, pueda acceder a la tutela judicial efectiva y pretender de forma eficaz la protección, sanción y reparación de sus derechos individuales. Sin cambios sistémicos no puede haber derechos individuales, van de la mano.

El aumento veloz de la violencia digital contra las mujeres y menores exige del Estado una intervención activa, dentro del marco de sus soberanía y fruto de negociaciones internacionales, que permita poner límites a la libertad que infringe los derechos de las personas. El mercado debe tener una perspectiva constitucional, que asegure los derechos de las personas.

Por tanto, los deberes del Estado por cambiar las estructuras que impiden erradicar la violencia machista deben cumplirse los deberes aquí someramente expuestos, teniendo en cuenta que cuando se trate de ciberviolencia, además, entraña un nivel de exigibilidad superior para el Estado, dada su complejidad en la averiguación del delito, obtención de fuentes de prueba y valoración de la misma, si seguimos patrones clásicos del proceso penal. En este sentido la perspectiva de género resulta neurálgica para entender estas realidades violentas por razones de género y cometidas a través de la tecnología.

El daño producido por una violencia institucional debe ser reparado por el Estado.

Abstract

La Sentencia del Tribunal Europeo del Caso *Buturugă v. Romania* nos recuerda que, el alcance de la diligencia debida de los Estados, representa una nueva etapa para las administraciones públicas, dado que existen obligaciones positivas y negativas destinadas a transformar las condiciones sistémicas que alimentan la violencia machista, también la ciberviolencia y violencia tecnológica. Así se deriva también del Convenio de Estambul, de la nueva directiva contra la violencia doméstica y de género, donde se tiene consciencia de que, para acabar con la violencia machista, en cualquiera de sus formas, en necesa-

rio transformar un modelo cultural, legal, administrativo, – también procesal y judicial – que de no hacerlo sigue alimentado los estereotipos y la violencia institucional. El Convenio de Budapest debe de ser reinterpretado a la luz de la perspectiva de género.

PALABRAS CLAVE: Inteligencia Artificial – ciberviolencia – diligencia debida – violencia basada en el género – perspectiva de género

LA CYBERVIOLENZA DI GENERE NEL QUADRO DELLA DIRETTIVA EUROPEA 2024/1385 E DELLA CONVENZIONE DI ISTANBUL: PROSPETTIVA DI GENERE E OBBLIGHI DELLO STATO

La sentenza della Corte europea nel caso *Buturugă c. La Romania* ci ricorda che il campo di applicazione della *due diligence* da parte degli Stati rappresenta una nuova tappa per le pubbliche amministrazioni, dato che esistono obblighi positivi e negativi volti a trasformare le condizioni sistemiche che alimentano la violenza sessista, così come la violenza informatica e la violenza tecnologica. Ciò deriva anche dalla Convenzione di Istanbul, dalla nuova direttiva contro la violenza domestica e di genere, dove si valorizza la consapevolezza che, per porre fine alla violenza di genere, in qualsiasi delle sue forme, è necessario trasformare un sistema culturale, giuridico, amministrativo, – anche processuale e giudiziario – che, se non trasformato, continua ad alimentare stereotipi e violenza istituzionale. La Convenzione di Budapest deve essere reinterpretata alla luce della prospettiva di genere.

KEYWORDS: Intelligenza Artificiale – cyberviolenza – due diligence – violenza di genere – prospettiva di genere

LA GIURISPRUDENZA DELLA CORTE DI STRASBURGO IN MATERIA DI VIOLENZA DIGITALE

*Valeria Tevere**

SOMMARIO: 1. Introduzione. – 2. Il primo caso sulla violenza digitale di genere: *Buturugă c. Romania* (Corte EDU, sentenza dell'11 febbraio 2020, ricorso n. 56867/15). – 3. Il caso *Volodina 2* sul *revenge porn* (Corte EDU, sentenza del 9 luglio 2021, ricorso n. 41261/17). – 4. Il secondo caso di condanna della Romania sulla cyberviolenza di genere: *MSD c. Romania* (Corte EDU, sentenza del 3 dicembre 2024, ricorso n. 28935/21). – 5. Considerazioni conclusive.

1. *Introduzione*

La cyberviolenza di genere rappresenta una nuova frontiera per la giurisprudenza europea.

La diffusione delle tecnologie informatiche, come un "Giano Bifronte", volendo attingere dalla mitologia classica, produce sia effetti positivi (ad esempio nelle applicazioni pratiche in medicina[1]) che negativi. L'utilizzo massiccio delle piattaforme digitali, dei social network, l'uso degli smartphone e delle numerose app, fino alle esperienze nel metaverso, determinano, infatti, significativi aumenti della criminalità informatica, soprattutto nei confronti dei soggetti vulnerabili. La stessa

* Avvocatessa e funzionario pubblico. Dottoressa di ricerca in Scienze giuridiche (curriculum internazionalistico-europeo-comparato), Università degli Studi di Salerno. Email: valeriatevere@gmail.com.

[1] Si è diffusa la medicina digitale che si basa sulle applicazioni delle tecnologie in campo medico, dalla diagnosi all'utilizzo di app per monitorare parametri vitali alla robotica per la riabilitazione psichica, fisica e cognitiva ed all'uso della realtà virtuale per la formazione dei medici. Inoltre, l'utilizzo dell'Intelligenza Artificiale sta diventando un utile supporto, ad esempio in oncologia, permettendo di individuare patologie già dallo stadio iniziale (cfr. Ministero della Salute, *I sistemi di intelligenza artificiale come strumento di supporto alla diagnostica*, 2021, in www.salute.gov.it).

violenza di genere sta transitando sempre più frequentemente nella dimensione digitale che ne rappresenta un *continuum*[2].

Tanto premesso, in questo contributo si analizzeranno tre recenti casi in materia di violenza digitale contro le donne esaminati dalla Corte europea dei diritti dell'uomo (Corte EDU), di cui due di condanna

[2] Per una ricostruzione generale del fenomeno si rinvia ad una ricerca dell'EIGE (Istituto europeo per l'uguaglianza di genere) del 2022 che ha fatto una classificazione dettagliata delle forme di cyberviolenza di genere comparando i diversi ordinamenti degli Stati membri (EIGE, *Combatting Cyber Violence against women and Girls*, 2022 in eige.europa.eu). Per una prima definizione di cyberviolenza (VAW) contro le donne si rinvia alla nozione fornita dalla Commissione europea che ha chiarito che si tratta di "un atto di violenza di genere commesso, direttamente o indirettamente, attraverso le tecnologie dell'informazione della comunicazione che dà origine, o è probabile che dia origine, a violenza fisica, sessuale, psicologica o economica e che comprende le minacce di compiere tali atti … la cyberviolenza fa parte del continuum della violenza contro le donne: non è un fenomeno isolato, piuttosto si origina da forme multiple di violenza offline e le alimenta" (cfr. Commissione europea, Comitato consultivo per l'eguaglianza delle possibilità tra donne e uomini, *Parere sulla lotta alla violenza online contro le donne*, 2020, disponibile su www.europart.europea.eu). Si veda, inoltre, il report delle Nazioni Unite sulla cyberviolenza contro le donne e le ragazze del 2015 (U.N. Broadband Commission, *Report on cyberviolence against women and girl,* 2015, disponibile su https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf). Valga anche richiamare il recente Libro Bianco *per la formazione sulla violenza maschile contro le donne*, pubblicato nel novembre 2024, della Presidenza del Consiglio dei ministri, Dipartimento per le Pari Opportunità, che, nella parte prima, dedica il paragrafo 2.7 alla cyberviolenza in www.pariopportunita.gov.it. Senza dubbio, inoltre, con l'approvazione da parte del Parlamento europeo e del Consiglio della direttiva (UE) 2024/1385, che attualmente rappresenta uno degli strumenti legislativi più avanzati in materia di VAW, per la prima volta, è stata disciplinata la violenza online si rinvia al contributo in questo Volume di A. FESTA, *Dalla strategia per la parità di genere all'inserimento della violenza digitale tra gli "eurocrimini": l'approccio olistico dell'Unione europea al fenomeno della violenza contro le donne e di genere/De la estrategia de igualdad de género a la inclusión de la violencia digital entre los "eurocrímenes": el enfoque holístico de la Unión europea ante el fenómeno de la violencia contra las mujeres y de género*, pp. 357-383. In dottrina si richiama sul tema, *ex multis*, A. IERMANO, *Violenza digitale e Convenzione di Istanbul: una dimensione distinta ma non separata dalla violenza contro le donne*, in *Freedom, Security & Justice: European Legal Studies*, 2024, n. 1, pp. 64-95; A. SCHIAVON, *La cyber-violenza maschile conto le donne: una nuova sfida per il diritto penale,* in *Studi sulla questione criminale*, 2019, nn. 1-2, pp. 207-222.

della Romania, ricondotti, come si vedrà nel dettaglio, alla violenza domestica.

È noto, infatti, che già da tempo i giudici di Strasburgo si misurano con il tema della violenza di genere e della violenza domestica assumendo posizioni *gender sensitive* e fornendo dei criteri interpretativi utili per i giudici nazionali.

Al riguardo, punto focale, anche nelle sentenze in esame, è senza dubbio la verifica del rispetto degli obblighi positivi di protezione delle vittime da parte degli Stati, ovvero degli obblighi di protezione di secondo livello, sia di natura sostanziale che procedurale[3].

La Corte ha evidenziato l'importanza del rispetto da parte degli Stati della *due diligence*. Si tratta di uno standard di tutela internazionale dei diritti umani. Per la tutela dei diritti delle donne vittime di violenza, nello specifico, l'art. 5 della Convenzione di Istanbul statuisce che "le parti adottano le misure legislative e di altro tipo necessarie per esercitare la debita diligenza nel prevenire, indagare, punire i responsabili e risarcire le vittime di atti di violenza commessi da soggetti non statali che rientrano nel campo di applicazione della presente Convenzione"[4].

[3] *Leading case* è il caso *Opuz c. Turchia* (Corte europea dei diritti dell'uomo, sentenza del 9 giugno 2009, ricorso n. 33401/02) in materia di violenza domestica in cui la Corte EDU ha riconosciuto la responsabilità dello Stato per non aver protetto la vittima. Sul medesimo crinale valga richiamare un caso nostrano, il caso *Talpis c. Italia* (Corte europea dei diritti dell'uomo, sentenza del 2 marzo 2017, ricorso n. 41237/14) in cui lo Stato italiano è stato condannato per violazione degli articoli 2, 3 e 14 CEDU per non aver agito con rapidità a protezione di una donna e del figlio da atti di violenza domestica commessi dal marito. Tra i commenti più significativi della sentenza si rinvia in dottrina a R. CONTI, *Violenza in danno dei soggetti vulnerabili tra obblighi secondari di protezione e divieto di discriminazione di genere*, *CorteEDU 2.03.2017, Talpis c. Italia*, 2017, disponibile su https://www.questionegiustizia.it/ articolo/violenze-in-danno-di-soggetti-vulnerabili_tra-obbl_23-03-2017.php; A. DI STASI, *Il diritto alla vita e all'integrità della persona con particolare riferimento alla violenza domestica*, in A. DI STASI (a cura di) *CEDU e ordinamento italiano. La giurisprudenza della Corte europea dei diritti dell'uomo e l'impatto nell'ordinamento interno (2016-2020)*, Milano, 2020, pp. 1-31.

[4] Per una ricostruzione della *due diligence* si rinvia a V.TEVERE, *La tutela internazionale dei diritti delle donne vittime di violenza. Riflessioni giuridiche in una prospettiva di genere*, Fisciano, 2021, pp. 98-100.

2. *Il primo caso sulla violenza digitale di genere:* Buturugă c. Romania *(Corte EDU, sentenza dell'11 febbraio 2020, ricorso n. 56867/15)*

Nella sentenza *Buturugă c. Romania* la Corte EDU tratta il primo caso di cyberviolenza di genere[5].

Nella fattispecie *de qua*, la ricorrente aveva lamentato l'inadeguatezza delle attività investigative delle autorità rumene, nei procedimenti penali avviati a seguito delle sue denunce di maltratta-

[5] La Corte EDU, già nel 2003, aveva deciso sulla cyberviolenza in generale nei confronti di un soggetto vulnerabile (nello specifico un minore) nel caso *K.U. c. Finlandia* (Corte europea dei diritti dell'uomo, sentenza del 2 marzo 2009, ricorso n. 2872/02). I fatti erano i seguenti: il 15 marzo 1999 una o più persone non identificate pubblicarono un annuncio su un sito di incontri su Internet a nome del ricorrente, all'epoca dodicenne, senza che lui ne fosse a conoscenza. L'annuncio menzionava la sua età e l'anno di nascita, forniva una descrizione dettagliata delle sue caratteristiche fisiche, un link alla sua pagina web ed il suo numero di telefono. Nell'annuncio, si affermava che si stava cercando una relazione intima con un ragazzo della sua età. Il ricorrente venne a conoscenza dell'annuncio a seguito di un'e-mail ricevuta da un uomo sconosciuto, che chiedeva di incontrarlo. Il padre del ricorrente chiese alla polizia di identificare la persona che aveva pubblicato l'annuncio al fine di sporgere denuncia. Il fornitore del servizio, tuttavia, aveva rifiutato di divulgare l'identità del titolare dell'indirizzo IP (*Internet Protocol*) per vincoli legati alla riservatezza nelle telecomunicazioni. La Corte, nella fattispecie, ha ritenuto senza dubbio violato l'arti. 8 CEDU essendo stata lesa la riservatezza della vittima. Si è statuito che la "vita privata" è un concetto che comprende l'integrità fisica e morale della persona. La Corte ha ribadito che "sebbene l'obiettivo dell'articolo 8 sia essenzialmente quello di proteggere l'individuo da interferenze arbitrarie da parte delle autorità pubbliche, esso non si limita a obbligare lo Stato ad astenersi da tale interferenza: oltre a questo impegno principalmente negativo, possono esserci obblighi positivi inerenti a un effettivo rispetto della vita privata o familiare. Tali obblighi possono comportare l'adozione di misure volte a garantire il rispetto della vita privata anche nella sfera delle relazioni degli individui (…) Esistono diversi modi per garantire il rispetto della vita privata (…) mentre la scelta dei mezzi per garantire il rispetto dell'articolo 8 nell'ambito della protezione contro gli atti dei singoli rientra, in linea di principio, nel margine di apprezzamento dello Stato, un'efficace deterrenza contro gli atti gravi, in cui sono in gioco valori fondamentali e aspetti essenziali della vita privata, richiede disposizioni di diritto penale efficaci" (par. 43). Inoltre, si è affermato che tra gli obblighi di protezione dal *cybercrime* da parte degli Stati, vi rientra la previsione di un sistema per proteggere le vittime minorenni dall'esposizione ad approcci pedofili tramite Internet.

menti familiari[6]. La donna aveva subito anche delle lesioni personali dal coniuge. Inoltre, quest'ultimo aveva violato la segretezza della corrispondenza della moglie, accedendo senza consenso all'account Facebook e aveva effettuato copie delle sue conversazioni private, dei suoi documenti e delle foto. Per questi ultimi fatti, la Procura aveva archiviato il procedimento non ritenendo le suddette condotte sufficientemente gravi e aveva condannato il compagno ad una sanzione amministrativa pari ad euro 250,00.

La signora Buturugă aveva, quindi, impugnato il provvedimento di archiviazione, ma il giudice aveva respinto il ricorso confermando la non pericolosità dei fatti. Inoltre, per l'organo giurisdizionale non sussistevano prove dirette delle lesioni subite.

Esaurite tutte le vie di ricorso interne, la donna ha invocato la tutela sussidiaria della Corte di Strasburgo per la violazione degli artt. 5 Convenzione europea dei diritti dell'uomo (CEDU) (diritto alla libertà e alla sicurezza), 6 CEDU (diritto ad un equo processo) e 8 CEDU (diritto al rispetto della vita privata e familiare).

Nella motivazione della sentenza, i giudici di Strasburgo riscontrano che, nella prassi, è adottato di solito un approccio "dualista" che scinde i profili della violenza domestica da quelli della violenza ordinaria e sottolineano che "i casi di violenza domestica devono essere intesi in modo più rigoroso rispetto alle altre forme di violenza ordinaria in conformità alla Convenzione di Istanbul" (parr .67 e 74).

La Corte EDU richiama, come parametro ermeneutico, la Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica (Convenzione di Istanbul) e sussume la fattispecie di accesso ai dati senza consenso dell'account privato della ricorrente nella violenza domestica e non nella più generale violenza ordinaria.

[6] In materia di maltrattamenti in famiglia, qualche anno prima, la Corte EDU ha deciso nel caso *Balsan c. Romania* (sentenza 23 maggio 2017, ricorso n. 49645/09) ravvisando la violazione dell'art. 3 CEDU in combinato disposto con l'art. 14 CEDU, da parte dello Stato per aver omesso di adottare tutte le misure ragionevolmente possibili per prevenire i maltrattamenti familiari. Nella fattispecie, le autorità giudiziarie avevano ritenuto che il caso non fosse di rilevanza penale e, disapplicando la normativa nazionale che puniva la violenza domestica (art. 199 c.p.), avevano irrogato al colpevole una mera sanzione amministrativa pecuniaria.

Valga ancora evidenziare come questa sentenza sia di interesse anche per la sua natura perché contiene delle implicite raccomandazioni allo Stato sul *modus operandi* nella conduzione delle indagini, invitando le autorità preposte a considerare tutti gli indizi utili per la comprensione del contesto. Secondo la dottrina, con questa tipologia di sentenza, si opererebbe un tentativo di "omogeneizzazione" giurisprudenziale[7].

Per quanto concerne la verifica del rispetto degli obblighi positivi da parte dello Stato, richiamando i principi della sentenza *Opuz c. Turchia*[8], al paragrafo 60 del *decisum*, si statuisce che sullo Stato gravano due obblighi positivi: da un lato, l'obbligo di adozione di misure ragionevoli volte a prevenire in concreto i maltrattamenti e, dall'altro, l'obbligo di condurre indagini efficaci, non bastando solo la sussistenza di un quadro giuridico formale di tutela delle vittime[9]. Ciò che conta è l'effettività della tutela[10].

[7] S. CECCHINI, *La cyberviolenza di genere: un caso di omogeneizzazione giurisprudenziale tra ordinamenti statali*, in *Giurisprudenza italiana*, 2020, Milano, p. 533. Si rinvia anche ai commenti in dottrina di A. IERMANO, *Violenza digitale e Convenzione di Istanbul: una dimensione distinta ma non separata dalla violenza contro le donne,* in *Freedom, Security and Justice: European Legal Studies*, 2024, n. 1, p. 71; E. LATORRE, *La Corte europea dei diritti dell'uomo si pronuncia sulla cyber-violenza*, in https://rivista.eurojus.it; A. SINCLAIR-BLAKEMORE, *Cyberviolence Against Women Under International Human Rights Law: Buturuga v. Romania and Volodina v. Russia (no.2)*, in *Human Rights Law Review*, 2023, n. 1 pp. 1-33; L.G. NITOIU, *Cyber violence-impact of the Buturuga case versus Romania on national law* in *Bulletin of the Transilvania University of Brasov*, vol 16(65), 2023, pp. 47-52; F. VAN LEEUWEN, *Cyberviolence,domestic abuse and lack of a gender-sensitive approach. Reflections on Buturuga versus Romania*, in https://strasbourgobservers.com.

[8] Corte europea dei diritti dell'uomo, sentenza del 9 giugno 2009, ricorso n. 33401/02, *Opuz c. Turchia*.

[9] Il quadro normativo di diritto penale in Romania punisce severamente la violenza domestica. Nel nuovo codice penale, in vigore dal 1° febbraio 2014, in vigore già all'epoca dei fatti, è stata introdotta una autonoma fattispecie di violenza familiare (art. 199 c.p.).

[10] All'uopo, valga richiamare anche il caso *Talpis c. Italia* (Corte europea dei diritti dell'uomo, *Talpis c. Italia*, cit.) in cui si statuisce che "il ruolo della Corte non è quello di sostituirsi all'autorità nazionale e scegliere in loro vece l'ampia gamma di possibili misure che potrebbero essere adottate per assicurare il rispetto degli obblighi positivi ai sensi dell'art. 3 della Convenzione. Tuttavia, allo stesso tempo, in conformità con il

In conclusione i giudici di Strasburgo ritengono che, nel caso di specie, sia stato violato l'art. 3 CEDU (divieto di trattamenti inumani e degradanti) e l'art. 8 CEDU (violazione vita privata e familiare) e non anche l'art. 5 (diritto alla libertà e sicurezza) e l'art. 6 CEDU (diritto ad un equo processo), di cui era stata invocata tutela.

3. *Il caso* Volodina n. 2 *sul* revenge porn *(Corte EDU, sentenza del 9 luglio 2021, ricorso n. 41261/17)*

Per comprendere il caso *Volodina n. 2* in tema di *revenge porn*[11], occorre fare un passo indietro al 2019, quando la Corte di Strasburgo ha, per la prima volta, condannato la Russia per la violazione dell'art. 3 (divieto di trattamenti disumani e degradanti) avendo considerato la violenza domestica come fenomeno strutturale[12].

Nella fattispecie, la ricorrente, Valeriya Volodina, aveva lamentato sistematiche forme di violenza domestica, perpetrate dal suo ex partner. Durante i tre anni della sua relazione, S. avrebbe aggredito la donna, compiuto atti persecutori, nascondendo, tra l'altro, nella borsa della vittima anche un GPS, minacciato ripetutamente, derubato e intimidito la vittima. La ricorrente aveva anche riferito di aver subito un aborto a causa di un pugno nello stomaco ricevuto dall'uomo. A causa dell'inerzia delle forze dell'ordine, nel 2018 aveva anche cambiato

principio della Convenzione che mira a garantire non diritti teorici o illusori ma diritti pratici ed effettivi, la Corte deve assicurare che l'obbligo di uno Stato di proteggere le persone sottoposte alla sua giurisdizione sia adeguatamente adempiuto" (par. 59).

[11] Corte europea dei diritti dell'uomo, sentenza del 9 luglio 2019, ricorso n. 41261/17, *Volodina c. Russia*.

[12] Secondo un sondaggio del Levada center un terzo delle donne russe ha subito violenza domestica e numerosi report di organizzazioni internazionali hanno denunciato costantemente questa diffusa violenza contro le donne (v. O. MERLIN, *Violence against women in Russia 13 million victims every year,* 30 maggio 2013). Il problema della violenza di genere in Russia, dunque, rappresenta un fenomeno su larga scala comprovato anche dalla condanna della Corte EDU nel caso *Volodina*. Anche lo Special Rapporteur on Violence against women, a seguito della sua missione in Russia nel 2024, ha evidenziato che nella Federazione Russa sono ancora fortemente radicate norme patriarcali e valori sociali che considerano l'uomo superiore alla donna e la violenza domestica come un fatto privato.

identità. Infine, l'ex partner aveva anche pubblicato, senza consenso, le immagini della donna. Orbene la Corte, in quella sede, aveva analizzato la questione sotto il profilo del rispetto degli obblighi positivi da parte dello Stato, tra i quali l'obbligo di stabilire e applicare un adeguato assetto di misure positive a protezione delle donne; l'obbligo di prevenire il rischio consapevole di trattamenti disumani e l'obbligo di condurre un'indagine effettiva. La Russia, ad avviso dei giudici europei, risultava carente di una legislazione *ad hoc* sulla violenza domestica, essendo quest'ultima inclusa nella più ampia e generale violenza contro la persona.

Inoltre, si osserva che la violenza viene presa in considerazione solo se è una violenza abituale e se nell'arco di dodici mesi è ripetuta. Ma vi è di più: per assumere valore deve essere fisica, non rilevando le forme non fisiche come le violenze verbali e psicologiche. Infine, può essere fatta valere solo su iniziativa del privato.

Nel caso *Volodina n. 1*, oltretutto, vengono forniti dei criteri interpretativi al fine di verificare la sussistenza della violazione dell'art. 14 CEDU e valutare l'esistenza di una possibile discriminazione.

Tra questi parametri interpretativi rileva la verifica della sussistenza di pregiudizi strutturali. Per accertare, dunque, una discriminazione occorrono delle carenze generalizzate nella valutazione dell'operato delle autorità statuali circa la gravità e l'effetto discriminatorio della violenza domestica, non essendo sufficiente la sola mancata adozione delle misure o delle sanzioni raccomandate nel singolo caso (par. 114).

A seguire, nella pronuncia *Volodina n. 2*, la ricorrente era la medesima della sentenza *Volodina n. 1*.

In questo secondo caso, i giudici europei si sono concentrati, in modo specifico, sui profili procedurali, vale a dire sugli aspetti e sulle modalità con cui le autorità di polizia russa avevano condotto le indagini sulla violenza digitale (nella fattispecie, il partner aveva adottato condotte di molestie informatiche, *cyberstalking* e *revenge porn*) su cui nel 2019 la stessa Corte non si era particolarmente soffermata.

In particolare, sono stati riscontrati dei ritardi da parte delle autorità preposte alle indagini che erano state condotte a quasi due anni di distanza dai fatti con l'inevitabile conseguenza del deterioramento delle prove.

Valga evidenziare qualche passaggio saliente della motivazione[13].

I giudici affermano che "le molestie informatiche sono attualmente riconosciute come un aspetto della violenza contro le donne e le ragazze e possono assumere varie forme, come le violazioni informatiche della vita privata e l'acquisizione, condivisione e gestione di informazioni e immagini, comprese quelle intime (...) nel contesto della violenza domestica, i partner intimi sono spesso i probabili autori di atti di *cyberstalking*" (par. 48). Prosegue la Corte: "la violenza online o cyberviolenza è correlata alla violenza offline e rappresenta una delle facce del fenomeno più complesso della violenza domestica.

Gli Stati hanno gli obblighi positivi di istituire ed applicare un sistema effettivo di punizione delle forme di violenza domestica e di prevedere misure di salvaguardia sufficiente per le vittime" (par. 49).

Valga evidenziare inoltre come non ci siano state *dissenting opinions* sul caso essendo la sentenza stata condivisa dai giudici europei all'unanimità.

4. *Il secondo caso di condanna della Romania sulla cyberviolenza di genere:* MSD c. Romania *(Corte EDU, sentenza del 3 dicembre 2024, n. ricorso 28935/21)*

La Romania torna sul banco di prova della Corte EDU in materia di cyberviolenza di genere a distanza di quattro anni e questa volta per la fattispecie di *revenge porn.*

La ricorrente è una donna che all'epoca dei fatti aveva appena 18 anni. Nell'estate 2016 la ricorrente aveva conosciuto su Facebook V.C.A., di qualche anno più grande ed aveva iniziato a scambiarsi messaggi online e foto intime. La ragazza era stata ammessa a frequentare la stessa facoltà universitaria di V.C.A.

A seguito della fine del rapporto sentimentale, iniziarono discussioni per motivi di gelosia. V.C.A. aveva creato dei profili falsi su Fa-

[13] Per ulteriori commenti del caso si rinvia in dottrina a R.A. COSTELLO, *Volodina v. Russia (no.2): intimate images, Domestic Violence and the Positive Obligations of Member States under Article 8 ECHR*, in *European Data Protection Law Review*, 2021, vol. 7, n. 4, p. 614 ss.

cebook usando le identità di alcuni amici della ricorrente. Successivamente furono inviate foto intime della vittima al fratello, allo zio e ad alcuni amici stretti. Furono, inoltre, pubblicate foto anche su alcuni siti di escort con la conseguenza che la ricorrente si trovò a ricevere numerose chiamate di persone sconosciute che le chiedevano dei servizi sessuali.

Esaurite le vie di ricorso interne, la ragazza ha invocato la tutela dei giudici di Strasburgo.

Senza dubbio, il caso di violenza digitale ivi sottoposto alla Corte è, per le sue dinamiche e ripercussioni nella Rete, molto più grave rispetto al solo accesso all'account del caso *Buturugă*.

Bisogna, tuttavia, evidenziare che già dopo la sentenza del primo caso deciso nel 2020, la Romania, in materia di cyberviolenza, ha apportato delle modifiche legislative *in melius* della normativa preesistente. In particolare è stato emendato l'art. 4 della Legge n. 217/2003 dalla Legge n.106/2020. Inoltre, la Legge n.171/2023, entrata in vigore il 18 giugno 2023, ha incluso il *revenge porn* ("pornografia di vendetta"), vale a dire la pubblicazione senza consenso di contenuti intimi, nell'art. 226 c.c. (violazione della vita privata). C'è stato, dunque, anche un rafforzamento della normativa sulla riservatezza. Il previgente art. 226 era insufficiente perché non includeva profili di responsabilità per gli autori di atti di "pornografia di vendetta" in quanto la maggior parte delle immagini intime detenute dagli autori erano già state ottenute consensualmente in un momento precedente alla vendetta. Si affermava, inoltre, che l'art. 226 non poteva coprire situazioni in cui le immagini intime erano state scattate in un ambiente diverso da quello di una casa o di una stanza. Inoltre, un singolo atto, o anche ripetuti atti, di "pornografia di vendetta" non potevano comprendere gli elementi costitutivi di reati quali molestie e incitamento a molestie in circostanze in cui le fotografie erano state inviate a persone diverse dalla vittima. Gli atti in questione non potevano nemmeno comprendere gli elementi costitutivi dei reati di comportamento minaccioso o ricatto. Inoltre, i rimedi civili erano insufficienti a dissuadere gli autori dal commettere tali atti.

Inoltre, i procedimenti civili erano lunghi e costosi, ponevano sulla vittima il difficile onere di provare il danno non patrimoniale e non potevano garantire che le fotografie illegali sarebbero state rimosse

dalle pagine web che le ospitavano, dato che le sentenze dei tribunali civili erano vincolanti solo per le parti del procedimento. La criminalizzazione della "pornografia di vendetta" era necessaria affinché a tali atti venisse riconosciuto un livello di stigma sociale appropriato, considerate le gravi conseguenze psicologiche, professionali e personali per le vittime di questo delitto.

Il caso di specie, tuttavia, si riferisce a fatti precedenti al 2023 e, quindi, non coperti dall'emendamento dello Stato rumeno.

Anche in questo caso la Corte EDU ha ricondotto la fattispecie di violenza virtuale, in continuità con i principi della sentenza nel caso *Buturugă* e della pronuncia sul caso *Volodina 2*, ad una *species* di violenza domestica e, quindi, ad una violazione dell'art. 8 CEDU (diritto al rispetto alla vita privata e familiare). Infatti, la Corte afferma che "il concetto di "vita privata", ai sensi dell'art. 8 CEDU è un termine ampio, non suscettibile di una definizione esaustiva che copre anche l'integrità fisica e psicologica di una persona. Si estende, inoltre, ad aspetti relativi all'identità personale, come il nome, la foto o l'immagine di una persona o il diritto di controllare l'uso di tale immagine. Inoltre il corpo di una persona riguarda un aspetto intimo della vita privata"[14].

Inoltre, si evidenzia che "le molestie online sono attualmente riconosciute come un aspetto della violenza contro le donne e possono assumere varie forme, come le violazioni della vita privata online e l'acquisizione, la condivisione e manipolazione di immagini, comprese quelle intime. È inoltre emerso che la violenza online o cyberviolenza è strettamente collegata con la violenza offline o "nella vita reale" e deve essere considerata come un altro aspetto del complesso fenomeno della violenza domestica"[15].

[14] *"The concept of "private life" within the meaning of Article 8 is a broad term which is not susceptible to exhaustive definition, which covers also the physical and psychological integrity of a person … It moreover extends to aspects relating to personal identity, such as a person's name, picture or image, and the right to control the use of that image… Furthermore, a person's body concerns an intimate aspect of private life*", Corte europea dei diritti dell'uomo, sentenza del 3 dicembre 2024, n. ricorso 28935/21, *MSD c. Romania*, par. 115.

[15] "*Online harassment is currently recognised as an aspect of violence against women and girls and can take a variety of forms, such as online violations of private life ...*

Conclude, dunque, la Corte EDU che anche nella fattispecie esaminata lo Stato non ha rispettato gli obblighi positivi, rispettivamente di assicurare un sistema di punizione di tutte le forme di violenza domestica, sia offline che online, di provvedere a misure di protezione adeguate per le vittime di violenza domestica e di condurre un'effettiva investigazione sugli atti di violenza.

5. *Considerazioni conclusive*

Volendo trarre delle brevi considerazioni alla luce dell'esame dei casi sottoposti alla Corte di Strasburgo sulla cyberviolenza di genere, *in primis* non si può non evidenziare che ben due riguardano lo Stato della Romania e uno concerne la Federazione Russa che non è più parte della CEDU, dal 2022[16].

Con riguardo alla Romania, è d'uopo altresì rilevare che esso è anche uno Stato membro dell'Unione europea e, pertanto, è destinataria anche degli obblighi derivanti dalla recente direttiva (UE) 2024/1385 sulla violenza di genere.

Senza dubbio quest'ultima fonte vincolante dell'Unione europea è un atto di fondamentale importanza, anche per la sua specifica disciplina in materia di violenza digitale. Inoltre, la stessa Corte EDU, come già ha fatto per altre fonti di diritto dell'Unione europea e altre fonti convenzionali (*in primis*, la Convenzione di Istanbul), avrà occasione di richiamarla, come parametro ermeneutico in futuri casi in materia.

Vi è, altresì, da rilevare che in queste tre pronunce la Corte di

and the taking, sharing and handling of information and images, including intimate ones". It has further found that online violence, or "cyberviolence", is closely linked with offline, or "real-life", violence and falls to be considered as another facet of the complex phenomenon of domestic violence", *ivi*, par.118.

[16] A seguito dei tragici fatti di guerra contro l'Ucraina, la Russia è stata espulsa dal Consiglio d'Europa il 16 marzo del 2022 ed è uscita, pertanto, anche dalla CEDU, a partire dal 16 settembre 2022. La Corte EDU, dunque, tratterà solo i ricorsi per la violazione delle norme convenzionali da parte di questo Stato fino al 16 settembre 2022 (v. *Resolution of the European Court of Human Rights on the consequences of the cessation of membership of the Russian Federation to the Council of Europe in light of Article 58 of the European Convention on Human Rights*, risoluzione del 22 marzo 2022).

Strasburgo conferma un *trend* interpretativo in materia di VAW (*Violence against women*) ponendosi in continuità con suoi precedenti provvedimenti (*ex multis*, *Opuz c. Turchia* e *Talpis c. Italia*) e specificando, di volta in volta, il ventaglio dei possibili obblighi di protezione, sia di natura sostanziale che procedurale, degli Stati nei confronti delle vittime di violenza di genere.

Questi obblighi di protezione sono uno spettro ampio. Essi vanno dallo stabilire un quadro giuridico normativo adeguato a tutela delle vittime di violenza, all'obbligo di adottare misure ragionevoli per scongiurare un rischio reale e immediato di violenza ed all'obbligo di condurre indagini efficaci sugli atti di violenza.

Nei casi *Buturugă c. Romania* e *MSD c. Romania*, lo Stato rumeno aveva adottato la prima categoria di obblighi ma sul piano dell'effettività è venuto meno nel condurre attività di indagine efficaci.

Nel caso *Volodina n.2 c. Russia*, lo Stato federale russo aveva omesso anche di adottare sul piano sostanziale un insieme di norme specifiche a tutela delle donne vittime di VAW.

In tutti i casi esaminati la cyberviolenza è inquadrata nella più generale violenza domestica.

Tuttavia, la nuova frontiera del *cybercrime* di genere, sia per gli Stati nazionali che per la giurisprudenza europea, che si intravede all'orizzonte, concerne la violenza di genere nel metaverso[17], essendoci delle forti implicazioni e dei seri rischi sui diritti fondamentali.

Di recente, l'Assemblea parlamentare del Consiglio d'Europa, nella seduta plenaria del 4 ottobre 2024, ha adottato la risoluzione n. 2578 (c.d. risoluzione sul metaverso), accompagnata da un rapporto esplicativo del 5 settembre[18], per provare a richiamare l'attenzione degli Stati sulla necessità di alcuni interventi, sia in relazione ai rischi, sia per fare in modo che siano superate le disparità di accesso al metaverso che, a causa dei costi,

[17] Il temine metaverso è stato coniato, per la prima volta, da Neal Stephenson, nel suo libro Snow Crash, scritto nel 1992 (N. STEPHENSON, *Snow Crash*, New York, 1992). Esso è descritto come una sorta di realtà virtuale, condivisa tramite Internet, dove si è rappresentanti tramite un avatar, una sorta di *alter ego* virtuale in 3d. Si sta discutendo sulla possibilità di configurare responsabilità penali per gli autori che operano tramite l'avatar nel mondo parallelo virtuale.

[18] Assemblea parlamentare del Consiglio d'Europa, *Risks and opportunities of the metaverse*, del 5 settembre 2024, Doc. 16031.

"può determinare nuove forme di discriminazione e aumentare il divario sociale". Sul punto l'Assemblea parlamentare ha bocciato l'ipotesi della sola autoregolamentazione chiedendo un intervento delle autorità pubbliche per assicurare il rispetto dei diritti fondamentali.

Inoltre, si sta discutendo sulla possibile configurabilità di responsabilità penali con atti di violenza sessuale nel metaverso. Mentre, infatti, sul piano civilistico, è pacifica la possibilità di rilevare profili di risarcimento per danni non patrimoniali, in dottrina si discute sulla possibilità di individuare delle responsabilità specifiche penali per gli autori nella realtà virtuale[19].

Se consideriamo, ad esempio, nell'ordinamento italiano, l'art. 609-*bis* c.p. rubricato "violenza sessuale" che recita che "chiunque con violenza e minaccia o mediante abuso di autorità costringe taluno a compiere o subire atti sessuali è punito con la reclusione da sei a dodici anni", emerge che la nozione ampia dell'elemento normativo extragiuridico di "atto sessuale" potrebbe far includere anche l'atto sessuale a distanza nella realtà del metaverso. A tal riguardo, anche la Cassazione penale ha fornito delle aperture interpretative con la sentenza dell'8 settembre 2020, n. 25266[20].

In Inghilterra, ad esempio, si è verificato di recente un caso di aggressione sessuale di gruppo avvenuto nel metaverso ai danni di una giovane cittadina britannica di 16 anni[21].

Anche nell'ambiente del metaverso di Meta, è stata denunciata una violenza virtuale da una ricercatrice di una società che sosteneva di essere stata palpeggiata e violentata da un avatar nella piattaforma virtuale che stava testando.

Non è da escludere, visto l'aumento dei casi denunciati di violenze virtuali, dunque, che anche il metaverso potrà in futuro giungere a Strasburgo.

[19] Già nella dottrina statunitense se ne è discusso cfr. C. MACKINNON, RICHARD, *Virtual rape in Journal of computer-mediated Communication*, 1997, vol. 2, n. 4, disponibile su https://academic.oup.com/jcmc/article/2/4/JCMC247/4584404.

[20] Cassazione penane, sentenza dell'8 settembre 2020, n. 25266.

[21] L. MIDILI, *Un caso di aggressione nel metaverso solleva interrogativi sul futuro dei processi legali per crimini virtuali*, 2024, disponibile su https://dirittodiinternet.it/un-caso-di-aggressione-sessuale-nel-metaverso-solleva-interrogativi-sul-futuro-dei-processi-legali-per-crimini-virtuali/.

Abstract

La violenza digitale, a causa dell'ampia diffusione delle tecnologie informatiche, sta diventando una nuova frontiera da esplorare per la giurisprudenza europea. Il contributo esamina la giurisprudenza della Corte EDU in materia di cyberviolenza, che rappresenta, secondo i giudici europei, una forma di violenza domestica.
In particolare sono state individuate tre pronunce rilevanti sul tema: il caso *Buturugă c. Romania*; il caso *Volodina n. 2 c. Russia* e il caso *M.S.D. c. Romania* relativa alla fattispecie di *revenge porn*.
Nelle motivazioni emerge il monito della Corte agli Stati al rispetto della *due diligence* e degli obblighi positivi di protezione delle vittime, sia di natura sostanziale che procedurale.

KEYWORDS: cyberviolenza – genere – violenza domestica – obblighi positivi di protezione – vita privata

LA JURISPRUDENCIA DEL TRIBUNAL DE ESTRASBURGO SOBRE VIOLENCIA DIGITAL

La violencia digital, debido a la amplia difusión de las tecnologías informáticas, se está convirtiendo en una nueva frontera a explorar para la jurisprudencia europea. El artículo examina la jurisprudencia del Tribunal EDU sobre ciberviolencia que, según los jueces europeos, representa una forma de violencia doméstica.
En particular, se han detectado tres sentencias relevantes sobre el tema: *Buturugă v. Rumanía*; el caso *Volodina n. 2* y el caso *M.S.D. v. Rumanía* (relativo a un caso de porno venganza).
Las motivaciones destacan la advertencia del Tribunal a los Estados de respetar la debida diligencia y las obligaciones positivas de protección a las víctimas, tanto de naturaleza sustancial como procesal.

PALABRAS CLAVE: ciberviolencia – género – violencia doméstica – obligaciones positivas de protección – vida privada

LA DIMENSIONE DIGITALE DELLA VIOLENZA CONTRO LE DONNE TRA DIRITTI UMANI E CYBERCRIMINALITÀ

*Daniela Marrani**

SOMMARIO: 1. L'eliminazione della violenza contro le donne nello spazio cibernetico quale obiettivo delle Nazioni Unite. – 2. La dimensione digitale della violenza contro le donne nella cornice dei diritti umani. – 3. Potenzialità e limiti delle Convenzioni di Istanbul e di Budapest del Consiglio d'Europa e sviluppi nel diritto dell'UE. – 4. Approccio preventivo tra obblighi degli Stati e partecipazione dei privati e della società civile.

1. *L'eliminazione della violenza contro le donne nello spazio cibernetico quale obiettivo delle Nazioni Unite*

Le Nazioni Unite costituiscono l'organizzazione internazionale a carattere universale che si è occupata per prima di tutelare e promuovere i diritti delle donne[1] e, più di recente, di affrontare i problemi di

* Professoressa associata di Diritto internazionale. Università degli Studi di Salerno, e-mail: dmarrani@unisa.it.

[1] L'attenzione al tema della violenza contro le donne a livello internazionale e regionale ha iniziato ad emergere sin dagli anni '70 del secolo scorso. La Convenzione sull'eliminazione di tutte le forme di discriminazione contro le donne (CEDAW), adottata dall'Assemblea generale delle Nazioni Unite il 18 dicembre 1979 è in vigore dal 3 settembre 1981. La Convenzione è stata ratificata dall'Italia il 10 giugno1985 con legge del 14 marzo 1985 n. 132 ed è in vigore dal 10 luglio 1985. Tra i numerosi atti di *soft law*, adottati sino ad oggi, va menzionata la Dichiarazione sull'eliminazione della violenza contro le donne proclamata dall'Assemblea generale delle Nazioni Unite con Risoluzione 48/104, del 20 dicembre 1993, A/RES/48/104. L'art. 1 della Dichiarazione definisce la violenza contro le donne *"any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life".* Di particolare rilievo per l'ampiezza e il livello di approfondimento è il Rapporto del Segretario Generale delle Nazioni Unite, *In-depth study on all forms of violence against women* del 6 luglio 2006, A/61/122/Add.1. Vanno richiamate, infine, le risoluzioni adottate a cadenza biennale dall'Assemblea generale, tra cui: *Intensifying global efforts for the elimination of female genital mutilation*,

governance del cyberspazio. Numerosi sono gli strumenti giuridici adottati in questi ambiti, sia a carattere vincolante, che di natura raccomandatoria e gli orientamenti indirizzati agli Stati. Tra questi ultimi, Agenda 2030 per lo sviluppo sostenibile stabilisce l'obiettivo 5 "*to achieve gender equality and empowerment of all women and girls*" e l'obiettivo 16 "*to promote peaceful and inclusive societies for sustainable development*"[2].

Gli sviluppi delle tecnologie digitali hanno modellato la vita sociale e ampliato a dismisura le modalità di interazione umana, basti considerare il diffuso utilizzo di smartphone, pc e tablet e, soprattutto, delle piattaforme di social media. In questo contesto, si è posto il problema di disciplinare o meno (con norme *ad hoc*) le attività degli Stati e dei privati in Internet, problema molto dibattuto che non ha trovato finora soluzioni globali[3]. Si ritiene, al riguardo, che ciò che è vietato

del 16 dicembre 2020, A/RES/75/160 e *Intensification of efforts to prevent and eliminate all forms of violence against women and girls*, del 16 dicembre 2020, A/RES/75/161; *Intensification of efforts to prevent and eliminate all forms of violence against women and girls* (*Report of the Secretary General*), del 18 agosto 2022, A/77/302; *Intensification of efforts to prevent and eliminate all forms of violence against women and girls: gender stereotypes and negative social norms*, del 15 dicembre 2022, A/RES/77/193.

[2] Assemblea generale, Risoluzione, *Transforming our world: the 2030 Agenda for Sustainable Development*, A/RES/70/1, del 21 ottobre 2015.

[3] Si veda G.M. RUOTOLO, A.M. GALLO, *Le norme sulla lotta alla violenza di genere online nel contesto della regolamentazione internazionale ed europea di Internet: alcune questioni generali e di metodo/Normas para combatir la violencia de género en línea en el contexto de la regulación internacional y europea de Internet: algunas cuestiones generales y metodológicas*, in questo Volume pp. 61-82. Sui profili di disciplina di Internet la bibliografia è molto vasta, si veda *ex multis*, M. NINO, *The Freedom of Expression and Hate Speech in Cyberspace*, in *La Comunità internazionale*, 2023, n.1, pp. 33-57; G.M. RUOTOLO, *Le fonti dell'ordinamento internazionale e la disciplina della Rete*, in *DPCE online*, 2021, pp. 701-741; A. ODDENINO, *La violazione di sistemi informatici contenenti informazioni riservate come illecito internazionale: tra dimensione interstatuale e tutela dei diritti umani*, in M. DISTEFANO (a cura di) *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, pp. 13-36; G.M. RUOTOLO, *Internet-ional law. Profili di diritto internazionale pubblico della rete*, Bari, 2012. Per gli aspetti relativi alla sicurezza dello spazio cibernetico e alle iniziative delle organizzazioni internazionali, sia consentito rinviare a D. MARRANI, *La cooperazione internazionale per la sicurezza e la stabilità nel* cyberspace, Napoli, 2020.

nel mondo "fisico" lo sia anche nello spazio cibernetico[4]. Emerge, quindi, l'esigenza di interpretare ed applicare le norme internazionali ed europee esistenti al fine di tutelare i diritti umani negli spazi digitali[5].

L'attenzione che le Istituzioni internazionali hanno rivolto alla protezione delle donne da ogni forma di discriminazione e gli strumenti adottati contro ogni forma di violenza anche domestica richiede, quindi, di considerare non solo le fattispecie del mondo fisico (offline) ma anche ogni violazione che emerga in Rete e negli spazi digitali (online), che si iscrive nel *continuum* con le prime[6], secondo una classificazione ancora indeterminata e non esaustiva[7].

Al livello globale, va considerata la Convenzione sull'eliminazione di tutte le forme di discriminazione contro le donne (CEDAW, secondo l'acronimo inglese)[8]. Particolare rilievo assume, per quanto concerne la violenza digitale di genere, la *General Recommendation No. 35 on gender-based violence against women* adottata dal Comitato per l'eliminazione delle discriminazioni contro le donne, (CEDAW Committee), secondo cui "*gender-based violence against women occurs in* all spaces and spheres of human interaction, *whether public or private. These include the family, the community, the public spaces, the workplace, leisure, politics, sport, health services, educational settings and*

[4] Se ciò è vero, in linea di massima, va tenuto conto anche del carattere ubiquitario di Internet e della capacità di diffondere gli effetti dannosi di una condotta criminosa (si pensi ad esempio alla diffamazione online) o, al contrario, di essere utilizzato per far conoscere e promuovere azioni lecite.

[5] Va appena evidenziato che la protezione dei diritti umani nell'era digitale costituisce, tra l'altro, uno degli otto ambiti di intervento prioritari (*key focus areas*) della *Roadmap for digital cooperation* delineata dal Segretario generale delle Nazioni Unite nel giugno 2020, disponibile su: https://www.un.org/en/content/digital-cooperation-roadmap/. L'adozione della *Roadmap* fa seguito all'istituzione da parte del Segretario generale delle Nazioni Unite dell'*High-level Panel on Digital Cooperation* nel luglio 2018.

[6] Per una descrizione del fenomeno ed un inquadramento generale si rimanda a A. IERMANO, *Violenza digitale e Convenzione di Istanbul: una dimensione distinta ma non separata dalla violenza contro le donne*, in *Freedom, Security and Justice: European Legal Studies*, n. 1, 2024, pp. 64- 95.

[7] La terminologia non è sempre precisa nei contenuti ed appare frammentaria.

[8] Vedi nota 1.

their redefinition through technology-mediated environments, such as contemporary forms of violence occurring on the Internet and digital spaces"[9](enfasi aggiunta).

Nel Rapporto presentato al Consiglio sui diritti umani, la relatrice speciale delle Nazioni Unite sulla violenza contro le donne, definisce il fenomeno della violenza digitale secondo una prospettiva di genere, come: "*any act [...] that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately*"[10]. Da tale definizione emerge, in particolare, il potenziale degli strumenti digitali di aggravare la violenza contro le donne. Il Rapporto sottolinea anche che non è sempre agevole distinguere le conseguenze di azioni "*that are initiated in digital environments from offline realities, and viceversa*"[11].

Sebbene il fenomeno della cyberviolenza si sia sviluppato in gran parte successivamente all'adozione della CEDAW, il Comitato CEDAW ha svolto un compito di particolare rilievo in quanto ha analizzato, progressivamente, l'impatto della violenza digitale contro le donne sulla violazione dei diritti garantiti dalla Convenzione ed ha richiamato gli Stati al rispetto degli obblighi positivi di prevenire, proteggere e perseguire la cyberviolenza contro donne e bambine[12]. Alcuni atti

[9] Committee on the Elimination of Discrimination against Women, General recommendation No. 35 *on gender-based violence against women, updating general recommendation No. 19*, del 26 luglio 2017, par. 20, p. 7.

[10] Vedi Human Rights Council, Report of the Special Rapporteur on violence against women, its causes and consequences on online, MS. DUBRAVKA ŠIMUNOVIĆ, *violence against women and girls from a human rights perspective*, A/HRC/38/47, del 18 giugno 2018, par. 23.

[11] *Ivi,* par. 20.

[12] In tale contesto, vanno menzionate alcune raccomandazioni del Comitato delle Nazioni Unite per l'eliminazione della discriminazione contro le donne, *General Recommendation No. 19 on violence against women*, A/47/38, 1992, la quale è stata in seguito aggiornata dalla Recommendation N° 35 (menzionata sopra alla nota 9) e, a seguire, la *General Recommendation n° 36 on the Right of Girls and Women to Education*, del 16 novembre 2017, CEDAW/C/GC/36 la quale sottolinea l'impatto negativo della cyberviolenza (in particolare di comportamenti on line quali *bulling*, *harassment* e *revenge porn*) sul godimento e la realizzazione del diritto all'istruzione di donne e minori.

di natura raccomandatoria delle Nazioni Unite, inclusi quelli del Consiglio sui diritti umani[13], hanno preceduto e preparato il lavoro del Comitato CEDAW a dimostrazione dell'attenzione costante e progressiva dell'Organizzazione sul tema.

Il Consiglio d'Europa e l'Unione europea, in linea con gli obiettivi delle Nazioni Unite, introducono specifici obblighi degli Stati al fine di tutelare in maniera effettiva le donne anche (sia pure non sempre in maniera diretta) dalla violenza digitale, come si dirà nel prosieguo. L'approccio adottato dalla Convenzione di Istanbul[14], in particolare, si articola su quattro tipologie di interventi degli Stati membri, indicati anche come 4 pilastri (4P): prevenzione, protezione, perseguimento penale e politiche coordinate. Anche l'Unione europea si è impegnata a dare attuazione alla Convenzione di Istanbul, alla quale ha aderito nel giugno 2023[15], mediante l'adozione della direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica, il 24

[13] Cfr. Risoluzione del Consiglio sui diritti umani, *Accelerating efforts to eliminate all forms of violence against women: eliminating domestic violence*, del 22 luglio 2015, A/HRC/RES29/14, la quale ha riconosciuto che: "*violence against women can take the form of an isolated act or pattern of abusive behaviour that may occur over a period of time, which as a pattern constitutes violence against women, and can include acts such as* cyberbulling *and* cyberstalking", par. 4; a seguire, l'Assemblea generale ha adottato la Risoluzione *The right to privacy in the digital age* del 25 gennaio 2017, A/RES/71/199, la quale invita gli Stati a prevenire e reprimere*: "violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women"* (par. 5, lett. g), alla quale è seguita la Risoluzione del Consiglio sui diritti umani, *The right to privacy in the digital age*, del 7 aprile 2017, A/HRC/RES/34.

[14] Consiglio d'Europa, Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, CETS/21. La Convenzione di Istanbul è stata adottata dal Consiglio d'Europa l'11 maggio 2011 ed è entrata in vigore a seguito del raggiungimento del numero previsto di dieci ratifiche (di cui 8 paesi membri del Consiglio d'Europa) il 1° agosto 2014. Al 4 febbraio 2025, la Convenzione conta 39 Stati parte. L'Italia ha sottoscritto la Convenzione il 27 settembre 2012 e il Parlamento ha autorizzato la ratifica con Legge n. 77/2013; si veda Camera dei Deputati, *La Convenzione di Istanbul contro la violenza nei confronti delle donne. L'attuazione nell'ordinamento interno*, in Documentazione e ricerche, del 15 novembre 2017, n. 50, reperibile online.

[15] La Convenzione di Istanbul è entrata in vigore nell'Unione europea il 1° ottobre 2023.

maggio 2024, con obbligo di recepimento degli Stati membri entro il 14 giugno 2027[16]. Nell'esaminare la disciplina internazionale ed europea avente ad oggetto la dimensione digitale della violenza contro le donne, il presente contributo si focalizzerà su alcuni aspetti della tutela dei diritti umani nell'ambito del Consiglio d'Europa e dell'Unione europea con particolare riguardo agli obblighi preventivi degli Stati e al necessario contributo degli attori privati e della società civile.

2. *La dimensione digitale della violenza contro le donne nella cornice dei diritti umani*

Nell'ambito delle Nazioni Unite, gli strumenti di protezione internazionale dei diritti umani, inclusa la CEDAW, non stabiliscono espressamente norme che sanzionino in maniera diretta ed autonoma la violenza contro le donne. La Convenzione si occupa della violenza contro le donne in quanto forma di discriminazione contemplata dalla CEDAW. A differenza della CEDAW, la Convenzione di Istanbul adottata dal Consiglio d'Europa nel 2011 ed entrata in vigore nel 2014, si propone espressamente l'obiettivo di "*protect women against all forms of violence, and prevent, prosecute and eliminate violence against women and domestic violence*" (art. 1, par. 1, a)). Come è stato osservato, la Convenzione di Istanbul codifica e sviluppa ulteriormente gli

[16] Per una accurata analisi della direttiva, si veda, in questo Volume, E. BERGAMINI, S. DE VIDO, *La cyberviolenza di genere nel rapporto fra la direttiva 2024/1385 e gli altri strumenti di diritto dell'Unione europea/La ciberviolencia de género en la relación entre la directiva 2024/1385 y otros instrumentos del derecho comunitario*, pp. 329-355; A. FESTA, *Dalla strategia per la parità di genere all'inserimento della violenza digitale tra gli "eurocrimini": l'approccio olistico dell'Unione europea al fenomeno della violenza contro le donne e di genere/De la estrategia de igualdad de género a la inclusión de la violencia digital entre los "eurocrímenes": el enfoque holístico de la Unión europea ante el fenómeno de la violencia contra las mujeres y de género*, pp. 357-383 nonché E. BERGAMINI, *Combating Violence Against Women and Domestic Violence from the Istanbul Convention to the EU Framework: the Proposal for an EU Directive*, in *Freedom, Security and Justice: European Legal Studies*, n. 2, 2023, pp. 21- 41. Di recente, si veda, M. FERRARI, *Violenza contro le donne: l'Unione europea adotta finalmente la direttiva (UE) 2024/1385*, in *Eurojus.it*, 17 giugno 2024.

standard elaborati dalla CEDAW a dimostrazione di una sinergia tra i due strumenti internazionali[17].

Particolare importanza assume il riconoscimento espresso della violenza contro le donne quale violazione dei diritti umani, oltre che come forma di discriminazione contro le donne (art. 3)[18]. Rileva anche la relazione tra parità di genere ed eliminazione della violenza contro le donne[19]. L'art. 4, par. 1, sancisce l'obbligo degli Stati parte di "*take the necessary legislative and other measures to promote and protect the right for everyone, particularly women, to live free from violence in both the public and the private sphere*". Disposizioni speculari all'art. 4 sono contenute in altre convenzioni regionali a tutela dei diritti umani. Si evince uno specifico diritto a vivere liberi dalla violenza che non è riconosciuto solo alle donne ma è richiesto agli Stati di rivolgere particolare attenzione alle donne. Parimenti, la norma precisa che la tutela è estesa sia all'ambito pubblico, tradizionalmente oggetto di rapporti disciplinati dal diritto internazionale, che all'ambito privato, come sollecitato dai difensori dei diritti delle donne e dei soggetti più vulnerabili[20].

L'applicazione della Convenzione si basa sulla considerazione secondo cui la violenza digitale contro le donne costituisce un *continuum* rispetto alla violenza che si realizza nelle fattispecie disciplinate dagli ordinamenti interni, aventi ad oggetto comportamenti posti in essere nella vita reale (offline). In generale, gli Stati parte si propongono di affrontare la dimensione digitale della violenza contro le donne come parte integrante di un approccio olistico e multisettoriale volto a con-

[17] Si veda S. DE VIDO, M. FRULLI, *Article 1 Purposes of the Convention*, in S. DE VIDO, M. FRULLI, *op. cit.*, p. 85 ss., e in partic. p. 87; D. ŠIMONOVIĆ, *Global and Regional Standards on Violence Against Women: The Evolution and Synergy of the CEDAW and Istanbul Conventions*, in *Human Rights Quarterly*, Vol. 36, No. 3, pp. 590-606.

[18] Vedi S. DE VIDO, M. FRULLI (a cura di), *op. cit.*, *passim*.

[19] In tema di genere e di violenza di genere in ambito internazionale ed europeo, si veda A. DI STASI, R. CADIN, A. IERMANO, V. ZAMBRANO (a cura di), *Donne migranti e violenza di genere nel contesto giuridico internazionale ed europeo*, Napoli, 2023.

[20] In proposito, si veda quanto osservato da A. SINCLAIR-BLAKEMORE, *Cyberviolence Against Women Under International Human Rights Law: Buturuga v. Romania and Volodina v. Russia (No 2)*, in *Human Rights Law Review*, 2022, n. 23, pp. 1- 27 e spec. p. 4.

trastare la violenza di genere. L'approccio appare giustificato dalla complessità del fenomeno e dalle molteplici implicazioni ed effetti che non si esauriscono al livello giuridico (o della violazione dei diritti umani) ma hanno implicazioni psicologiche, sociologiche, economiche e sociali, per citarne solo alcune.

In particolare, gli Stati parte si sono impegnati ad adempiere agli obblighi stabiliti dalla Convenzione che consistono nel criminalizzare i comportamenti di violenza contro le donne secondo la definizione contenuta nell'art. 3, lett. a)[21]. Tali comportamenti includono la violenza digitale, seppure non espressamente menzionata dalla Convenzione e non ancora oggetto di una categorizzazione completa ed esaustiva, che comprendono, tra l'altro, i seguenti: violenza psicologica online; *stalking* online; la condivisione di immagini non consensuale; il bullismo a sfondo sessuale online; le molestie sessuali con mezzi digitali ed altri ancora[22].

L'ampio ventaglio di comportamenti oggetto di studio ai fini di una categorizzazione il più possibile esaustiva include tutte le forme di violenza online e le forme di violenza *agevolate dalla tecnologia* ("online *and technology-facilitated violence against women*")[23].

[21] Per violenza contro le donne ai sensi dell'art. 3, lett. a), della Convenzione di Istanbul si intende: "*a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life*". In attuazione della Convenzione, gli Stati hanno l'obbligo di criminalizzare specifiche condotte che costituiscono forme di violenza contro le donne, quali, ad esempio, il matrimonio forzato (art. 37, par. 1, della Convenzione di Istanbul). Cfr. S. DE VIDO, *A Legal Analysis of the Contributing Factors to Trafficking in Women: Points of Strength and Weakness of the Recent Developments in Europe*, in *Freedom Security & Justice*, *European Legal Studies*, 2023, n. 1, pp. 41- 73, e spec. p. 53.

[22] Si veda, per ulteriori approfondimenti, A. IERMANO, *Violenza digitale e Convenzione di Istanbul*, cit., pp. 69- 70.

[23] Un contributo all'inquadramento concettuale delle diverse forme di violenza digitale è contenuto in Consiglio d'Europa, A. VAN DER WILK, *Protecting women and girls from violence in the digital age. The relevance of the Istanbul Convention and the Budapest Convention on cybercrime in addressing online and technology-facilitated violence against women*, 2021, p. 9 e ss.

Della necessità di interpretare il testo della Convenzione di Istanbul alla luce dei cambiamenti tecnologici e sociali più recenti si è fatto carico il Gruppo di esperti del Consiglio d'Europa sulla lotta contro la violenza nei confronti delle donne e la violenza domestica (GREVIO), il quale ha elaborato nel 2021 una raccomandazione indirizzata agli Stati parte (Raccomandazione n. 1) contenente dettagliati orientamenti ai fini dell'applicazione della Convenzione[24].

La Raccomandazione n. 1, in particolare, considera alcune forme di violenza online o agevolate dalla tecnologia quali comportamenti vietati da specifiche norme della Convenzione di Istanbul. In specie, sono menzionate: la violenza psicologia online (art. 33), lo *stalking* online o compiuto nella sfera in digitale (art. 34) e le molestie sessuali online o mediante mezzi digitali (art. 40).

3. *Potenzialità e limiti delle convenzioni di Istanbul e di Budapest del Consiglio d'Europa e sviluppi nel diritto dell'UE*

La Convenzione di Istanbul, come sopra evidenziato, stabilisce obblighi piuttosto estesi degli Stati parte con l'obiettivo di contrastare la violenza contro le donne e la violenza domestica ma non disciplina direttamente la violenza digitale[25]. Questo aspetto, che è stato descritto come un elemento di debolezza della Convenzione[26], insieme ad altri aspetti meno rilevanti ai nostri fini, sembra superato dal contributo interpretativo della Corte europea dei diritti dell'uomo (Corte EDU) e dalla sopra menzionata Raccomandazione n. 1 del GREVIO. Anche la Convenzione di Budapest il cui scopo è il perseguimento dei crimini informatici, unitamente al Protocollo sulla raccolta delle prove digita-

[24] Consiglio d'Europa, GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women*, Strasbourg, 2021, disponibile su: https://rm.coe.int/grevio-rec-no-on-digital-violence-against women/1680a49147.

[25] G. GUNEY, *The Istanbul Convention: A Missed Opportunity in Mainstreaming Cyberviolence against Women in Human Rights Law?*, in *EJIL:Talk!*, 10 marzo 2022.

[26] Cfr. S. DE VIDO, M. FRULLI, *Introduction to preventing and combating violence against women and domestic violence*, in S. DE VIDO, M. FRULLI-(a cura di), *op. cit.*, p. 2.

li[27], presenta limiti e potenzialità nel contrastare la violenza digitale contro le donne[28]. Va evidenziato, infatti, che la Convenzione di Budapest, il cui scopo è il perseguimento dei crimini informatici, non si occupa espressamente di violenza digitale. Il coordinamento tra le due convenzioni del Consiglio d'Europa, pertanto, è necessario e rimesso all'attività interpretativa dei giudici e della dottrina[29].

La giurisprudenza della Corte EDU svolge un ruolo fondamentale allo scopo di inquadrare il fenomeno della violenza digitale contro le donne all'interno dei diritti umani di cui l'ordinamento internazionale e quello dell'Unione europea, integrato con il sistema della Convenzione europea dei diritti dell'uomo (CEDU), si fanno carico di assicurare una tutela piena ed effettiva[30].

Nei casi *Buturugă c. Romania, Volodina c. Russia* e, più di recente, *M.S.D. c. Romania*[31] la Corte si pronuncia sulla base degli artt. 2, 3, 8 e 14 della CEDU. In particolare, è alla luce dell'art. 8 della CEDU che la Corte argomenta al fine di riconoscere i diritti delle vittime di violenza digitale. L'analisi delle pronunce in parola esula dall'ambito del presente lavoro, basti evidenziare le critiche espresse dalla dottrina in me-

[27] G.M. RUOTOLO, *Il secondo Protocollo alla Convenzione cybercrime: le prove elettroniche tra diritto internazionale e relazioni esterne dell'Unione europea*, in *Diritto penale e processo*, 2022, n. 8, p. 1022 ss.

[28] Si veda, al riguardo, Council of Europe*, Cybercrime Convention Committee, Working Group on Cyberbullying and Other Forms of Online Violence, especially against Women and Children*, *Mapping Study on Cyberviolence*, T-CY (2017)10, del 9 luglio 2018.

[29] In argomento, si veda, A. IERMANO, *Convenzione di Istanbul e Convenzione di Budapest: una risposta coordinata alla cyberviolenza contro le donne/Convenio de Estambul y Convenio de Budapest: una respuesta coordinada al fenómeno de la ciberviolencia contra las mujeres*, in questo Volume pp. 185-213.

[30] Per un approfondimento sui casi decisi dalla Corte europea dei diritti dell'uomo in tema di cyberviolenza si veda V. TEVERE, *La giurisprudenza della Corte di Strasburgo in materia di violenza digitale/La jurisprudencia del Tribunal de Estrasburgo sobre violencia digital*, in questo Volume, pp. 257-272.

[31] Corte europea dei diritti dell'uomo, sentenza dell'11 febbraio 2020, ricorso n. 56867/15, *Buturugă c. Romania*; Corte europea dei diritti dell'uomo, sentenza del 9 luglio 2019, ricorso n. 41261/17 *Volodina c. Russia*; Corte europea dei diritti dell'uomo, sentenza del 3 dicembre 2024, ricorso n. 28935/21, *M.S.D. c. Romania*.

rito al richiamo dell'art. 8 della CEDU, norma ritenuta "debole" (in confronto all'art. 3) rispetto alla gravità delle violazioni commesse.

La prevenzione della violenza digitale contro le donne, in particolare, è oggetto non solo di interpretazione da parte della giurisprudenza ma anche di specifiche raccomandazioni formulate dal GREVIO, su cui si tornerà nel prosieguo[32].

L'Unione europea ha adottato la direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica, il 24 maggio 2024, con obbligo di recepimento degli Stati membri entro il 14 giugno 2027[33]. La direttiva sarà obbligatoria anche per gli Stati membri che non hanno ratificato la Convenzione di Istanbul. I suoi contenuti coincidono in gran parte con quelli della Convenzione, con l'aggiunta, tra l'altro, di aspetti relativi alla violenza online[34].

Un ruolo decisivo nell'affermazione dei diritti delle donne vittime di violenza digitale potrà essere svolto dalla Corte di giustizia, la quale terrà conto sia della giurisprudenza della Corte europea dei diritti dell'uomo che della Raccomandazione n. 1 del GREVIO al fine di garantire l'uguaglianza dei diritti delle donne nell'UE[35].

Questa considerazione va inserita in un quadro più ampio che prende come riferimento il processo di integrazione europea nel suo complesso, in cui la protezione dei valori dell'UE, inclusi i diritti fondamentali e i dati personali, vanno di pari passo con la costruzione di uno spazio di libertà sicurezza e giustizia, che include la prevenzione e la repressione dei reati e con gli sforzi per garantire la sicurezza interna ed esterna dell'Unione europea[36]. È auspicabile che questa prospettiva

[32] Vedi par. 4.

[33] Si veda, A. FESTA, *Dalla strategia per la parità di genere all'inserimento della violenza digitale tra gli "eurocrimini": l'approccio olistico dell'Unione europea al fenomeno della violenza contro le donne e di genere/De la estrategia de igualdad de género a la inclusión de la violencia digital entre los "eurocrímenes": el enfoque holístico de la Unión europea ante el fenómeno de la violencia contra las mujeres y de género*, in questo Volume pp. 357-383, e l'ulteriore bibliografia citata alla nota 16.

[34] V. Parte II del presente Volume.

[35] Per un esempio di dialogo tra le Corti europee in materia di diritti umani si veda, da ultimo, A. DI STASI, *Human Dignity and Migrants in the Case law of the ECHTR and CJEU: Embryonic Character of the Jurisprudential "Dialogue" between the two Courts*, in *Revista General de Derecho Europeo*, 2024, pp. 1-23.

[36] Sul punto, si veda A. ORIOLO, *Transnational Crime and EU Law: Towards*

ampia ed integrata ispiri il dibattito sulla protezione dei dati personali, quali diritti fondamentali dei cittadini dell'UE, nell'ottica dell'ampio utilizzo di tecnologie digitali sempre più intrusive della sfera privata e in grado di apportare numerosi benefici, come l'Intelligenza Artificiale (IA).

Nella medesima prospettiva di prevenzione e di repressione della criminalità, vale la pena ricordare che, recentemente, sono state introdotte specifiche deroghe alla direttiva 2002/58 (vedi regolamento (UE) 2024/1307 e regolamento (UE) 2021/1232) per quanto riguarda l'utilizzo di tecnologie da parte dei *provider* per contrastare l'abuso sessuale online di minori[37]. Il regolamento (UE) 2024/1307 proroga fino al 3 aprile 2026 il periodo di applicazione del quadro giuridico temporaneo in materia di abusi sessuali sui minori previsto dal regolamento (UE) 2021/1232 in deroga alla direttiva 2002/58.

4. *Approccio preventivo tra obblighi degli Stati e partecipazione dei privati e della società civile*

Nell'ambito dell'ampio ventaglio di misure che gli Stati parte della Convenzione di Istanbul si sono impegnati ad adottare al fine di contrastare tutte le forme di violenza contro le donne che rientrano nel suo ambito di applicazione, inclusa la violenza digitale, articolate nei menzionati 4P, la prevenzione costituisce il fine ultimo ("*the ultimate aim*", come è stato osservato)[38], e con ogni probabilità l'obiettivo più ambizioso della Convenzione.

Gli strumenti repressivi che le norme penali possono offrire, uni-

Global Action against Cross-Borders Threats to Common Security, Rule of Law and Human Rights, in *Bulletin of the Transilvania University of Brasov*, 2023, p. 197 ss.

[37] Regolamento (UE) 2024/1307 del Parlamento europeo e del Consiglio, *che modifica il regolamento (UE) 2021/1232 relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei prestatori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori,* del 29 aprile 2024, GUUE L del 14 maggio 2024.

[38] Così S. DE VIDO e M. FRULLI, *Article 1 Purposes of the Convention*, in S. DE VIDO, M. FRULLI (a cura di), *op. cit.*, p. 91.

tamente alle politiche coordinate non risultano sufficienti ad offrire una soluzione efficace alla violenza contro le donne e ancor meno alla violenza digitale che dilaga in maniera spesso sommersa e subdola con la complicità delle tecnologie e delle piattaforme digitali, e ancor più spazio potrà guadagnare in futuro avvalendosi di strumenti di IA e di nuovi sviluppi tecnologici.

L'approccio olistico che combina diversi livelli di azione (dalle misure penali a quelle civili; dal perseguimento dei reati alla protezione delle vittime; dalle attività in ambito pubblico a quelle dei privati e, inoltre, le misure preventive e di protezione) appare il più adatto a tutelare in maniera effettiva le donne da ogni forma di violenza oggi immaginabile e richiederà un grande impegno di diversi soggetti ed attori ed un significativo coordinamento a diversi livelli.

Ai fini del presente lavoro, si utilizzerà il termine "prevenzione" in maniera ampia che potrà includere sia le politiche coordinate sia la *due diligence* degli Stati nei confronti di comportamenti di attori non statali, ai sensi dell'art. 5 della Convenzione di Istanbul.

L'art. 12 definisce gli obblighi generali in materia di prevenzione: "Le Parti adottano le misure necessarie per promuovere i cambiamenti nei comportamenti socio-culturali delle donne e degli uomini, al fine di eliminare pregiudizi, costumi, tradizioni e qualsiasi altra pratica basata sull'idea dell'inferiorità della donna o su modelli stereotipati dei ruoli delle donne e degli uomini" (par. 1), ed inoltre "Le Parti adottano le misure legislative e di altro tipo necessarie per impedire ogni forma di violenza rientrante nel campo di applicazione della presente Convenzione commessa da qualsiasi persona fisica o giuridica" (par. 2).

La violenza contro le donne nella sua dimensione digitale viene spesso commessa attraverso piattaforme digitali private, ad esempio: società di social media, tecnologie di comunicazione della telefonia, siti di *microblogging*, applicazioni di messaggistica o di incontri o alcuni siti web pornografici. Inoltre, le principali piattaforme che aggregano e indicizzano la conoscenza mondiale e progettano gli algoritmi che influenzano le informazioni diffuse online sono società private[39]. Come è

[39] Sui profili di regolamentazione delle piattaforme digitali, si veda, tra gli altri, F. BASSAN, *Digital Platforms and Global Law*, Cheltenham, 2021.

stato osservato, è essenziale collaborare con tali società al fine di prevenire la violenza digitale[40].

Allo stato attuale, tuttavia, come è stato rilevato dal Consiglio sui diritti umani nel 2018, le responsabilità delle piattaforme digitali non sono ancora pienamente affermate nel quadro internazionale dei diritti umani[41]. Inoltre, mentre è stata prestata particolare attenzione alle responsabilità dei fornitori intermediari di servizi Internet, non si è considerato in maniera adeguata l'impatto delle norme e delle prassi di tali intermediari sulle donne[42].

In questo contesto, l'art. 5, par. 2 stabilisce l'obbligo generale degli Stati di esercitare la *due diligence* nel prevenire, indagare, punire i responsabili e risarcire le vittime di atti di violenza commessi da attori non statali. Come osservato nell'*Explanatory Report* e dal GREVIO, tali obblighi consistono in obblighi di condotta e non di risultato. Gli Stati parte sono in ogni caso tenuti ad impegnarsi (*display best effort*)[43] investendo in tutte le necessarie azioni di prevenzione, indagine, punizione, riparazione e protezione[44]. Di conseguenza, come è emerso dalla giurisprudenza di alcune Corti internazionali sui diritti umani, gli Stati possono essere ritenuti responsabili sul piano internazionale per la violazione di obblighi di prevenzione degli atti di violenza compiuti da attori non statali[45]. Allo stesso modo, la *due diligence* nei confronti de-

[40] Plateforme des mécanismes indépendants d'experts sur la discrimination et la violence à l'égard des femmes, Rapporto tematico, *La dimension numérique de la violence à l'égard des femmes abordée par les sept mécanismes de la Plateforme EDVAW*, 17 novembre 2022, p. 3.

[41] Consiglio sui diritti umani, Report, par. 71. Vedi sopra nota 10.

[42] *Ivi*, par. 73.

[43] Cfr. A. OLLINO, *State obligations and* due diligence, in S. DE VIDO, M. FRULLI (a cura di), *op. cit*., p. 136 ss. in partic. p. 140 s.

[44] Si veda, sul punto, E. MARTÍNEZ GARCÍA, *Ciberviolencia machista en el marco de la directiva (UE) 2024/1385 y Convenio de Estambul: perspectiva de género y obligaciones del Estado/La cyberviolenza di genere nel quadro della direttiva (UE) 2024/1385 e della Convenzione di Istanbul: prospettiva di genere e obblighi dello Stato*, in questo Volume pp. 215-255.

[45] Cfr. Corte interamericana dei diritti dell'uomo, sentenza del 17 agosto 1990, *Case of Velásquez Rodríguez v. Honduras*, Interpretation of the judgment of reparations and costs, par. 172; Corte europea dei diritti dell'uomo, sentenza del 9 giugno 2009, ricorso n. 33401/02, *Opuz c. Turchia*, par. 129.

gli attori non statali è stata raccomandata dal Comitato CEDAW nella *General Recommendation n. 35*[46].

Nella prospettiva di ottenere un risultato utile, la Raccomandazione n. 1 invita gli Stati parte a coinvolgere le aziende (*Information and Communications Technology*) negli sforzi per ritenere gli autori di violenza contro le donne responsabili delle loro azioni e raccomanda in particolare di istituire meccanismi di denuncia, segnalazione e rimozione di contenuti efficaci, adottando pratiche di moderazione dei contenuti e garantendo che le tecnologie siano progettate in modo da rispettare la dimensione di genere[47].

Nell'ambito delle azioni di prevenzione, in senso ampio e, nello specifico, delle politiche coordinate, va menzionato l'art. 9 della Convenzione, il quale evidenzia il significativo contributo delle ONG e della società civile. Come suggerito nell'*Explanatory Report*, l'art. 9 impegna gli Stati parte a riconoscere il lavoro di ONG e società civile, ad esempio "*by tapping into their expertise and involving them as partners in multi-agency co-operation or in the implementation of comprehensive government policies which Article 7 calls for*"[48].

In particolare, le politiche coordinate dovranno occuparsi di rimuovere stereotipi e pregiudizi che sono all'origine della violenza contro le donne, e tutelare le donne con identità intersezionale (ovvero con diverse vulnerabilità, quali: povertà, minore età, bisessualità, disa-

[46] Comitato delle Nazioni Unite per l'eliminazione della discriminazione contro le donne, *General Recommendation n. 35 on gender-based violence against women, updating general recommendation No. 19 (1992)*, del 26 luglio 2017: "*That obligation, frequently referred to as an obligation of due diligence, underpins the Convention as a whole and accordingly States parties will be held responsible should they fail to take all appropriate measures to prevent, as well as to investigate, prosecute, punish and provide reparations for, acts or omissions by non-State actors that result in gender-based violence against women, including actions taken by corporations operating extraterritorially. In particular, States parties are required to take the steps necessary to prevent human rights violations perpetrated abroad by corporations over which they may exercise influence, whether through regulatory means or the use of incentives, including economic incentives*", par. 24.

[47] Consiglio d'Europa, GREVIO, *General Recommendation No 1 on the digital dimension of violence against women*, 2021, par. 57 g).

[48] Cfr. Consiglio d'Europa, *Explanatory Report to the Convention on preventing and combating violence against women and domestic violence*, par. 69.

bilità, donne migranti). Come è stato suggerito: "*Initiatives that aim to modify harmful stereotypes and promote change at societal level for more gender equality will thus positively impact behaviors online and offline*"[49].

In aggiunta ai cambiamenti culturali e sociali in tema di uguaglianza di genere, gli ordinamenti degli Stati dovranno tenere conto, nella loro legislazione, di tutte le forme di violenza digitale contro le donne, compresi: molestie, *stalking*, violenza psicologica e incitamento all'odio[50]. Al riguardo, il ruolo che i giudici potranno svolgere nel contribuire all'evoluzione della legislazione sarà fondamentale.

Come è stato sottolineato, al fine di eliminare le cause profonde della violenza contro le donne gli Stati devono investire in programmi educativi a tutti i livelli "*that explain the endemic and structural nature of violence against women (…) and promote non-violence and gender equality*"[51]. Tali programmi devono andare di pari passo con le misure di contrasto agli stereotipi e a campagne informative sulle diverse forme di violenza contro le donne, incluse la violenza psicologica e la violenza digitale[52]. L'investimento dovrà includere la formazione di differenti figure professionali da utilizzare allo scopo (docenti, forze dell'ordine, magistrati, avvocati, personale sanitario, giornalisti ed altri)[53].

Nell'ambito delle azioni preventive e delle politiche integrate, in attuazione della Convenzione di Istanbul, un ruolo fondamentale è svolto dalle Università nella promozione della cultura delle pari opportunità che costituisce il sostrato nel quale germogliano e crescono

[49] Così Consiglio d'Europa, *Protecting women and girls from violence in the digital* age, cit., p. 40.

[50] Nell'ambito delle numerose iniziative legislative adottate in Italia a seguito della ratifica della Convenzione di Istanbul, va menzionata in particolare, per quanto riguarda le misure di prevenzione anche della violenza digitale contro le donne, la Legge 24 novembre 2023, n. 168

[51] Così S. DE VIDO, M. FRULLI, *Article 1 Purposes of the Convention*, in S. DE VIDO, M. FRULLI (a cura di), *op. cit.*, p. 91.

[52] *Ibidem*.

[53] Un ruolo importante al fine di realizzare programmi educativi sull'uguaglianza di genere è svolto dalla scuola. In Italia va menzionata, da ultimo, la proposta di Legge AC 1266 recante "Modifiche alla legge 20 agosto 2019, n. 92, concernenti l'introduzione dell'educazione alle pari opportunità femminili nell'ambito dell'insegnamento dell'educazione civica", presentata il 30 giugno 2023.

l'uguaglianza e il rispetto e si coltivano i talenti per la costruzione di società umane e solidali[54], il miglior antidoto alla violenza di genere.

Abstract

Il contributo parte dall'assunto secondo cui la Convenzione di Istanbul sulla violenza contro le donne e la violenza domestica e la Convenzione di Budapest e il suo secondo Protocollo addizionale sulla cooperazione rafforzata e la divulgazione delle prove elettroniche affrontino ciascuno in maniera indiretta e parziale la dimensione digitale della violenza contro le donne e debbano essere applicati in maniera integrata dagli Stati. Rilevati i limiti della tutela repressiva per gli atti di cybercriminalità contro le donne, anche alla luce della giurisprudenza della CEDU, il lavoro si interroga sull'opportunità per gli Stati membri di investire sul paradigma preventivo e di protezione alla luce dell'art. 5, par. 2 della Convenzione di Istanbul, come suggerito dal GREVIO nella raccomandazione n. 1. In questa prospettiva, considerati gli sviluppi e le sfide dell'intelligenza artificiale, il contributo suggerisce di valorizzare il ruolo degli attori non statali e della società civile.

KEYWORDS: violenza digitale – diritti umani – cybercriminalità – Consiglio d'Europa – prevenzione

LA DIMENSIÓN DIGITAL DE LA VIOLENCIA CONTRA LAS MUJERES ENTRE LOS DERECHOS HUMANOS Y LA CIBERDELINCUENCIA

El presente trabajo parte del supuesto según el cual el Convenio de Estambul sobre prevención y lucha contra la violencia contra las mujeres y la violencia

[54] Un esempio di azioni orientate allo scopo è l'itinerario che si realizza da alcuni anni nell'Università degli Studi di Salerno, meglio conosciuto come *Roadmap* UniSa, di cui alcuni risultati sono illustrati nel volume che raccoglie gli atti del Convegno internazionale di studi tenuto in occasione della giornata internazionale della donna 2023: A. DI STASI (a cura di), *Dalla non discriminazione alle pari opportunità: un itinerario di confronto, ricerca e sperimentazione di buone prassi a UNISA...e oltre*, Milano, 2024.

doméstica y el Convenio de Budapest y su Segundo Protocolo adicional sobre la ciberdelincuencia, relativo à la cooperación reforzada y la divulgación de pruebas electrónicas abordan de manera indirecta y parcialmente la dimensión digital de la violencia contra las mujeres y deben ser aplicados de manera integrada por los Estados. Habiendo identificado los límites de la protección represiva por actos de cibercrimen contra las mujeres, también à la luz de la jurisprudencia del TEDH, el trabajo cuestiona la oportunidad para los Estados miembros de invertir en el paradigma preventivo y de protección à la luz del art. 5, párr. 2 del Convenio de Estambul, tal como lo sugiere GREVIO en la recomendación núm. 1. Desde esta perspectiva, considerando los desarrollos y desafíos de la inteligencia artificial, se sugiere mejorar el papel de los actores no estatales y de la sociedad civil.

PALABRAS CLAVE: violencia digital – derechos humanos – ciberdelincuencia – Consejo de Europa – prevención

DIMENSIONE CIBERNETICA DELLA VIOLENZA E DELLE MOLESTIE DI GENERE IN AMBITO LAVORATIVO: IL CONTESTO INTERNAZIONALE ED EUROPEO

*Claudia Morini**

"'Work' is no longer a well-defined activity with sharp boundaries in terms of time, location and tools. All three have blurred boundaries, which serve to modify the understanding that employees and employers have of civility, bullying and the limits of their corresponding rights and obligations"

(B. WEST, ET AL., *Cyberbullying at Work: in Search of Effective Guidance*, in *Laws*, 2014, Vol. 3, p. 599).

1. *Considerazioni introduttive*

La crescente digitalizzazione delle attività umane – che ha subito un'accelerazione senza precedenti anche a seguito della pandemia da

* Professoressa associata di Diritto dell'Unione europea, Università del Salento. Coordinatrice del Modulo Jean Monnet "EUPROWOMEN – Protection and Promotion of Women's Rights in the European Legal Order: from Gender Equality to Active Participation in the Democratic Life of the European Union" (2022-2025). Email: claudia.morini@unisalento.it.

Covid-19 – ha portato a trasformazioni significative nel mondo del lavoro, ma ha al contempo facilitato l'affermarsi di nuove dimensioni di vulnerabilità, tra cui la violenza e le molestie di genere perpetrate attraverso strumenti tecnologici[1]. La dimensione cibernetica della violenza e delle molestie di genere anche in ambito lavorativo è, infatti, un fenomeno sempre più rilevante, che si concretizza per mezzo delle nuove tecnologie, strumenti il cui *misuse* veicola e facilita abusi, discriminazioni e molestie contro donne e, più in generale, contro i soggetti più vulnerabili delle nostre società. Questo deprecabile fenomeno, noto anche come violenza di genere c.d. *ICT-facilitated* (acronimo in inglese TFVAW), include comportamenti quali il *cyberstalking*, il *trolling*, le minacce online, la diffusione non consensuale di contenuti intimi (*revenge porn*), e altre forme di abuso digitale[2].

Sempre più spesso, invero, le lavoratrici in vari settori – media, politica, arti e cultura, amministrazione pubblica e accademia – si trovano a dover svolgere una consistente parte del loro lavoro online. In questo contesto, insulti, diffamazioni, minacce e discorsi d'odio sono abilitati e facilitati proprio dalle tecnologie digitali[3].

[1] Sulla particolare vulnerabilità delle donne, ci sia consentito rinviare a C. MORINI, *La vulnerabilità declinata al femminile: la risposta dell'ordinamento europeo*, in G. GIOFFREDI, V. LORUBBIO, A. PISANÒ (a cura di), *Diritti umani in crisi? Emergenze, disuguaglianze, esclusioni*, Pisa, 2021, pp. 177-190.

[2] Vedi C. MORINI, *Libertà di espressione e tutela della dignità delle giornaliste: il contrasto all'*online sexist hate speech *nello spazio digitale europeo*, in *Freedom, Security and Justice: European Legal Studies*, 2022, n. 3, pp. 67-104.

[3] Sebbene gli abusi contro le figure pubbliche preesistessero al dirompere delle tecnologie digitali, queste ultime, grazie spesso all'anonimato che possono garantire, li hanno resi più facili, frequenti e, spesso, più intensi, andando a colpire in modo sproporzionato le donne, le persone di colore e i membri della comunità LGBTIQ+. Vedi European Union Agency for Fundamental Rights, *Challenges to women's human rights in the EU. Gender discrimination, sexist hate speech and gender-based violence against women and girls*, 2017, disponibile su https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-challenges-to-women-human-rights_en.pdf; European Institute for Gender Equality, *Tackling cyber violence against women and girls: The role of digital platforms*, *Publications Office of the European Union*, Luxembourg, 2024, disponibile su https://op.europa.eu/en/publication-detail/-/publication/85ea273e-b6ac-11ef-91ed-01aa75ed71a1/language-en#:~:t ext=This%20brief%20by%20the%20European%20Institute%20for%20Gender,and%20practices%20to%20combat%20CVAWG.%20Download%20and%20languages.

Nel 2018, in un report sulla violenza contro le donne, la UN Special Rapporteur on violence against women ha elaborato un'importante definizione di violenza c.d. *ICT-facilitated*: "*The definition of online violence against women […] extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately*"[4].

Questa definizione è sufficientemente ampia da: a) enfatizzare la continuità della violenza di genere contro le donne sia online che offline; b) considerarla come una "nozione-quadro" alla quale si riferiscono diverse forme di violenza cibernetica.

La cyberviolenza nel contesto della violenza di genere è da intendersi come molestie online, incitamento online all'odio basato sul genere anche attraverso lo *stalking* online, le minacce online, la pubblicazione di informazioni o contenuti avente natura grafica intima senza consenso, l'accesso illegale a comunicazioni intercettate e ai dati privati e ogni altra forma di uso abusivo dell'informatica e delle comunicazioni da parte dell'interessato quali uso di computer, smartphone o altri dispositivi simili, che utilizzano le telecomunicazioni in grado di connettersi a Internet e di inviare e-mail o utilizzano piattaforme social, con l'obiettivo di sbugiardare, umiliare, spaventare, minacciare o mettere a tacere la vittima[5].

[4] Vedi Human Rights Council, Report of the Special Rapporteur on violence against women, its causes and consequences, MS. DUBRAVKA ŠIMONOVIĆ, *on online violence against women and girls from a human rights perspective*, A/HRC/38/47, 18 giugno 2018, par. 23.

[5] A livello internazionale sono però diversi gli organismi che hanno condiviso la loro definizione di forme di violenza c.d. "*technology-facilitated*": 1) "*includes a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs). Cyber violence can start online and continue offline, or start offline and continue online, and it can be perpetrated by a person known or unknown to the victim*" - European Institute for Gender Equality (EIGE), *Cyber Violence against Women and Girls. Key Terms and Concepts* (22 October 2022) 4 disponibile su https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf; 2) "*an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified*

Tali condotte, però, stanno iniziando a ricevere sempre maggiore attenzione da parte delle istituzioni internazionali, che hanno iniziato a richiamare gli Stati alla loro responsabilità di arginare e contrastare efficacemente questo fenomeno[6].

in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender" - United Nations Population Fund (UNFPA), https://www.unfpa.org/TFGBV ; 3) "*action by one or more people that harms others based on their sexual or gender identity, or by enforcing harmful gender norms. This action is carried out using the internet and/or mobile technology and includes stalking, bullying, sexual harassment, defamation, hate speech and exploitation*" - L. HINSON, J. MUELLER, L. O'BRIEN-MILNE, N. WANDERA, *Technology-facilitated gender-based violence: What is it, and how do we measure it?*, Washington D.C., International Center for Research on Women (ICRW), 2018. Infine, in un recente studio di UN Women, *Technology-facilitated violence against women: Report of the foundational meeting of the expert group*, marzo 2023, ritroviamo questa definizione: "*any act that is committed, assisted, aggravated or amplified by the use of ICTs or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms*". In essa, come emerge, non troviamo alcuna elencazione di fattispecie-tipo perché ciò, secondo gli esperti che vi hanno lavorato, garantirebbe una "resistenza al tempo" della stessa (c.d. *time-invariant definition*).

[6] Vedi Consiglio d'Europa, *Combating Sexist Hate Speech*, 2016 disponibile su https://rm.coe.int/1680651592, pp. 2 e 4; *Commissione europea, #DigitalRespect4Her Factssheet*, 2019, disponibile su https://digital-strategy.ec.europa.eu/en/library/digitalrespect4her-factsheet; Parlamento europeo, , *Bullying and sexual harassment at the workplace, in public spaces, and in political life in the EU. A study requested by the FEMM committee*, settembre 2018, disponibile su http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604949/IPOL_STU(2018)604949_EN.pdf; Parlamento europeo, *Cyber violence and hate speech online against women. Women's Rights & Gender Equality. A study for the FEMM committee*, marzo 2018, disponibile su http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf. Da ultimo, vedi il *Pact for the Future and Global Digital Compact and Declaration on Future Generation*, adottato in seno alle Nazioni Unite lo scorso 22 settembre 2024 in occasione del *Summit for the Future*, disponibile su https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf, p. 38. Nel testo della *Declaration*, all'*ACTION 31 - WE WILL ENSURE THAT SCIENCE, TECHNOLOGY AND INNOVATION IMPROVE GENDER EQUALITY AND THE LIVES OF ALL WOMEN AND* GIRLS, gli *stakeholders* hanno inserito tra le priorità quella di "*[a]ddress gender-related risks and challenges emerging from the* use of technologies*, including all forms of violence, including sexual and gender-based violence, trafficking in persons, harassment, bias and*

Ad esempio, nel 2018, in un'importante Risoluzione sulla *promotion, protection and enjoyment of human rights on the Internet*, lo *Human Rights Council* condannò inequivocabilmente "*online attacks against women, including sexual and gender-based violence and abuse of women, in particular where women journalists, media workers, public officials or others engaging in public debate are targeted for their expression", richiamando gli Stati affinchè adottassero "gender-sensitive responses that take into account the particular forms of online discrimination*" (par. 11)[7].

Messaggio simile è quello che troviamo in una Risoluzione dell'Assemblea generale del 2020, nella quale essa aveva chiesto a tutti gli Stati di prevenire, affrontare e proibire tutte le forme di violenza "*including sexual harassment, against women and girls* in public and political life, *including women in leadership positions, journalists and other media workers and human rights defenders, […] including in* digital contexts, *are promptly brought to justice and held accountable through impartial investigations*" (enfasi aggiunta)[8].

discrimination against all women and girls that occur through or are amplified by the use of technology*, including against* women migrant workers" (enfasi aggiunta, p. 22). Le donne migranti sono soggetti particolarmente vulnerabili, spesso vittime di discriminazione c.d. intersezionale. Sul punto ci sia consentito rinviare a C. MORINI, *Discriminazione intersezionale e contrasto ai reati generati dall'odio contro le donne migranti: tutele attuali e prospettive evolutive in senso all'Unione europea*, in A. DI STASI, R.CADIN, A. IERMANO, V. ZAMBRANO (a cura di), *Donne migranti e violenza di genere nel contesto giuridico internazionale ed europeo*, Napoli, 2023, pp. 663-690.

[7] Par. 11, Human Rights Council, *Resolution on The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/38/7, adottata il 5 luglio 2018 disponibile su https://digitallibrary.un.org/record/1639840/?v=pdf. La necessità di tutelare queste figure professionali da forme di violenza facilitate dalle nuove tecnologie è stata poi ribadita anche in una successiva risoluzione, adottata il 13 luglio 2021 (Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/47/16).

[8] Vedi, Assemblea generale, *Resolution on Intensification of efforts to prevent and eliminate all forms of violence against women and girls*, A/RES/75/161, adottata il 16 dicembre 2020, par. 16. In generale, per una panoramica sulle Nazioni Unite e "*technology-facilitated gender-based violence*" vedi tutti i riferimenti e i richiami contenuti nella pagina dedicata "How Technology-Facilitated Gender-Based Violence Impacts Women and Girls" disponibile su https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/.

Quanto alla dottrina che si è occupata del tema degli abusi di matrice cibernetica contro le donne attive in contesti professionali, ad oggi essa verte prevalentemente su categorie di lavoratrici specifiche, quali le giornaliste[9], le donne impegnate in politica o che agiscono in difesa dei diritti umani[10] o le accademiche[11].

Spesso la violenza cibernetica è utilizzata contro le donne in posizioni di potere, soprattutto se sono giovani o appartengono a una mi-

[9] Vedi M. FERRIER, N. GARUD-PATKAR, *TrollBusters: Fighting Online Harassment of Women Journalists*, in J.R. VICKERY, T. EVERBACH (eds.), *Mediating Misogyny*, London, 2018, pp. 311-332; UNESCO, J.R. HENRICHSEN, M. BETZ, AND J.M. LISOSKY, *Building digital safety for journalism: A survey of selected issues*, 2015: https://unesdoc.unesco.org/ark:/48223/pf0000232358; J. MIRANDA, M.J. SILVEIRINHA, S. SAMPAIO-DIAS, B. DIAS, B. GARCEZ ET AL., *"It comes with the job": How journalists navigate experiences and perceptions of gendered online harassment*, in *International Journal of Communication*, 2023, Vol. 17, pp. 5128-5148; J. POSETTI, *Fighting Back Against Prolific Online Harassment: Maria Ressa*, in UNESCO, L. KILMAN (ed.), *An Attack on One is an Attack on All*, 2017, pp. 37-40; R. REGO, *Changing Forms and Platforms of Misogyny: Sexual Harassment of Women Journalists on Twitter* in *Media Watch*, 9(3), 2018, pp. 472-485; UNESCO, J. POSETTI, N. SHABBIR, D. MAYNARD, K. BONTCHEVA, N. ABOULEZ, *The Chilling: Global Trends in Online Violence Against Women Journalists*, Paris, 2021, disponibile su https://unesdoc.unesco.org/ark:/48223/pf0000377223.

[10] Vedi Inter-Parliamentary Union, *Sexism, harassment and violence Against Women in Parliaments in Europe*, 2018, disponibile su https://www.ipu.org/resources/publications/issue-briefs/2018-10/sexism-harassment-and-violence-against-women-in-parliaments-in-europe; J. ERIKSON, S. HÅKANSSON, C. JOSEFSSON, *Three Dimensions of Gendered Online Abuse: Analysing Swedish MPs' Experiences of Social Media*, in *Perspectives on Politics*, 2023, Vol. 21, No. 3, pp. 896-912; R. LEWIS, M. ROWE, C. WIPER, *Online abuse of feminists as an emerging form of violence against women and girls* in *British journal of criminology,* vol. 57, Issue 6, 2017, pp. 1462-1481. Dal menzionato studio dell'Unione interparlamentare, condotto in 45 paesi europei, è emerso che oltre la metà delle parlamentari e del personale parlamentare intervistato (58%) aveva subito attacchi sessisti sui social media, tra cui insulti misogini ripetuti, incitamento all'odio, fotomontaggi nudi e video pornografici. Questa è stata la forma principale di violenza di genere sperimentata dalle intervistate, ma meno del 10% ha segnalato gli incidenti. La metà delle intervistate (47%) aveva ricevuto minacce di morte o di stupro. Nella maggior parte dei casi (76%), i colpevoli erano uomini anonimi.

[11] Vedi E. KAVANAGH, L. BROWN, *Towards a research agenda for examining online gender-based violence against women academics*, in *Journal of Further and Higher Education*, 44(10), 2019, pp. 1-9.

noranza etnica o sessuale, per delegittimare il loro potere e la loro influenza. L'impatto degli abusi online sulla vita professionale e personale delle donne può essere devastante, con molte donne colpite che scelgono, ad esempio, di ritirarsi da determinati social network nonostante la loro utilità in ambito professionale, di scrivere solo in modo anonimo, di evitare di diffondere il loro lavoro e di abbandonare del tutto una professione particolarmente "esposta" a questo tipo di violenza.

La correlazione tra permanenza di atteggiamenti discriminatori nei confronti delle donne e incremento di episodi di violenza e di molestie nei loro confronti resta un dato incontrovertibile a cui l'ordinamento internazionale sta cercando di dare risposte concrete, anche con riferimento all'ambito lavorativo.

Consapevoli della necessità di esplorare quelle che sono le possibili risposte giuridiche a questo fenomeno lesivo della dignità e della libertà delle donne, con il presente saggio esamineremo il *framework* internazionale ed europeo relativo al contrasto alla violenza e alle molestie di genere cibernetiche nel contesto lavorativo, analizzando la disciplina esistente, le sfide attuali e le possibili prospettive future per la loro prevenzione e contrasto.

2. *Molestie di genere e spazio cibernetico: l'azione delle istituzioni internazionali in riferimento all'ambito lavorativo*

Come è noto, tra i Sustainable Developments Goals (SDGs)[12], l'SDG 5 sull'uguaglianza di genere richiede alla comunità internazionale azioni mirate per eliminare tutte le forme di violenza contro le donne e le ragazze, incluse, pertanto, quelle facilitate dalle tecnologie dell'informazione e della comunicazione.

Allo stesso modo, l'SDG 8, esorta i governi a raggiungere un'occupazione piena e produttiva e un lavoro dignitoso per tutte le donne e gli uomini, anche attraverso la parità di retribuzione, e a garantire condizioni di lavoro sicure per ogni individuo.

Da una lettura integrata dei due obiettivi emerge, dunque, la necessità che la comunità internazionale si impegni a fare in modo che i

[12] Vedi https://sdgs.un.org/.

luoghi di lavoro siano luoghi "liberi" da ogni forma di molestia e violenza.

Se è vero che la violenza e le molestie contro le donne sono anche il risultato della persistente discriminazione di cui esse continuano ad essere vittime, è opportuno avviare le nostre riflessioni dal più importante strumento internazionale volto al contrasto della discriminazione contro le donne, ovvero la Convenzione per l'eliminazione di tutte le forme di discriminazione contro le donne (CEDAW) del 1979. Essa, invero, pur imponendo agli Stati di intraprendere misure volte ad eliminare "pregiudizi e stereotipi basati sulla convinzione dell'inferiorità o della superiorità dell'uno o dell'altro sesso", non prevedeva però esplicitamente norme specifiche volte a contrastare la violenza. A ciò si pose poi riparo con le Raccomandazioni generali nn. 12/1989 e 19/1992 sul contrasto alla violenza di genere e, in seguito, con la n. 35/2017 che ha anche incluso nella nozione di "violenza di genere" quella a carattere cibernetico. In essa, infatti, può leggersi che: "[*g*]*ender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private, including in the contexts of the family, the community, public spaces, the workplace, leisure, politics, sport, health services and educational settings, and the redefinition of public and private through* technology-mediated environments, *such as* contemporary forms of violence occurring online and in other digital environments" (par. 20, enfasi aggiunta)[13]. Qui, come emerge,

[13] Committe on the Elimination of Discrimination against Women, General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992), 26 luglio 2017, CEDAW/C/GC/35, disponibile su https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/231/54/PDF/N1723154.pdf?OpenElement. Tra le altre cose, si richiede agli Stati contraenti di "*[e]ncourage, through the use of incentives and corporate responsibility models and other mechanisms, the engagement of the private sector, including businesses and transnational corporations, in efforts to eradicate all forms of gender-based violence against women and in enhancing its responsibility for such violence in the scope of its action, which should entail protocols and procedures addressing all forms of gender-based violence that may occur in the* workplace or affect women workers, *including effective and accessible internal complaints procedures, the use of which should not exclude recourse to law enforcement authorities, and should also address* workplace *entitlements for victims/survivors*" (enfasi aggiunta). Su questa raccomandazione, in dottrina vedi, per tutti, S. DE VIDO, *The Prohibition of Violence against Women as Customary Interna-*

oltre al riconoscimento delle nuove tecnologie come "strumenti" per perpetrare molestie e violenza contro le donne, viene anche riconosciuto come i luoghi di lavoro possono prestarsi a essere degli spazi in cui tali eventi lesivi della dignità e dell'integrità psico-fisica delle donne possono verificarsi.

Alcuni mesi dopo, il Segretario generale dell'ONU, nel suo report su *Intensification of efforts to eliminate all forms of violence against women and girls*, ha avuto modo di rilevare come "*[t]he impact of* online and ICT-facilitated violence *extends into educational settings and the* workplace. *According to the results of a study released in 2022 […]*, online abuse of women in professional contexts *is widespread, with 51 per cent of women who experienced online abuse also reporting a serious impact on their* professional life *because of the abuse*" (enfasi aggiunta, par. 24)[14]. Questo passaggio sottolinea un aspetto fondamentale della violenza di genere facilitata dalle nuove tecnologie: il suo impatto concreto sul percorso educativo e professionale delle donne. Il dato in percentuale di donne che subiscono abusi online con conseguenze sulla loro vita lavorativa è particolarmente significativo, poiché dimostra che questa forma di violenza non si esaurisce nello spazio digitale, ma ha effetti reali e dannosi sulle opportunità di carriera, sul benessere psicologico e sulla partecipazione delle donne al mondo del lavoro. Questa evidenza supporta una lettura della dimensione cibernetica della violenza di genere non solo come un problema di sicurezza individuale, ma come una barriera strutturale alla piena uguaglianza di genere. Se le donne, a causa delle molestie digitali, si trovano costrette a ridurre la loro presenza in determinati ambienti professionali o accademici, il problema diventa sistemico e impatta la loro rappresentanza in settori chiave della società.

tional Law? Remarks on the General Recommendation No. 35 (CEDAW) in *Diritti umani e diritto internazionale*, 2018, vol. 12, pp. 379-396.

[14] Assemblea generale, *Report on Intensification of efforts to eliminate all forms of violence against women and girls*, A/77/302, del 18 agosto 2022l, disponibile su https://www.unwomen.org/sites/default/files/2022-10/A-77-302-SG-report-EVAWG-en.pdf. Il report si riferisce allo studio di B. HARRIS, D. WOODLOCK, *Women in the Spotlight: Women's Experiences with Online Abuse in Their Working Lives*, in *eSafety Commissioner Australia*, 2022, disponibile su https://www.esafety.gov.au/research/how-online-abuse-impacts-women-working-lives.

Più di recente, l'Assemblea generale ha adottato un'importante Risoluzione sull'intensificazione degli sforzi per prevenire ed eliminare tutte le forme di violenza contro donne e ragazze, in riferimento all'ambiente digitale, con la quale ha chiesto agli Stati, tra le altre cose, di prevenire, affrontare e proibire "*sexual and gender-based violence, including sexual harassment, against all women and girls, both offline and online, in the* world of work *and in public and political life, including women in leadership positions, journalists and other media workers, feminists and women human rights defenders […]*" (enfasi aggiunta)[15]. Un aspetto particolarmente rilevante di questo passaggio è l'attenzione dedicata a gruppi di donne particolarmente esposti agli abusi, come *leader* politiche, giornaliste, lavoratrici dei media, femministe e attiviste per la tutela dei diritti umani. Questa specificazione evidenzia una preoccupazione crescente per le forme di violenza mirate a silenziare e marginalizzare le donne impegnate nella sfera pubblica, riducendo la loro partecipazione attiva alla vita politica, sociale e lavorativa.

Sempre nel quadro delle Nazioni Unite, occorre ricordare che il 20 marzo 2023 la Commission on the Status of Women (CSW), al termine della sua 67ª sessione, aveva presentato le sue "*agreed conclusions*" dedicate proprio al tema "*Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls*"[16]. Qui, tra le altre cose, la Com-

[15] Vedi Assemblea generale, *Resolution on Intensification of efforts to prevent and eliminate all forms of violence against women and girls: the digital environment*, A/RES/79/152, 17 dicembre 2024, disponibile su https://docs.un.org/en/A/RES/79/152, lett. o). La Risoluzione, inoltre, ha richiesto l'adozione di misure per garantire un'identificazione proattiva e tempestiva, nonché una risposta adeguata ed efficace per prevenire minacce, molestie, violenze ed esecuzioni extragiudiziali, e per contrastare l'impunità, assicurando che i responsabili di violazioni e abusi – compresa la violenza sessuale e di genere e le minacce e anche nei contesti digitali – siano prontamente portati davanti alla giustizia e giudicati al termine di indagini imparziali.

[16] Vedi Commission on the Status of Women, *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls*, Sixty-seventh session, 6-17 marzo 2023, disponibile su https://docs.un.org/en/E/CN.6/2023/L.3. Queste forme di violenza, invero, impediscono loro di esercitare il diritto di partecipare alla vita pubblica su un piano di parità con gli uomini.

missione ha riconosciuto che "*violence against women and girls, including sexual harassment in private and public spaces, including in educational institutions and the* world of work, *as well as in* digital contexts, *impedes participation and decision-making in the context of innovation and technological change, and education in the digital age, and leads to a hostile environment*" (enfasi aggiunta). Inoltre, nei paragrafi successivi (53-56) la Commissione ha espresso preoccupazione per la continuità e l'interconnessione tra violenza, molestia e discriminazione contro donne e ragazze, sia online che offline, condannando l'aumento di atti violenti commessi o amplificati dall'uso della tecnologia. Inoltre, ha sottolineato l'impatto negativo che queste forme di violenza, comprese quelle di genere, hanno sulla salute psicologica, fisica, sociale, politica ed economica delle donne e delle ragazze, con effetti devastanti sulla loro vita e sui loro diritti, specialmente per quelle attive nella sfera pubblica, come politiche, giornaliste, atlete e attiviste di organizzazioni femminili[17].

In conclusione, dunque, emerge la piena consapevolezza delle istituzioni internazionali dell'esistenza dai documenti richiamati, della gravità del fenomeno della violenza e delle molestie di genere cibernetiche in ambito lavorativo, pratiche ormai estremamente diffuse e che necessitano di risposte specifiche ed efficaci al fine di tutelare la sicurezza, la dignità e il benessere delle lavoratrici[18].

3. *Il ruolo dell'International Labour Organization (ILO) e la sua Convenzione sull'eliminazione della violenza e delle molestie nel mondo del lavoro*

Nell'ampio panorama delle organizzazioni internazionali a vocazione universale, l'International Labour Organization (ILO) ha, negli

[17] Vedi anche il recente UN Women, *Position Paper - Placing Gender Equality at The Heart of the Global Digital Compact Taking Forward the Recommendations of the Sixty-Seventh Session of the Commission on the Status of Women*, 2024, disponibile su https://www.unwomen.org/sites/default/files/2024-03/placing-gender-equality-at-the-heart-of-the-global-digital-compact-en.pdf.

[18] Vedi B.A. GUTEK, *Sex and the Workplace*, San Francisco, 1985; C.E. O'CONNELL, K. KORABIK, *Sexual Harassment: The Relationship of Personal Vulnerability, Work Context, Perpetrator Status, and Type of Harassment to Outcomes*, in *Journal of Vocational Behavior*, 2000, pp. 299-329.

ultimi anni, rivestito un ruolo di primo piano in materia di contrasto alla violenza e molestie di genere nel mondo del lavoro, anche qualora tali condotte siano facilitate dalle nuove tecnologie[19].

Nel 2018 infatti, venne pubblicato uno studio fondamentale per inquadrare esattamente il tema di cui ci stiamo occupando: *The Threat of Physical and Psychosocial Violence and Harassment in Digitalized Work*[20]. In esso si evidenziava la necessità di una risposta giuridica più strutturata alle nuove forme di violenza e molestie nel lavoro c.d. digitalizzato. La legislazione all'epoca esistente, invero, avrebbe dovuto essere aggiornata per includere le specifiche problematiche legate alla digitalizzazione, garantendo soprattutto una protezione adeguata alla salute mentale e fisica di lavoratori e lavoratrici. La responsabilità dei datori di lavoro in questo ambito veniva identificata come fondamentale, richiedendo l'adozione di politiche efficaci per prevenire la violenza digitale, tutelando i diritti fondamentali e promuovendo ambienti di lavoro sicuri e rispettosi.

Ed è stato proprio in seno all'ILO che è stato adottato un importante strumento vincolante in materia: la Convenzione n. 190 del 2019 sulla violenza e le molestie nel mondo del lavoro. Entrata in vigore sul piano internazionale il 25 giugno 2021, si tratta del primo trattato internazionale in materia. L'Italia l'ha ratificata il 29 ottobre 2021[21]. Es-

[19] Vedi https://www.ilo.org/ e, in dottrina, C. RIEGELMAN LUBIN, A. WINSLOW, *Social Justice for Women the International Labor Organization and Women*, Duhram, 1990. Più in generale, vedi A. ZANOBETTI, *Diritto internazionale del lavoro. Norme universali, regionali e dell'Unione europea*, Milano, 2021.

[20] Vedi P. V. MOORE, *The Threat of Physical and Psychosocial Violence and Harassment in Digitalized Work*, *International Labour Office*, Geneva, 2018.

[21] Per l'Italia è entrata in vigore il 29 ottobre 2022. Il testo è reperibile al seguente *link*:
https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C190. In dottrina vedi, S. SCARPONI, *La Convenzione OIL 190/2019 su violenza e molestie nel lavoro e i riflessi sul diritto interno*, disponibile su: https://www.fondazioneforensebolognese.it/uploads/files/02%20-%201%20ottobre%20RGLScarponiConvenzione%20OIL.pdf. La Convenzione è accompagnata dalla Raccomandazione n. 206 sull'eliminazione della violenza e delle molestie nel mondo del lavoro; al 25 gennaio 2025 sono 46 gli Stati che l'hanno ratificata. Disponibile su https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-rome/documents/normativeinstrument/wcms_713418.pdf.

sa, sebbene rappresenti un *unicum* nel panorama normativo internazionale, ha comunque recepito istanze provenienti da altri strumenti internazionali. Si pensi, per tutti, alla CEDAW che, come ricordato, sebbene non si occupi – anche in ragione dell'epoca in cui fu adottata – specificamente di violenza digitale, al suo art. 11 fa però riferimento al diritto delle donne a lavorare in ambienti liberi da discriminazione e molestie: "1. Gli Stati Parti prendono ogni misura appropriata per eliminare la discriminazione contro le donne nel settore dell'occupazione, al fine di assicurare, sulla base della parità dell'uomo e della donna, gli stessi diritti, in particolare: […] f) il diritto alla tutela della salute ed alla sicurezza delle condizioni di lavoro […]". Un aspetto molto interessante di questa norma è che nel successivo par. 3, si chiedeva agli Stati contraenti di tener conto di possibili evoluzioni a livello di "conoscenze scientifiche e tecnologiche", al fine di "attualizzare" periodicamente le leggi di tutela relative alle questioni affrontate in materia di protezione delle lavoratrici, sottoponendole "conseguente revisione, abrogazione o ampliamento a seconda delle necessità". L'odierno impatto nel mondo del lavoro delle nuove tecnologie rientra, dunque, a pieno titolo, tra le evoluzioni menzionate nel testo. Inoltre, ricordiamo come già nella Raccomandazione generale n. 35 /2017 si riconoscevano le "*contemporary forms of violence occurring online and in other digital environments*".

Una lettura finalisticamente orientata di tali testi ci consente oggi di ritenere che la Convenzione ILO n. 190 si sia posta perfettamente in linea con la richiesta di nuovi standard di tutela già richiesti a livello di CEDAW in quanto, come vedremo qui di seguito, essa persegue l'obiettivo di garantire che tutte le lavoratrici, e dunque anche quelle che sono vittime di cyberviolenza, possano lavorare in un ambiente sicuro e rispettoso della loro dignità.

La Convenzione n. 190 è, appunto, il primo strumento giuridico internazionale a trattare in modo completo il problema della violenza e delle molestie sul posto di lavoro e a riconoscerle come violazione dei diritti umani. In virtù degli obblighi che da essa derivano, gli Stati contraenti sono tenuti a garantire che i datori di lavoro adottino misure adeguate a prevenire e gestire le diverse condotte che costituiscono un *vulnus* alla dignità, alla libertà e all'integrità fisica e psicologica delle lavoratrici (e dei lavoratori), anche attraverso politiche aziendali e

formazione specifica[22]. In particolare, in base all'art. 9, i datori di lavoro devono fare ricorso a misure adeguate e proporzionate per prevenire la violenza e le molestie nel mondo del lavoro, inclusi la violenza e le molestie di genere[23].

Quanto a queste particolari forme di violenza, occorre innanzitutto rilevare come la Convenzione presti un'attenzione particolare alle donne e all'impatto che molestie e violenza possono avere in relazione alla loro vita lavorativa. Nel Preambolo, infatti, si evidenzia come queste condotte possono impedire che gli individui, e in particolare le donne, entrino, rimangano e progrediscano nel mercato del lavoro: sono, dunque, minacce concrete al raggiungimento delle pari opportunità e dell'*empowerment* femminile[24].

Quanto all'ambito di applicazione *ratione personae*, i soggetti che possono beneficiare della protezione derivante dalla sua attuazione a livello statale, includono le lavoratrici, i lavoratori – a prescindere da quale sia il loro *status* contrattuale – e le altre persone che a vario titolo

[22] In generale, la Convenzione è esplicita nel riconosce che lavoratori e lavoratrici hanno il diritto a un ambiente di lavoro sicuro e sano, libero dunque da violenza e molestie. Vedi J. BEQIRAJ, *Convention Concerning the Elimination of Violence and Harassment in the World of Work*, in *International Legal Materials*, vol. 58, n. 6, 2019, pp. 1167-1176.; N. SHARMA, B. SHARMA, P. PANT, *Sexual Harassment at Workplace vis-à-vis Recent Developments of International Labour Organization*, in *International Journal of Law and Politics Studies*, vol. 2, n. 1, 2020, pp. 15-20.

[23] La Convenzione, poi, in modo lungimirante mette in relazione la violenza domestica di cui la lavoratrice può essere vittima in ambito familiare/relazionale, con le ripercussioni che ciò può avere anche sulla sua occupazione, sulla sua produttività e sulla sua salute e sicurezza: di conseguenza, tale strumento esorta i governi, le organizzazioni dei datori di lavoro e i sindacati, e le istituzioni del mercato del lavoro ad agire in modo coordinato e integrato "al fine di identificare, reagire e intervenire sulle conseguenze della violenza domestica".

[24] Inoltre, sempre nel testo del Preambolo si rileva come questi fenomeni siano incompatibili con lo sviluppo di imprese sostenibili e abbiano un impatto negativo sull'organizzazione del lavoro, sui rapporti nei luoghi di lavoro e sulla piena partecipazione a tutte le attività da parte delle lavoratrici. Ancora, dopo aver ribadito che molestie e violenza di genere colpiscono sproporzionatamente donne e ragazze, la Convenzione richiama la necessità di adottare un "approccio inclusivo, integrato e in una prospettiva di genere, che intervenga sulle cause all'origine e sui fattori di rischio, ivi compresi stereotipi di genere, forme di discriminazione multiple e interconnesse e squilibri nei rapporti di potere dovuti al genere".

gravitano nel "mondo del lavoro", come, ad esempio, coloro che seguono un corso di formazione, lavoratrici e lavoratori licenziati, volontari e persone in cerca di un impiego o candidate a una posizione lavorativa[25].

Tutta la disciplina convenzionale è articolata su tre pilastri principali: protezione e prevenzione, verifica dell'applicazione e meccanismi di ricorso e di risarcimento, e orientamento, formazione e sensibilizzazione[26].

Le misure di orientamento, formazione e sensibilizzazione sono cruciali per prevenire ed eliminare la violenza e le molestie sul lavoro. A questo proposito, la Raccomandazione n. 206 fornisce linee guida per sviluppare programmi informativi e formativi che affrontino le cause alla base di questi fenomeni, come la discriminazione, l'abuso di potere e le norme culturali e sociali[27].

[25] La tutela prevista dalla Convenzione si estende poi anche agli individui che esercitano l'autorità, i doveri e le responsabilità di datrice o datore di lavoro (art. 2, par. 1). Infine, qualora ciò possa rilevare, la Convenzione richiede agli Stati di tenere in considerazione la violenza e le molestie che possono coinvolgere soggetti terzi (art. 4, par. 2).

[26] Per quanto riguarda la protezione e la prevenzione, ogni Stato è chiamato a rispettare e promuovere i diritti fondamentali nel mondo del lavoro, adottando leggi e regolamenti che obblighino i datori di lavoro ad adottare misure adeguate di prevenzione, includendo la violenza e le molestie di genere. La definizione, l'attuazione e il monitoraggio di tali misure devono coinvolgere attivamente i lavoratori e le lavoratrici, così come i loro rappresentanti. Gli Stati devono garantire l'esistenza di meccanismi adeguati e funzionali per i ricorsi e il risarcimento, comprendenti procedimenti di denuncia e risoluzione delle controversie sul posto di lavoro. Questo include anche l'accesso a tribunali o giurisdizioni competenti, protezione contro le ritorsioni nei confronti delle vittime, testimoni e informatori, nonché un adeguato supporto legale, medico e sociale. Inoltre, è fondamentale che venga riconosciuto il diritto delle vittime di abbandonare il posto di lavoro in caso di grave pericolo per la loro salute e sicurezza, e che siano previsti risarcimenti per i danni subiti.

[27] Vedi Organizzazione internazionale del Lavoro, *Raccomandazione 206 sull'eliminazione della violenza e delle molestie nel mondo del lavoro*, 21 giugno 2019, disponibile su https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40europe/%40ro-geneva/%40ilo-rome/documents/normativeinstrument/wcms_713418.pdf. Tali programmi devono rivolgersi sia ai lavoratori che ai datori di lavoro, nonché agli operatori pubblici come giudici, ispettori del lavoro e forze dell'ordine. La Convenzione promuove anche lo sviluppo di codici di condotta e strumenti per la va-

4. Segue. *L'applicabilità della Convenzione alla violenza e alle molestie di genere facilitate dalle nuove tecnologie*

Identificati gli aspetti principali e a carattere generale della Convenzione, veniamo ora a definire l'ambito di applicazione materiale, con particolare riguardo al tema di cui ci stiamo occupando. All'art. 1 si fornisce una definizione molto ampia di "violenza e molestie nel contesto lavorativo". In particolare, violenza e molestie sono definite come *qualsiasi comportamento, atto o minaccia che crei un ambiente di lavoro ostile, degradante, intimidatorio, umiliante o offensivo*: questi comportamenti possono essere tenuti da datori di lavoro, colleghi, clienti, fornitori o altre terze parti capaci di esercitare un'influenza sulla vittima.

La violenza di genere è poi menzionata esplicitamente, dal momento che si riconosce che le donne sono particolarmente vulnerabili a certe forme di violenza, comprese le molestie sessuali e la violenza psicologica.

Volgendo la nostra attenzione alla violenza cibernetica, l'assetto definitorio sopra richiamato può a nostro avviso produrre i suoi effetti anche in relazione al mondo digitale. Quest'ultimo, invero, è assimilabile a un "luogo lavorativo" in cui una donna può subire molestie. L'art. 3 lett. d) della Convenzione, infatti, afferma che essa trova applicazione con riferimento "alla violenza e alle molestie nel mondo del lavoro che si verifichino in occasione di lavoro, in connessione con il lavoro o che scaturiscano dal lavoro: "d) a seguito di comunicazioni di lavoro, incluse quelle rese possibili dalle *tecnologie dell'informazione e della comunicazione*" (enfasi aggiunta)[28].

Appare evidente, dunque, che potrebbero essere portate a termine una serie di condotte abusive agilmente riferibili a ciò che, ai sensi del-

lutazione dei rischi legati alla violenza sul posto di lavoro, e la realizzazione di campagne di sensibilizzazione pubblica per diffondere il messaggio di "tolleranza zero" verso la violenza e le molestie, affrontando atteggiamenti discriminatori e prevenendo la stigmatizzazione di vittime, testimoni e informatori.

[28] A sostegno di questa interpretazione vedi, anche, V. DE STEFANO, I. DURRI, C. STYLOGIANNIS, M. WOUTERS, *"System needs update": Upgrading protection against cyberbullying and ICT-enabled violence and harassment in the world of work*, in *ILO Working Paper*, n. 1, 2020, ILO, Geneva.

la Convenzione, può accadere "in occasione di lavoro, in connessione con il lavoro o che scaturiscano dal lavoro". Le violenze e le molestie digitali in ambito lavorativo potrebbero assumere la forma di molestie online – sessuali e non – *stalking* digitale, cyberbullismo e minacce o violenze psicologiche.

Quanto alla prima tipologia di condotta, essa potrebbe concretizzarsi in messaggi inappropriati, immagini o contenuti sessuali inviati tramite e-mail, messaggi privati, o piattaforme di videoconferenza come Zoom o Microsoft Teams.

Le molestie online, potrebbero invece concretizzarsi in un monitoraggio ossessivo delle attività online di una collega o la sorveglianza invasiva delle sue comunicazioni e dei suoi movimenti.

Lo *stalking* digitale, invece, ricalca comportamenti tipici dello *stalking* attuato nella "vita reale", ma utilizza strumenti digitali: offese, insulti o comportamenti denigratori vengono, infatti, veicolati tramite social media aziendali, chat di lavoro o e-mail.

Infine, quelle stesse tecnologie possono essere usate in modo distorto per minacciare o intimidire una lavoratrice, rendendo l'ambiente di lavoro ostile e psicologicamente dannoso. In proposito, l'attenzione della Convenzione n. 190 anche alla violenza psicologica è uno dei suoi tratti di modernità, visto che ormai è chiaramente riconosciuto che la violenza fisica e sessuale sono solo alcune delle forme di manifestazione di tale intollerabile fenomeno.

Quanto al pilastro relativo a "orientamento, formazione e sensibilizzazione", in virtù dell'art. 11, lett. b), i datori di lavoro, insieme ai lavoratori e alle rispettive organizzazioni, devono avere accesso a misure di orientamento, risorse, formazione o altri strumenti sui temi della violenza e delle molestie nel mondo del lavoro. Qui, il riferimento a "violenza e molestie" è ad ampio spettro e, alla luce degli scopi della Convenzione, è senza dubbio possibile includere quelle forme facilitate dal ricorso sempre più massiccio alle nuove tecnologie.

Accanto alla Convenzione n. 190, l'ILO come ricordato ha adottato la Raccomandazione n. 206, consistente in linee guida su come attuare efficacemente le diverse misure previste dalla Convenzione, alla luce delle specifiche situazioni lavorative e dei contesti locali.

Quanto alle specifiche implicazioni per il mondo digitale la Raccomandazione n. 206 suggerisce che, nella valutazione dei rischi del

digitale, sui luoghi di lavoro di cui all'art. 9 della Convenzione, si dovrebbe tenere conto dei fattori che aumentano la probabilità di violenza e molestie. A tal proposito, un'attenzione particolare "dovrebbe essere prestata ai pericoli e ai rischi che: a) siano conseguenza *delle condizioni e delle modalità di lavoro*, dell'organizzazione del lavoro e della gestione delle risorse umane, a seconda dei casi" (par. 8, enfasi aggiunta): in un contesto di crescente digitalizzazione del lavoro, saranno proprio peculiari modalità lavorative "informatizzate" a poter esporre maggiormente le donne a eventuali molestie online. Questo è particolarmente rilevante in quei contesti di lavoro che prevedono, ad esempio, comunicazioni virtuali regolari (attraverso e-mail aziendali, videoconferenze, o social media professionali come LinkedIn), o l'utilizzo di piattaforme per *meeting* ed eventi.

In un mondo del lavoro sempre più digitalizzato, dunque, la Convenzione n. 190 e la Raccomandazione n. 206 dell'ILO costituiscono fondamentali parametri normativi al fine di affrontare efficacemente il fenomeno della violenza e delle molestie di genere sul posto di lavoro, ivi comprese quelle di natura cibernetica.

5. *Il contrasto alla violenza di genere cibernetica nel contesto del Consiglio d'Europa e la sua applicabilità anche in ambito lavorativo*

Nel contesto europeo, l'azione sinergica del Consiglio d'Europa e dell'Unione europea – nei limiti delle rispettive competenze – sta contribuendo a disegnare il *framework* globale di contrasto alle molestie e alla violenza contro le donne facilitate dalle nuove tecnologie, anche in ambito lavorativo.

Muovendoci, innanzitutto, entro i confini ordinamentali del Consiglio d'Europa, occorre partire dall'analisi di un'importante presa di posizione da parte del Comitato dei Ministri rispetto alla matrice subculturale alla base di queste condotte criminose, ovvero il sessismo, anche nelle sue manifestazioni online. Essa risale al 2019, con l'adozione della Raccomandazione sulla prevenzione e la lotta al sessismo[29]. Dopo aver fornito una definizione condivisa di "sessismo", che

[29] Vedi Comitato dei Ministri, *Raccomandazione CM/Rec(2019)1 del Comitato dei*

include ogni atto, gesto, rappresentazione visiva, proposta orale o scritta, pratica o comportamento fondato sull'idea che una persona o un gruppo di persone siano inferiori per via del loro genere, e che si verifica nella sfera pubblica o privata, online oppure offline, la Raccomandazione si sofferma sulla previsione di specifiche misure da adottare per prevenire e lottare contro il sessismo.

Ai fini del nostro contributo, rilevano quelle contenute nella sezione II.B. (Internet, reti sociali e discorso d'odio sessista in rete) e nella II. D., dedicata alle azioni da intraprendere proprio nei luoghi di lavoro. Qui, invero, si evidenzia come sia nel settore pubblico che nel privato, le manifestazioni del sessismo possono assumere forme diverse, andando da–commenti e comportamenti sessisti nei confronti di una dipendente o di un gruppo di dipendenti, al fatto di zittire o ignorare le persone.

Una lettura combinata delle due sezioni offre un quadro chiaro dell'impegno che il Consiglio d'Europa chiede agli Stati per arginare il fenomeno degli attacchi online, in quanto "nuocciono non solo alla dignità delle donne, ma possono impedire loro, anche *nel contesto lavorativo*, di esprimere le proprie opinioni con la conseguenza di allontanarle dalla rete compromettendo il diritto alla libertà d'espressione e d'opinione in una società democratica, limitando le *opportunità professionali* e rafforzando il deficit democratico legato al genere" (enfasi aggiunta, sezione II.B.).

Se lo specifico tema della violenza contro le donne facilitata dalle nuove tecnologie è stato solo di recente affrontato in seno al Consiglio d'Europa, è da oltre un decennio, comunque, che questo sistema regionale volto alla promozione e protezione dei diritti umani si occupa del più ampio tema del contrasto alla violenza di genere e alla violenza domestica. La Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica (c.d. Convenzione di Istanbul) dal 2011 è, infatti, il più importante ed evoluto strumento normativo internazionale in questo ambi-

Ministri agli Stati membri sulla prevenzione e la lotta contro il sessismo, adottata il 27 marzo 2019, in occasione della 1342ª riunione dei Delegati dei Ministri, CM/Rec/2019), disponibile su https://rm.coe.int/cm-rec-2029-1-italian/16809e671b.

to[30]. Essa ha come obiettivo primario la prevenzione della violenza contro le donne, la protezione delle vittime e il perseguimento dei col-

[30] A livello globale, si tratta del terzo trattato regionale che affronta la violenza contro le donne ed è il più completo dopo la Convenzione interamericana sulla prevenzione, la punizione e l'eradicazione della violenza contro le donne (c.d. Convenzione di Belém) adottata dall'Assemblea generale dell'Organizzazione degli Stati Americani a Belém do Pará, Brasile, il 9 giugno 1994 ed entrata in vigore il 5 marzo 1995 e il Protocollo alla Carta africana dei diritti dell'uomo e dei popoli sui diritti delle donne in Africa (c.d. Protocollo di Maputo) adottato dall'Assemblea dell'Unione africana, l'11 luglio 2003 ed entrato in vigore il 25 novembre 2005. La Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, invece, è stata adottata dal Consiglio d'Europa il 7 aprile 2011 e aperta alla firma il successivo 11 maggio; essa è entrata in vigore il 1° agosto 2014. Si compone di un Preambolo, 81 articoli – suddivisi a loro volta in 12 capitoli – e un allegato relativo ai privilegi e alle immunità dei componenti del GREVIO, ovvero del "Gruppo di esperti sulla lotta contro la violenza nei confronti delle donne e la violenza domestica", meccanismo di controllo di cui all'art. 66 della Convenzione. Nel portale del Consiglio d'Europa è possibile accedere a una pagina dedicata alla Convenzione di Istanbul e alla sua attuazione attraverso il seguente link: https://www.coe.int/en/web/istanbul-convention/home?. In dottrina vedi, tra gli altri, M. CASTELLANETA, *Violenza contro le donne: pubblicata la legge di ratifica della Convenzione di Istanbul*, 11 luglio 2013, disponibile su www.marinacastellaneta.it; S. DE VIDO, *Donne, violenza e diritto internazionale. La Convenzione di Istanbul del Consiglio d'Europa del 2011*, Udine, 2016; A. DI STEFANO, *Violenza contro le donne e violenza domestica nella nuova Convenzione del Consiglio d'Europa*, in *Diritti umani e diritto internazionale*, 2012, n. 1, pp. 169-223; L. GAROFALO, *Alcune considerazioni sulle norme "self-executing" contenute nella Convenzione di Istanbul del 2011*, in *Ordine Internazionale e Diritti Umani*, 2018, n. 5, pp. 536-543; G. PASCALE, *L'entrata in vigore della Convenzione di Istanbul sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica*, in *Osservatorio costituzionale*, 2014, n. 3, pp. 1-12; F. POGGI, *Violenza di genere e Convenzione di Istanbul: un'analisi concettuale*, in *Diritti umani e diritto internazionale*, 2017, n. 1, pp. 51-76; A. VALENTINI, *Recenti sviluppi in seno al Consiglio d'Europa in tema di violenza contro le donne*, in *La Comunità internazionale*, 2012, n. 1, pp. 77-98. Sulla questione dell'adesione dell'Unione europea alla Convenzione vedi, S. DE VIDO, *The ratification of the Council of Europe Istanbul Convention by the EU: a step forward in the protection of women from violence in the European legal system*, in *European Journal of Legal Studies*, 2017, vol. 9, n. 2, pp. 69-102 e, ci sia consentito rinviare anche al nostro: *La questione dell'adesione dell'Unione europea alla Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica*, in *Freedom, Security and Justice: European Legal Studies*, 2021, n. 3, pp. 136-162.

pevoli, attraverso la creazione di un sistema legislativo favorevole all'eliminazione della violenza di genere. Sebbene non affronti esplicitamente la dimensione digitale, le sue disposizioni sono applicabili a tutti i contesti in cui si manifesta la violenza, compresi quelli online. Ciò è stato in seguito confermato dalla *General Recommendation No. 1 on the digital dimension of violence against women*, con la quale è stata introdotta la definizione "dimensione digitale della violenza sulle donne", che comprende sia gli atti di violenza perpetrati online – ad esempio condividere immagini umilianti, insulti, minacce di morte e di stupro – sia atti di violenza compiuti utilizzando tecnologie esistenti o non ancora inventate – come, ad esempio, tecnologie di tracciamento[31].

La sua applicazione, inoltre, riguarda una serie di aspetti che la rendono rilevante anche per il contesto del lavoro, tra cui, innanzitutto, la prevenzione della violenza, grazie all'inclusione di misure preventive nei luoghi di lavoro, che potrebbero comprendere politiche contro tutte le molestie, comprese quelle digitali. In materia di protezione delle vittime, la Convenzione prevede un sistema di supporto per tutte le vittime di violenza, comprese quindi quelle che subiscono molestie sul posto di lavoro e anche online. In relazione al perseguimento dei colpevoli, la Convenzione, infine, promuove l'adozione di leggi che puniscano la violenza e, anche in virtù della Raccomandazione generale n. 1, sono da intendersi incluse anche le violenze facilitate dalle tecnologie digitali.

Dunque, sebbene la Convenzione di Istanbul non si concentri esclusivamente sulla violenza subita dalle donne in ambito lavorativo, molti dei suoi principi e articoli, anche alla luce della Raccomandazione generale n. 1, si allineano oggi con quelli della Convenzione ILO n. 190. I due strumenti, pertanto, si completano vicendevolmente andando a promuovere attraverso gli obblighi che impongono agli Stati contraenti, la creazione di ambienti di lavoro sani, sicuri e inclusivi. Ciò, è tanto più vero, se si ha riguardo ad alcuni aspetti specifici che qui evidenzieremo.

[31] Vedi Consiglio d'Europa, GREVIO, *General Recommendation No 1 on the digital dimension of violence against women*, Strasbourg, 2021, disponibile su https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

Innanzitutto, la Convenzione di Istanbul fornisce una definizione chiara e completa di violenza di genere, che include ogni tipo di violenza basata sul genere e che comporta danni fisici, sessuali, psicologici o economici. Questo concetto si allinea con la definizione di violenza e molestie contenuta nella Convenzione ILO n. 190, che include sia violenze fisiche che psicologiche, comprese quelle digitali, che spesso sono perpetrate in contesti di discriminazione di genere.

La Convenzione di Istanbul, inoltre, sottolinea l'importanza della prevenzione come strumento fondamentale per combattere la violenza di genere. Questo principio è fatto proprio anche dalla Convenzione ILO n. 190 che, come abbiamo visto, richiede agli Stati membri e ai datori di lavoro di adottare politiche di prevenzione contro la violenza e le molestie nei luoghi di lavoro, comprese quelle digitali. La Convenzione di Istanbul stabilisce a sua volta che le politiche contro la violenza devono essere adottate in vari contesti, inclusi quelli lavorativi[32].

Sia la Convenzione di Istanbul che la Convenzione ILO n. 190 prevedono, infine, come cardine dell'azione preventiva l'importanza di attuare concrete misure di formazione e di sensibilizzazione. Nello specifico, la Convenzione ILO n. 190 richiede che i datori di lavoro promuovano una cultura di rispetto attraverso la formazione continua, che potrebbe includere anche la violenza digitale come parte del problema delle molestie di genere sul posto di lavoro. La Convenzione di Istanbul incoraggia a sua volta la formazione delle autorità, dei professionisti e delle comunità, che dovrebbe includere anche i settori professionali che trattano la violenza di genere in modo diretto, come i consulenti legali e sociali, i giudici e, appunto, i datori di lavoro.

In questo contesto, dunque, la Convenzione di Istanbul contribuisce a rafforzare la protezione contro la violenza di genere nel mondo del lavoro, anche digitale. La sua enfasi sulla prevenzione e la protezione delle vittime, unita alla necessità di adottare misure per contra-

[32] Ancora, la Convenzione di Istanbul prevede l'istituzione di servizi di supporto per le vittime, tra cui il sostegno psicologico, legale e materiale. Questi principi si estendono facilmente anche al contesto del lavoro, come descritto dalla Convenzione ILO n. 190, che richiede politiche di supporto e assistenza per le vittime di violenza sul luogo di lavoro.

stare tutte le forme di violenza sessuale, psicologica e fisica, è essenziale per comprendere come la violenza digitale possa essere trattata.

La Convenzione ILO n. 190, dal canto suo, applica tutti questi principi al mondo del lavoro, affinché vengano adottate politiche che proteggano le lavoratrici dalle molestie online, inclusi comportamenti abusivi su piattaforme professionali, attraverso e-mail, social media o altre forme di comunicazione online.

Le due convenzioni sono, dunque, sinergiche, con la Convenzione ILO n. 190 che fornisce una dimensione più specifica per il mondo del lavoro, concentrandosi sull'eliminazione delle molestie e della violenza di genere in contesti professionali, inclusi quelli digitali. I due strumenti, pertanto, si completano, offrendo un sistema normativo più ampio e integrato per proteggere le vittime di violenza di genere, comprese quelle che subiscono abusi digitali e per prevenire e contrastare la violenza nel mondo del lavoro, in ogni sua forma.

6. *L'impegno dell'Unione europea per contrastare il fenomeno della violenza cibernetica e delle molestie nel mondo del lavoro, anche alla luce della direttiva 2024/1385*

Uno studio dell'European Institute for Gender Equality (EIGE), ha illustrato come il crescente problema della violenza di genere facilitata dalle tecnologie digitali sia diventato un nuovo "rischio professionale", in particolare per le donne che svolgono peculiari professioni. In esso, si esaminano due degli aspetti più rilevanti di questo fenomeno: gli abusi online contro le donne attive nel settore pubblico e i rischi affrontati dalle donne lavoratrici delle piattaforme[33].

Partendo dal presupposto che l'uso delle tecnologie digitali è diventato una parte integrante della vita professionale di donne e uomini in vari contesti lavorativi, non sorprende che alcune delle esperienze negative di cui possono essere vittime le donne sul posto di lavoro,

[33] Vedi European Institute for Gender Equality, G*ender Equality Index 2020: Digitalisation in the world of work*, 16 ottobre 2020, disponibile su https://eige.europa.eu/publications-resources/publications/gender-equality-index-2020-digitalisation-and-future-work.

come le molestie di diversa natura, inclusa quella sessuale, siano dunque, sempre più mediate dalle tecnologie digitali.

Nel più recente Gender Equality Index del 2024, invero, è stato rilevato che "*[w]omen are particularly exposed to sexual harassment, as well as to other forms of violence at work. Insecure contracts, new precarious forms of work (e.g. platform work), home-based work, digital surveillance and poor work-life balance are all considered risk factors for workplace violence*"[34].

Lo scorso 25 novembre 2024, infine, l'Agenzia europea per i dirit-

[34] Vedi European Institute for Gender Equality, *Gender Equality Index 2024. Sustaining Momentum on a Fragile Path*, 10 dicembre 2024, disponibile su https://eige.europa.eu/publications-resources/publications/gender-equality-index-2024-sustaining-momentum-fragile-path?token=P8NRbkzhiASb-1jQ2xmXoqvXCzbMPUk5tgdU_wV-ae4. Alcune riflessioni specifiche sono opportune in relazione alla posizione delle donne lavoratrici delle piattaforme digitali, che sono al centro di relazioni di potere che si svolgono tra "fornitori di servizi" e "acquirenti di servizi", mediati dalla tecnologia. Il senso di impunità e anonimato dato ai clienti delle piattaforme *on-demand* è un fattore che mette i lavoratori vulnerabili in una situazione precaria, compreso il rischio di pregiudizi, discriminazioni e abusi di genere. Sebbene manchi una quantità significativa di dati quantitativi sugli abusi e la violenza subiti dalle donne lavoratrici delle piattaforme, la ricerca ha messo in evidenza come le donne coinvolte nell'economia delle piattaforme siano particolarmente esposte al rischio di violenza da parte degli utenti. Questo è vero soprattutto per i ruoli in cui le lavoratrici interagiscono con gli utenti e i clienti in spazi chiusi senza terze parti presenti, come i servizi di *ride-hailing*, condivisione di case o servizi personali e domestici (vedi Overseas Development Institute, A. HUNT, E. SAMMAN, *Gender and the Gig Economy Critical Steps for Evidence-Based Policy*, gennaio 2019, disponibile su https://media.odi.org/documents/12586.pdf). Le donne che lavorano in questi settori sono frequentemente esposte al rischio di molestie sessuali e aggressioni, e gli abusi fisici e sessuali delle donne lavoratrici delle piattaforme sono spesso facilitati o abilitati da alcuni aspetti del design della piattaforma e dei termini di servizio. Ad esempio, premiare i lavoratori con i profili più dettagliati li incoraggia a condividere informazioni private significative, come il nome, la posizione, l'età e la fotografia, per essere utilizzate come criteri di selezione dagli utenti. Alcune piattaforme impediscono anche ai lavoratori di accedere a informazioni che potrebbero aiutarli a valutare la sicurezza di un incarico prima di accettarlo, una strategia basata su una "asimmetria informativa". Sebbene alcune piattaforme abbiano reagito alle preoccupazioni per la sicurezza delle lavoratrici offrendo possibilità di interazioni solo tra donne o attraverso un maggiore coinvolgimento delle lavoratrici delle piattaforme, questi sforzi non sono però ancora sufficienti.

ti fondamentali (FRA) ha pubblicato l'esito di una "Ricerca sull'incidenza della Violenza di Genere nell'UE", il cui capitolo IV è espressamente dedicato al tema "Sexual Harassment at Work". Alle donne intervistate è stato chiesto esplicitamente se fossero state vittime di molestie sessuali, includendo anche quelle "*technology-facilitated*". I dati si sono rivelati allarmanti[35].

Anche l'Agenzia europea per la sicurezza e la salute sul lavoro presta particolare attenzione al tema dell'impatto delle nuove tecnologie sul benessere dei lavoratori e delle lavoratrici. In particolare, in un recente rapporto su *Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025*, si è evidenziato come tra i maggiori fattori di rischio persistano proprio discriminazioni, violenze e molestie, in quanto *"facilitated by the rise in the use of ICT-ETs and social networking at work"*[36].

La promozione di ambienti di lavoro, inclusi oggi quelli digitali, liberi da molestie e violenza, con particolare attenzione alla tutela delle lavoratrici è, dunque, un obiettivo importante anche per l'Unione europea[37]. Esso, invero, è sancito dal Trattato sul funzionamento

[35] Nell'UE, infatti, il 30,8% delle donne ha subito molestie sessuali sul posto di lavoro nel corso della vita. Tra gli Stati membri, la percentuale di donne che hanno subito molestie sessuali sul posto di lavoro nella loro vita varia dal 55,4% in Svezia, al 53,7% in Finlandia, al 53,0% in Slovacchia è al 52,9%; in Italia ci si aggira intorno al 14%. Il paese con il tasso più basso è la Lettonia, con l'11%. I risultati relativi alle molestie sessuali sul posto di lavoro si riferiscono alle esperienze delle donne che erano impiegate o lavoratrici autonome al momento dell'indagine o che avevano lavorato in passato. Vedi European Union Agency for Fundamental Rights, European Institute for Gender Equality, Eurostat, *EU gender-based violence survey – Key results. Experiences of women in the EU-27, Publications Office of the European Union*, Luxembourg, 2024, disponibile su *https://fra.europa.eu/sites/default/files/fra_uploads/eu-gender_based_violence_survey_key_results.pdf*.

[36] Vedi N. STACEY, P. ELLWOOD, S. BRADBROOK, J. REYNOLDS, H. WILLIAMS, D. LYE, *Foresight on new and emerging occupational safety and health risks associated digitalisation by 2025 – Final report commissioned by the European Agency for Safety and Health at Work* (EU-OSHA), Luxembourg, 2018, disponibile su https://osha.europa.eu/sites/default/files/Foresight_new_OSH_risks_2025_report.pdf, p. 140.

[37] Vedi anche la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Quadro strategico dell'UE in materia di salute e sicurezza sul luogo di lavoro 2021-2027. Si-*

dell'Unione europea (artt. 151 e 153), dalla Carta dei diritti fondamentali dell'Unione europea (art. 31), oltre che dalla Carta sociale europea, rivista nel 1996 (art. 26)[38].

Dato che la violenza e le molestie sul lavoro possono avere un impatto negativo sulle condizioni di lavoro, in particolare sul mantenimento di un ambiente di lavoro sano, sull'uguaglianza e sulla non discriminazione delle lavoratrici, l'UE si è attivata per contribuire alla risposta globale a tale nuova sfida[39].

A livello di *soft law*, un ruolo importante è stato ed è svolto dal Parlamento europeo (PE). Di particolare rilevanza è una Risoluzione del 2021 sulla lotta alla violenza di genere e in particolare sulla violen-

curezza e salute sul lavoro in un mondo del lavoro in evoluzione, del 28 giugno 2021, COM(2021) 323 def. Sulla protezione della salute mentale dei lavoratori, con particolare riferimento al c.d. diritto alla disconnessione, vedi, di recente, A. ROSANÒ, *Promozione della salute mentale dei lavoratori nel diritto dell'Unione europea: considerazioni* de iure condito *e* de iure condendo, in *Papers di diritto europeo*, 2024, n. 1, disponibile su https://www.papersdidirittoeuropeo.eu/fascicolo-2024-n-1/.

[38] Vedi M. ROCCELLA, T. TREU, M. AIMO, D. IZZI (a cura di), *Diritto del lavoro dell'Unione europea*, Milano, 2023; C. PESCE, *Carta di Nizza e tutela dei lavoratori nell'Unione europea*, in *I post di AISDUE*, 2020, n. II, disponibile su https://www.aisdue.eu/wp-content/uploads/2020/12/Post-Celeste-Pesce-Focus-Carta.pdf. Vedi anche il Principio 10 del Pilastro europeo dei diritti sociali del 2017, in base al quale "a. I lavoratori hanno diritto a un elevato livello di tutela della salute e della sicurezza sul luogo di lavoro. b. I lavoratori hanno diritto a un ambiente di lavoro adeguato alle loro esigenze professionali e che consenta loro di prolungare la partecipazione al mercato del lavoro. c. I lavoratori hanno diritto alla protezione dei propri dati personali nell'ambito del rapporto di lavoro", disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017C1213(01). A livello di diritto derivato, la disciplina fondamentale in materia di salute e sicurezza dei lavoratori la troviamo nella direttiva 89/391/CEE del Consiglio*, concernente l'attuazione di misure volte a promuovere il miglioramento della sicurezza e della salute dei lavoratori durante il lavoro* (c.d. *Direttiva quadro*), del 12 giugno 1989, in GUUE L 183, del 29 giugno 1989, pp. 1-8.

[39] Nel 2007 le parti sociali europee hanno concluso, a norma dell'attuale art. 155 TFUE, un *Accordo quadro sulle molestie e sulla violenza sul luogo di lavoro* (COM(2007) 686 def.), risultato di una consultazione delle parti sociali europee organizzata dalla Commissione in merito alla violenza sul luogo di lavoro e ai suoi effetti sulla salute e la sicurezza sul lavoro (C(2004)5220). Tale accordo fornisce ai datori di lavoro, ai lavoratori e ai loro rappresentanti un quadro di azioni concrete per individuare, prevenire e gestire le situazioni di molestie e di violenza sul luogo di lavoro.

za online, nella quale ha evidenziato come, poiché i posti di lavoro richiedono e dipendono con sempre maggiore frequenza da soluzioni digitali, ci troviamo di fronte a un "rischio crescente per le donne di incontrare la v*iolenza di genere online nello svolgimento dell'attività lavorativa ed economica*;" (enfasi aggiunta, lett. J)[40].

Di particolare interesse è, pure, la Risoluzione sulla salute mentale nel lavoro digitale, adottata il 5 luglio 2022: essa è stata una risposta alle nuove sfide poste dal lavoro digitale, particolarmente in seguito agli effetti prodotti anche in ambito lavorativo dalla pandemia da Covid-19. Al fine di tutelare la salute mentale delle lavoratrici, il PE ha rammentato che le molestie online tendono ad avere un impatto sproporzionato sui gruppi più vulnerabili, ivi compreso appunto le lavoratrici, invitando al contempo "la Commissione e gli Stati membri a proporre misure obbligatorie mirate per invertire e affrontare questo problema crescente sul lavoro e proteggere le vittime con tutte le risorse necessarie" (par. 13)[41].

[40] Vedi Parlamento europeo, *Risoluzione recante raccomandazioni alla Commissione sulla lotta alla violenza di genere: violenza online*, del 14 dicembre 2021, in GUUE C 251 del 30 giugno 2022, (2020/2035(INL), p. 2 ss.: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52021IP0489. In relazione alle particolari categorie di lavoratrici di cui abbiamo detto in apertura di questo saggio, il Parlamento ha qui evidenziato come "la violenza di genere online stia diventando sempre più comune e riduca la partecipazione delle donne e delle persone LGBTIQ alla vita pubblica e al dibattito che, di conseguenza, erode la democrazia dell'Unione e i suoi principi e impedisce loro di esercitare pienamente i loro diritti e libertà fondamentali, in particolare la libertà di parola; si rammarica, inoltre, del fatto che la violenza di genere online porti anche alla censura; lamenta che tale "effetto museruola" sia stato mirato soprattutto nei confronti delle attiviste, comprese le donne e le ragazze femministe, le attiviste LGBTIQ+, le artiste, le donne nei settori in cui la forza lavoro è prevalentemente maschile, le giornaliste, le rappresentanti politiche, le difenditrici dei diritti umani e le blogger, al fine di scoraggiare la presenza delle donne nella vita pubblica, comprese la politica e le sfere decisionali; esprime preoccupazione per il fatto che l'effetto dissuasivo causato dalla violenza di genere online si ripercuote spesso sulla realtà offline e che la normalizzazione della violenza online nei confronti delle donne che partecipano al dibattito pubblico contribuisce attivamente all'insufficiente segnalazione di tali reati e limita in particolare il coinvolgimento delle giovani donne" (par. 34).

[41] Vedi Risoluzione del Parlamento europeo*, sulla salute mentale nel mondo del lavoro digitale*, del 5 luglio 2022, disponibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0279_IT.html.

Quanto alla necessità per gli Stati membri di adeguarsi agli standard internazionali emergenti nella materia di cui ci stiamo occupando, già nella Strategia dell'UE per l'Uguaglianza di genere (2020-2025) la Commissione europea, dopo aver identificato il contrasto la violenza di genere, inclusa quella online, come una priorità, aveva incoraggiato gli Stati membri a ratificare la Convenzione n. 190 al fine di affrontare le molestie e la violenza in ambito lavorativo[42]. Quest'azione di stimolo nei confronti dei paesi membri era dovuta alla circostanza per cui, non potendo l'Unione direttamente ratificare la Convenzione n. 190 ILO in quanto aperta ai soli Stati membri dell'Organizzazione, sin da subito si era percorsa la strada della promozione della sua ratifica da parte di tutti gli Stati UE[43].

L'interesse dell'Unione affinché tutti i suoi membri ratifichino la Convenzione è dovuto alla rilevanza di alcuni aspetti della Convenzione, così come integrata dalla Raccomandazione, per l'attuazione di alcuni settori disciplinati dal diritto dell'Unione europea. In particolare, il riferimento è all'art. 153, par. 1, lett. a) e i), e all'art. 157, par. 3 TFUE, in base ai quali l'Unione deve sostenere e completare l'azione degli Stati membri in materia di miglioramento dell'ambiente di lavoro per proteggere la sicurezza e la salute dei lavoratori, nonché in relazione alla parità tra uomini e donne per quanto riguarda le opportunità sul mercato del lavoro e il trattamento sul posto di lavoro, adottando misure che assicurino l'applicazione del principio di pari opportunità e parità di trattamento tra uomini e donne in materia di occupazione e impiego.

L'interesse, inoltre, emerge anche dalla portata di diversi atti di diritto derivato già adottati dall'Unione in materia[44].

[42] Vedi Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'UE sui diritti delle vittime (2020-2025)*, del 24 giugno 2020, COM(2020) 258 final.

[43] Vedi Commissione europea, *Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Violence and Harassment Convention, 2019 (No. 190) of the International Labour Organization*, del 22 gennaio 2020, COM(2020)24 final.

[44] Vedi la già menzionata direttiva quadro 89/391/CEE, *che stabilisce misure per migliorare la sicurezza e la salute dei lavoratori durante il lavoro, compreso il trattamento dei rischi psicosociali come le molestie e la violenza*; la direttiva 2006/54/CE del Par-

In proposito, nella loro Raccomandazione concernente il progetto di decisione del Consiglio che invitava gli Stati membri a ratificare la Convenzione n. 190, le Commissioni congiunte del Parlamento europeo per l'occupazione e gli affari sociali (EMPL) e per i diritti delle donne e l'uguaglianza di genere (FEMM) avevano rilevato come "[i]l maggiore utilizzo delle *tecnologie digitali online* nel *mondo del lavoro* ha inoltre esacerbato il rischio di violenza e molestie, in quanto queste forniscono una nuova piattaforma per il loro verificarsi. Se non vengono messe in atto le politiche giuste, è probabile che le *tecnologie digitali* creino le condizioni per l'emergere di comportamenti antisociali, tra cui la violenza fisica di terzi e il bullismo o le *molestie sul luogo di lavoro*. È pertanto importante che la convenzione risponda alla realtà secondo cui gli *atti di violenza e molestie non devono necessariamente verificarsi esclusivamente in un luogo di lavoro fisico tradizionale*. Le relatrici ritengono inoltre che l'UE debba fare di più per garantire la *protezione delle lavoratrici* e dei lavoratori e in tutti i contesti, compresi quelli *digitali* […]" (enfasi aggiunta)[45].

lamento europeo e del Consiglio*, riguardante l'attuazione del principio delle pari opportunità e della parità di trattamento fra uomini e donne in materia di occupazione e impiego (rifusione),* del 5 luglio 2006, in GUUE L 204 del 26 luglio 2006 p. 23; la direttiva 2000/78/CE*,* del Consiglio*, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro,* del 27 novembre 2000, in GU L 303 del 2 dicembre 2000, p. 16. Inoltre, alcuni aspetti della Convenzione e della Raccomandazione sono connessi ad ambiti disciplinati dal diritto dell'Unione nei settori della cooperazione giudiziaria e dei diritti delle vittime, della migrazione, dell'asilo e della libertà di circolazione, in cui il diritto derivato dell'Unione stabilisce il diritto delle vittime di reato e dei loro familiari a ricevere informazioni, assistenza e protezione adeguate, partecipare ai procedimenti penali e essere trattati in modo rispettoso e non discriminatorio (vedi direttiva 2012/29/UE del Parlamento europeo e del Consiglio, *che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI*, del 25 ottobre 2012, in GUUE L 315 del 14 novembre 2012, p. 57).

[45] Vedi Commissioni congiunte EMPL e FEMM, *Raccomandazione concernente il progetto di decisione del Consiglio che invita gli Stati membri a ratificare la Convenzione sulla violenza e sulle molestie*, *2019 (Convenzione 190) dell'Organizzazione internazionale del lavoro*, A9-0040/2024 del 16 febbraio 2024 disponibile su: https://www.europarl.europa.eu/doceo/document/A-9-2024-0040_IT.pdf.

Il 25 marzo 2024, il Consiglio ha, infine, accolto la proposta della Commissione, adottando la decisione con la quale ha, appunto, invitato gli Stati a procedere a ratifica[46].

Due mesi dopo l'adozione di tale decisione, ha finalmente visto la luce la tanto attesa direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica[47]. Si tratta di un atto che, inizialmente elaborato anche per ovviare ai ritardi nella ratifica da parte dell'Unione europea della Convenzione di Istanbul – avvenuta il 28 giugno 2023 – si è poi distinto per la particolare attenzione verso alcune condotte riferibili ad atti di violenza e molestie facilitati dalle nuove tecnologie: un passo avanti, dunque, rispetto alle disposizioni della stessa Convenzione del Consiglio d'Europa.

Ai fini del nostro contributo, rileva subito evidenziare come essa si qualifichi espressamente quale strumento dell'UE per sostenere gli "impegni internazionali assunti dagli Stati membri per combattere e prevenire la violenza contro le donne e la violenza domestica, in particolare […] la Convenzione dell'Organizzazione internazionale del lavoro sull'eliminazione della violenza e delle molestie nel mondo del lavoro, firmata a Ginevra il 21 giugno 2019" (par. 4). La direttiva, dunque, rappresenta un tassello del *framework* internazionale che ruota attorno alla Convenzione n. 190.

In riferimento alle molestie online, per le quali la direttiva stabilisce norme minime, si chiarisce come esse siano spesso dirette a colpire donne politiche, giornaliste e difensore dei diritti umani o altre donne conosciute, e possono anche verificarsi in contesti diversi, ad esempio

[46] Vedi decisione (UE) 2024/1018 del Consiglio*, che invita gli Stati membri a ratificare la Convenzione sulla violenza e sulle molestie, 2019 (Convenzione 190) dell'Organizzazione internazionale del lavoro*, del 25 marzo 2024. in GUUE L del 2 aprile 2024.

[47] Vedi direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio*, sulla lotta alla violenza contro le donne e alla violenza domestica*, del 14 maggio 2024*,* in *GUUE* L del 24 maggio 2024 disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32024L1385. Per un'accurata disamina della direttiva in oggetto si rinvia al capitolo di E. BERGAMINI e S. DE VIDO, *La cyberviolenza di genere nel rapporto fra la direttiva 2024/1385 e gli altri strumenti di diritto dell'Unione europea/La ciberviolencia de género en la relación entre la directiva 2024/1385 y otros instrumentos del derecho comunitario*, pubblicato in questo Volume a pp. 329-355.

nei campus universitari, nelle scuole e, appunto, sul luogo di lavoro (par. 24)[48]. Pertanto, l'ambito di applicazione delle norme attuative in materia di definizione dei reati che sono richieste a livello statale dovrà estendersi anche all'ambito lavorativo, al fine di dare piena attuazione alla direttiva in parola, coerentemente con la volontà del legislatore europeo.

Inoltre, anche tutte le misure previste dalla direttiva, sia di carattere preventivo (art. 34) che relative alla formazione e informazione del personale con funzioni di vigilanza sul luogo di lavoro e dei datori di lavoro (art. 36), come quelle fondamentali in materia di assistenza alle vittime (art. 25), devono estendersi anche agli effetti causati delle forme cibernetiche della violenza e delle molestie di genere.

Accanto a questa importante pietra miliare dell'impegno dell'UE per il contrasto alla violenza di genere, merita attenzione anche un più recente atto normativo con una vocazione specifica rispetto al tema dell'impatto della digitalizzazione nel mondo del lavoro, adottato alcuni mesi dopo la direttiva 2024/1385: si tratta della direttiva (UE) 2024/2831 relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali[49].

[48] Anche se non strettamente connesso allo specifico tema di cui ci stiamo occupando, ricordiamo che la direttiva, pur non avendo fornito una definizione unionale di "molestie sessuali sul lavoro", ha però previsto a carico degli Stati l'obbligo di adottare una serie di misure sia di tipo preventivo che di assistenza e tutela alle vittime di tali abusi. Inoltre, all'art. 45 è previsto che entro il 14 giugno 2032 la Commissione valuti "la necessità di ulteriori misure a livello dell'Unione per contrastare efficacemente le molestie e la violenza sessuali sul luogo di lavoro, tenendo conto delle convenzioni internazionali applicabili, del quadro giuridico dell'Unione sulla parità di trattamento tra uomini e donne in materia di occupazione e impiego e del quadro giuridico in materia di salute e sicurezza sul lavoro".

[49] Vedi direttiva (UE) 2024/2831 del Parlamento europeo e del Consiglio*, relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali*, del 23 ottobre 2024, in GUUE L dell'11 novembre 2024. In dottrina, vedi E. RAIMONDI, *Il lavoro nelle piattaforme digitali e il problema della qualificazione della fattispecie*, in *Labour & Law Issues*, 2019, pp. 57-94. In questo contributo riteniamo di non doverci soffermare sull'impatto in materia di molestie e violenza cibernetica del c.d. *Digital Services Act* (Regolamento (UE) 2022/2065*,* del Parlamento europeo e del Consiglio, *relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)*, del 19 ottobre 2022, in GUUE L 277 del 27 ottobre 2022), in quanto non strettamente attinente al nostro tema. Ci sia però concesso di

Il lavoro mediante piattaforme digitali, invero, implica lo svolgimento di un'attività da parte del prestatore tramite l'infrastruttura digitale delle piattaforme di lavoro digitali che forniscono un determinato servizio ai propri clienti. Tale tipologia di attività può essere svolta in relazione a una vasta gamma di ambiti e si caratterizza per un elevato livello di eterogeneità, sia con riferimento alle tipologie di piattaforme di lavoro digitali, sia ai settori interessati e alle attività svolte. Anche i profili di coloro che lavorano attraverso queste piattaforme sono molto variabili[50].

evidenziare come, per quanto concerne la "valutazione del rischio" da parte dei gestori delle piattaforme nell'art. 34 del regolamento, relativo alla valutazione del rischio, la violenza di genere rientra tra i "rischi sistemici" cui appunto bisogna prestare massima attenzione: "I fornitori di piattaforme, online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi individuano, analizzano e valutano con diligenza gli eventuali rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi. […] La valutazione del rischio deve essere specifica per i loro servizi e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità, e deve comprendere i seguenti rischi sistemici: […] d) qualsiasi effetto negativo, attuale o prevedibile, in relazione alla *violenza di genere*, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona". Il successivo art. 35, invece, rimarca la necessità che vengano adottate adeguate misure di attenuazione di tali rischi, anche attraverso la rapida rimozione dei contenuti oggetto della notifica o la disabilitazione dell'accesso agli stessi, in particolare anche in relazione all'incitamento illegale alla violenza online. In definitiva, sebbene il DSA non sia stato concepito specificamente per proteggere le lavoratrici dalla violenza o dalle molestie di genere online, esso contribuisce certamente a creare un ambiente digitale più sicuro per tutti gli utenti delle piattaforme, e quindi anche per loro. In dottrina vedi, tra gli altri, B. DUIVENVOORDE, *The Liability of Online Marketplaces under the Unfair Commercial Practices Directive, the E-commerce Directive and the Digital Services Act*, in *Journal of European Consumer and Market Law*, 2022, n. 2, pp. 43-52; G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021; G.M. RUOTOLO, *Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di bis in idem*, in *SIDIBlog*, 29.03.202; A. TURILLAZZI, F. CASOLARI, M. TADDEO, L. FLORIDI, *The Digital Services Act: an analysis of its ethical, legal, and social implications*, in *Legal, and Social Implications*, 12 gennaio 2022; F. ZORZI GIUSTINIANI, *L'Unione europea e regolamentazione del digitale: il Digital Services Package e il Codice di buone pratiche sulla disinformazione*, in *Nomos*, 2022, n. 2, pp. 1-5.

[50] Attraverso gli algoritmi, le piattaforme di lavoro digitali organizzano, in misura

Un aspetto da non sottovalutare è che si tratta di una tipologia lavorativa in rapida evoluzione e, pertanto, che non sempre rientra entro sistemi di protezione esistenti. In proposito, la direttiva evidenzia come coloro "che svolgono un lavoro mediante piattaforme digitali sono esposte, in particolare nel lavoro in loco mediante piattaforme digitali, a un *rischio di violenza e molestie*, senza disporre di un luogo di lavoro fisico in cui possano presentare denunce. Le molestie, incluse quelle sessuali, possono avere un impatto negativo sulla salute e sulla sicurezza dei lavoratori delle piattaforme digitali" (par. 51, enfasi aggiunta). Di conseguenza, si richiede agli Stati membri, al fine di garantire la sicurezza e la salute di questi lavoratori, anche per quanto riguarda il rischio di subire violenza e molestie, di adottare "misure preventive, compresi canali di segnalazione efficaci" (art. 12, par. 5)[51].

7. *Considerazioni conclusive*

In conclusione, l'approfondimento del quadro giuridico internazionale ed europeo in materia di violenza e molestie di genere nel mondo del lavoro, con particolare attenzione alla dimensione cibernetica, ha evidenziato l'importanza di un impegno globale e coordinato per tutelare i diritti delle lavoratrici. Strumenti giuridici come la Convenzione ILO n. 190 e la direttiva 2024/1385 dell'UE, sono fondamentali per richiamare gli Stati alle loro responsabilità in materia di contrasto alla violenza e alle molestie di genere, inclusi gli abusi cibernetici anche nei luoghi di lavoro.

Tuttavia, affinché questi strumenti giuridici abbiano un impatto concreto, è necessario che la loro attuazione a livello statale sia accom-

minore o maggiore a seconda del loro modello di *business*, l'esecuzione del lavoro, la retribuzione per il lavoro svolto e il rapporto tra i clienti e le persone che svolgono il lavoro. Il lavoro mediante piattaforme digitali può essere svolto esclusivamente online con strumenti elettronici o secondo modalità ibride che combinano un processo di comunicazione online con una successiva attività da portare a termine nel mondo fisico. Molte delle piattaforme di lavoro digitali ad oggi esistenti sono multinazionali che svolgono attività e sviluppano modelli di *business* in diversi Stati membri o a livello transfrontaliero.

[51] Il termine di attuazione di tale direttiva è stato fissato al 2 dicembre 2026.

pagnata da una trasformazione culturale e organizzativa, che favorisca ambienti lavorativi rispettosi e sicuri, soprattutto per le donne.

Un aspetto cruciale di questa trasformazione potrebbe riguardare il coinvolgimento delle donne nelle STEM (*Science, Technology, Engineering, Mathematics*): aumentare la partecipazione femminile in questi settori, storicamente dominati dagli uomini, non solo contribuirebbe a ridurre le disuguaglianze di genere, ma avrebbe anche un impatto positivo nella lotta contro le molestie cibernetiche e la violenza nel mondo del lavoro[52].

Oltre a ciò, a nostro avviso in questo settore il coinvolgimento attivo degli attori non statali è poi cruciale. I datori di lavoro svolgono, infatti, un ruolo fondamentale nella prevenzione e gestione della violenza di genere cibernetica, in quanto sono responsabili della creazione di ambienti di lavoro sicuri, sia fisici che digitali. L'adozione di politiche aziendali proattive, che includano linee guida chiare contro le molestie cibernetiche, è essenziale per garantire che le lavoratrici possano operare in un contesto privo di abusi. Le aziende, inoltre, devono investire in formazione continua, sensibilizzando le dipendenti su come riconoscere e contrastare le molestie online, e creando canali sicuri per le segnalazioni.

Ancora, anche i sindacati possono svolgere un ruolo rilevante, agendo come mediatori tra le lavoratrici e le aziende, promuovendo politiche di contrasto alla violenza cibernetica e supportando le lavoratrici nel denunciare comportamenti abusivi. Inoltre, possono contribuire a sensibilizzare l'opinione pubblica e ad organizzare campagne educative sul tema della cyberviolenza di genere, incrementando la

[52] Il maggior coinvolgimento delle donne nelle STEM potrebbe svolgere un ruolo centrale in diversi modi: in primo luogo, le donne, portando esperienze e prospettive diverse, possono essere protagoniste di una progettazione tecnologica più inclusiva e rispettosa, sviluppando soluzioni per prevenire e contrastare fenomeni di cyberbullismo e molestie online. In secondo luogo, la presenza femminile nelle STEM può contribuire a una cultura del lavoro più equilibrata e più attenta al benessere psicologico e fisico di lavoratrici e lavoratori. Le donne, spesso maggiormente sensibili alle dinamiche di violenza e discriminazione, possono fungere da catalizzatrici di cambiamenti culturali all'interno delle organizzazioni, promuovendo un approccio di inclusività e rispetto che si riflette anche nelle politiche aziendali contro le molestie cibernetiche.

consapevolezza riguardo ai rischi legati alle nuove tecnologie e promuovendo l'adozione di misure di protezione adeguate.

Infine, il coinvolgimento delle aziende tecnologiche è altrettanto determinante. Queste aziende sono spesso alla base della creazione delle piattaforme che facilitano le interazioni tra i lavoratori, e pertanto hanno una responsabilità diretta nella protezione dei dati personali e nella prevenzione degli abusi online. Le aziende tecnologiche devono impegnarsi non solo nella progettazione di sistemi che garantiscano la sicurezza, ma anche nello sviluppo di strumenti di monitoraggio per individuare rapidamente episodi di violenza cibernetica di genere. Inoltre, esse devono collaborare con i legislatori e con le organizzazioni che tutelano i diritti delle lavoratrici per garantire che le normative siano adeguate e siano adeguate ed efficacemente applicate.

In definitiva, dunque, sebbene un appropriato ed aggiornato quadro normativo internazionale sia un punto di partenza essenziale per contrastare il fenomeno della violenza e delle molestie di genere facilitate dalle nuove tecnologie, è fondamentale che in modo capillare datori di lavoro, sindacati, aziende tecnologiche e altre realtà, statali e non, si impegnino in un'azione congiunta per garantire la protezione delle lavoratrici dalla violenza e dalle molestie cibernetiche, in un ambiente di lavoro – fisico e digitale – sempre più sicuro, inclusivo e rispettoso delle diversità e dei diritti fondamentali.

Abstract

Il saggio analizza il fenomeno delle molestie di genere nello spazio cibernetico, con particolare attenzione al contesto lavorativo e all'azione delle istituzioni internazionali. Dopo un'introduzione sul tema, si esamina il ruolo dell'International Labour Organization (ILO) e l'applicabilità della sua Convenzione n. 190 alla violenza e alle molestie facilitate dalle nuove tecnologie. Successivamente, si approfondisce l'approccio del Consiglio d'Europa, evidenziandone le implicazioni per la tutela delle vittime nel mondo del lavoro. Un'attenzione specifica è dedicata, infine, all'Unione europea e alle misure recentemente adottate, in particolare alla direttiva 2024/1385, che rafforza la protezione contro la violenza cibernetica di genere.

PAROLE CHIVE: violenza cibernetica – ambito lavorativo – OIL – Unione europea – sessismo

DIMENSIÓN CIBERNÉTICA DE LA VIOLENCIA DE GÉNERO Y DEL ACOSO EN EL LUGAR DE TRABAJO: EL CONTEXTO INTERNACIONAL Y EUROPEO

El ensayo analiza el fenómeno del acoso por razón de sexo en el ciberespacio, con especial atención al contexto laboral y a la acción de las instituciones supranacionales. Después de una introducción sobre el tema, se examina el papel de la Organización Internacional del Trabajo (OIT) y la aplicabilidad de su Convenio núm. 190 a la violencia y el acoso facilitados por las nuevas tecnologías. Posteriormente, se profundiza en el enfoque del Consejo de Europa, destacando sus implicaciones para la protección de las víctimas en el mundo del trabajo. Por último, se presta especial atención a la Unión Europea y a las medidas recientemente adoptadas, en particular la Directiva 2024/1385, que refuerza la protección contra la ciberviolencia de género.

PALABRAS CLAVE: violencia cibernética – lugar de trabajo – OIT – Unión Europea – sexismo

PARTE II

LA DIRETTIVA UE 2024/1385 E LA SUA TRASPOSIZIONE NELL'ORDINAMENTO ITALIANO E SPAGNOLO

LA DIRECTIVA UE 2024/1385 Y SU TRANSPOSICIÓN EN EL ORDENAMIENTO ITALIANO Y ESPAÑOL

LA CYBERVIOLENZA DI GENERE NEL RAPPORTO FRA LA DIRETTIVA 2024/1385 E GLI ALTRI STRUMENTI DI DIRITTO DELL'UNIONE EUROPEA

Elisabetta Bergamini[*] *– Sara De Vido*[**]

1. *La cyberviolenza di genere nella direttiva 2024/1385: introduzione e obiettivi della ricerca*

Sono ormai già alcuni anni che l'Unione europea ha deciso di intervenire in maniera sempre più concreta nei confronti della violenza di genere nei confronti delle donne e della violenza domestica, tenendo conto non solo degli strumenti già esistenti a livello internazionale – come dimostrato dall'adesione alla Convenzione di Istanbul dell'11 maggio 2011[1] avvenuta il 1° giugno 2023 – ma anche utilizzando stru-

[*] Professoressa ordinaria di Diritto dell'Unione europea, Università di Udine. Email: elisabetta.bergamini@uniud.it. È autrice dei parr. 2, 4 e 7. Introduzione e conclusioni sono scritte congiuntamente.

[**] Professoressa ordinaria di Diritto internazionale, Università Ca' Foscari di Venezia. Email sara.devido@unive.it. È autrice dei parr. 3, 5, e 6.

[1] Sulla convenzione di Istanbul per approfondimenti relative al suo contenuto si rinvia a S. DE VIDO, M. FRULLI (a cura di), *Preventing and combating violence against women and domestic violence. A Commentary to the Istanbul Convention*, Cheltenham-Northampton, 2023. Sull'*iter* relativo alla sua firma e ratifica per parte dell'Unione

menti di diritto interno, il più recente e importante dei quali è la direttiva (UE) 2024/1385 (nel seguito anche direttiva VAW – *Violence against women*)[2].

L'obiettivo di questo contributo è affrontare le previsioni della direttiva VAW in materia di cyberviolenza di genere nei confronti delle donne, collocandole a confronto con gli altri strumenti esistenti e in corso di approvazione o modifica nell'ordinamento dell'Unione europea al fine di valutare se e come la direttiva si ponga in continuità e coordinamento con tali strumenti e se il lavoro congiunto fra gli stessi possa rappresentare un risultato soddisfacente per prevenire la cyberviolenza di genere e per proteggere le vittime[3].

europea si veda S. DE VIDO, *The ratification of the Council of Europe Istanbul Convention by the EU: A step forward in the protection of women from violence in the European legal system,* in *European Journal of Legal Studies, European University Institute,* 2017, n. 9, pp. 69-102; ID, *La violenza di genere contro le donne nel contesto della famiglia: sviluppi nell'Unione Europea alla luce della Convenzione di Istanbul*, in *Federalismi*, 27 dicembre 2017, pp. 7-13 e C. MORINI, *La questione dell'adesione dell'Unione europea alla Convenzione di Istanbul alla luce del parere 1/19 della Corte di giustizia dell'Unione europea*, in *Freedom, Security and Justice: European Legal Studies*, 2021, n. 3, pp. 145-157. La ratifica è avvenuta con decisione (UE) 2023/1075 del Consiglio, *relativa alla conclusione, a nome dell'Unione europea, della convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica per quanto riguarda le istituzioni e l'amministrazione pubblica dell'Unione*, dell'1 giugno 2023, in GUUE L 143 I/1 del 2 giugno 2023, pp. 1-3 e con decisione (UE) 2023/1076 del Consiglio, *relativa alla conclusione, a nome dell'Unione europea, della convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica per quanto riguarda la cooperazione giudiziaria in materia penale, l'asilo e il non respingimento*, dell'1 giugno 2023, in GUUE, L 143 I/4 del 2 giugno 2023, pp. 4-6. Sulle implicazioni giuridiche dell'adesione nel sistema dell'UE, S. DE VIDO, *EU law in light of the Istanbul Convention: legal implications after accession,* Luxembourg, Publications office of the EU, in corso di pubblicazione.

[2] Sulla proposta di direttiva, E. BERGAMINI, *Combating Violence against Women and Domestic Violence from the Istanbul Convention to the EU Framework: the Proposal for a EU Directive*, in *Freedom, Security and Justice: European Legal Studies*, 2023, n. 2, pp. 21-41.

[3] Per semplicità si userà nel testo il termine cyberviolenza di genere o violenza nel mondo digitale anche se riteniamo che il termine più corretto e completo sia quello usato da S. DE VIDO e L. SOSA ossia "*gender-based ICT-facilitated violence against women*" (v. S. DE VIDO, L. SOSA, *Criminalisation of gender-based violence against women*

Se è vero che la direttiva in esame qualifica per la prima volta come "eurocrimini" certe forme di violenza contro le donne sulla base dell'art. 83 par. 1 Trattato sul funzionamento dell'Unione europea (TFUE) e rafforza l'accesso alla giustizia per le vittime di tali crimini, garantendo alle donne adeguata protezione e supporto in base all'art. 82 par. 2 lett. c) TFUE, vale la pena ricordare come l'Unione europea abbia già da tempo cercato di creare un coordinamento fra le normative nazionali in settori che in qualche modo vanno ad intersecarsi con quello in oggetto, situazione che diviene ancora più rilevante in attesa dell'attuazione della direttiva VAW, che dovrà avvenire entro luglio 2027. Di rilievo nella direttiva VAW è altresì la prevenzione della violenza contro le donne, inclusa quella nel mondo digitale, che passa attraverso azioni di educazione (v. *digital literacy*) e di formazione.

La criminalizzazione e la prevenzione della cyberviolenza di genere, in particolare, sono tra gli aspetti più innovativi della direttiva, la cui rilevanza emerge anche dagli interventi della Corte europea dei diritti umani (Corte EDU), a partire dalla sentenza *Buturugă c. Romania,* nella quale lo Stato membro veniva condannato per non essere intervenuto al fine di prevenire, proteggere e punire atti di cyberviolenza contro le donne sulla base della violazione dell'art. 8 Convenzione europea dei diritti dell'uomo (CEDU)[4]. Nello specifico, questo contributo si concentrerà su due delle forme incluse nella direttiva: l'istigazione

in European States, including ICT-facilitated violence. A Special Report, Luxembourg, Publications office of the EU, 2021, p. 53).

[4] Per un commento alla sentenza della Corte europea dei diritti dell'uomo, sentenza dell' 11 febbraio 2020, ricorso n. 56867/15, *Buturugă v Romania*, v. il contributo di V. TEVERE, *La giurisprudenza della Corte di Strasburgo in materia di violenza digitale/La jurisprudencia del Tribunal de Estrasburgo sobre violencia digital*, in questo Volume pp. 257-272, e A. SINCLAIR-BLAKEMORE, *Cyberviolence Against Women Under International Human Rights Law: Buturuga v Romania and Volodina v Russia (No2)*, in *Human Rights Law Review*, 2022, n. 23, pp. 1-27, (in particolare p. 22 sulla necessità di invocare la violazione dell'art. 3, anziché dell'art. 8 CEDU al fine di avere "*[a] substantial impact on allocation of resources and the seriousness with which the issue is treated by national authorities*"). V. anche A. VAN DER WILK, *Protecting Women and Girls from Violence in the Digital Age: The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing On line and Technology-Facilitated Violence against Women*, Council of Europe Publishing, Strasburgo, Dicembre 2021, p. 9 ss.

alla violenza o all'odio nei confronti di un gruppo di persone o di un membro di detto gruppo definito con riferimento al genere (discorso d'odio) e produzione e condivisione non consensuale di materiale manipolato (*deepfake*). Se la stessa Convenzione di Istanbul non affronta la violenza nel mondo digitale in maniera specifica, vale la pena ricordare come già il rapporto periodico dello UN Special Rapporteur on Violence against Women, its causes and consequences del 2018 su *"online violence against women and girls from a human rights perspective"*[5] raccomandi agli Stati di procedere ad adottare misure finalizzate a combattere la violenza di genere online come anche ribadito dal GREVIO (*Group of Experts on Action against Violence against Women and Domestic Violence*) nella sua prima *General recommendation* del 2021 sulla dimensione digitale della VAW[6]. D'altronde gli studi in materia hanno chiarito, se ce ne fosse bisogno, che le donne sono maggiormente soggette a forme di violenza online rispetto agli uomini, rendendo così vieppiù necessario un intervento specifico sul punto[7].

A livello di Unione europea il Parlamento, nella sua risoluzione del 14 dicembre 2021, ha sottolineato come gli strumenti esistenti nel diritto dell'Unione europea a quella data non prevedessero i meccanismi necessari ad affrontare adeguatamente la violenza di genere online invitando quindi "gli Stati membri e la Commissione a formulare e attuare misure legislative e non legislative, ad affrontare la violenza onli-

[5] Human Rights Council, Report of the Special Rapporteur on violence against women its causes and consequences, sulla violenza contro le donne, le sue cause e conseguenze, MS. DUBRAVKA ŠIMONOVIĆ, *on online violence against women and girls from a human rights perspective,* A/HRC/38/47, 18 giugno 2018.

[6] GREVIO, Raccomandazione Generale n. 1, *sulla dimensione digitale della violenza contro le donne*, adottata il 20 ottobre 2021. Per un commento sulla *General recommendation* con riferimento alla relazione fra strumento di *soft law* e *hard law* riferito alla cyberviolenza contro le donne si veda G. GUNEY, *The Istanbul Convention: a Missed Opportunity in Mainstreaming Cyberviolence against Women in Human Rights Law?*, in *EJIL Talk!*, 2022, disponibile al https://www.ejiltalk.org/the-istanbul-convention-a-missed-opportunity-in-mainstreaming-cyberviolence-against-women-in-human-rights-law/.

[7] Sul punto vedi S. DE VIDO, L. SOSA, *Criminalisation of Gender-Based Violence against Women in European States, Including ICT Facilitated Violence. A Special Report*, cit., p. 52 ss. e le fonti ivi citate.

ne di genere"[8] sottolineando che i nuovi strumenti (quale, oggi, la direttiva VAW) dovranno operare in linea con quelli esistenti come il *Digital Services Act* (al tempo ancora in fase di proposta), la direttiva (UE) 2011/36 del Parlamento europeo e del Consiglio [9] e la direttiva (UE) 2012/29[10]. D'altronde, come avremo modo di vedere, il Parlamento europeo ha da tempo manifestato una particolare attenzione verso le problematiche correlate alla violenza di genere attuata attraverso le nuove tecnologie[11].

2. *(in particolare) Il discorso d'odio di genere online e il c.d.* deepfake

Rispetto ai crimini nel mondo digitale coperti dalla direttiva VAW, questo scritto si concentra su due dei comportamenti illeciti che rientrano nel suo ambito di applicazione: il primo è il discorso d'odio sulla base del genere, alla luce dei possibili sviluppi normativi in materia in seno all'UE, e il secondo è il *deepfake,* che raramente trova un suo riconoscimento all'interno dei codici penali degli Stati membri. In entrambi i casi, infatti, il coordinamento con esistenti o potenziali strumenti normativi dell'UE diventa cruciale.

[8] Risoluzione del Parlamento europeo, *recante raccomandazioni alla Commissione sulla lotta alla violenza di genere: violenza online*, del 14 dicembre 2021 (2020/2035(INL), in GUUE C 251 del 30 giugno 2022, pp. 2-22. Si veda anche lo studio condotto da N. LOMBA, C. NAVARRA, M. FERNANDES, *Combating gender-based violence: Cyber violence - European added value assessment*, Servizio Ricerca del Parlamento europeo (EPRS), marzo 2021.

[9] Direttiva (UE) 2011/36 del Parlamento europeo e del Consiglio, *concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime, e che sostituisce la decisione quadro del Consiglio 2002/629/GAI*, del 5 aprile 2011, in GUUE L 101 del 15 aprile 2011, pp. 1-11.

[10] Direttiva (UE) 2012/29 del Parlamento europeo e del Consiglio, *che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI*, del 25 ottobre 2012, in GUUE L 315 del 14 novembre 2012, pp. 57-73.

[11] Vedi N. LOMBA, C. NAVARRA, M. FERNANDES, *Combating gender-based violence: Cyber violence - European added value assessment*, cit.. Si veda altresì A. VAN DER WILK, *Cyberviolence and hate speech online against women*, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, Settembre 2018.

Il discorso d'odio sulla base del genere ha le sue radici in una cultura patriarcale che legittima, sostiene, giustifica. È una forma di violenza nei confronti delle donne e perpetua la discriminazione di genere. Si diffonde soprattutto online con pericolose derive offline, silenziando le persone che ne sono colpite. Il discorso d'odio sessista è dovuto ad una cultura della discriminazione di genere che passa attraverso le parole [12]. Non ne sono esenti le donne in politica, che, anzi, costituiscono tra le categorie più colpite[13]. I discorsi d'odio contro le donne sono riconosciuti in strumenti di *soft law*, come si vedrà, e a livello nazionale un crescente numero di paesi contempla questa forma di violenza di genere. Se non sono riconosciuti giuridicamente come comportamento vietato per legge, i discorsi d'odio contro le donne vengono normalizzati, declassati al livello di mero scherzo o passatempo sul web. Un'autrice ha evidenziato che i discorsi sessisti, al di là di pochi casi specifici (ad esempio le narrazioni degli stupratori, i discorsi antiabortisti e la pornografia), sono stati ignorati nella discussione generale sul discorso d'odio o sminuiti nel senso di non incontrare i caratteri di questa fattispecie di reato:

The question is why? Why are scholars, even feminist scholars, reluctant to categorize sexist discourse as hate speech? The answer, I believe, is that while racism and homophobia remain 'visible', sexism has been rendered 'invisible', both by the dominant patriarchy and, ironically, by third-wave feminism itself[14].

La Raccomandazione del Consiglio d'Europa contro il sessismo del 2019 ha colto questo aspetto, là dove sottolinea che i discorsi

[12] F. FALOPPA, *#Odio. Manuale di resistenza alla violenza delle parole*, Milano, 2020.

[13] V., ad esempio, Inter-Parliamentary Union, *Sexism, Harassment and Violence against Women in Parliaments in Europe*, 2018, https://www.ipu.org/resources/publications/issue-briefs/2018-10/sexism-harassment-and-violence-against-women-in-parliaments-in-europe e Assemblea parlamentare del Consiglio d'Europa, Risoluzione n. 2274, *per la promozione di parlamenti scevri da sessismi e violenze sessuali*, del 9 aprile 2019.

[14] D.L. LILLIAN, *A Thorn by Any Other Name: Sexist Discourse as Hate Speech*, in *Discourse & Society*, 2017, vol. 18, n. 6, pp. 719-740, p. 736.

d'odio su base etnica o religiosa sono stati riconosciuti come contrari agli standard internazionali ed europei di tutela dei diritti umani, ma non così i discorsi d'odio contro le donne[15]. Va da sé che riconoscere la gravità del discorso d'odio contro le donne non sminuisce l'urgenza del contrasto a tutte le sue forme. Si potrebbe peraltro argomentare che il dibattito sul contrasto dei discorsi d'odio contro le donne contribuirebbe a rivitalizzare il dibattito contro i discorsi d'odio in generale, spingendo anche verso importanti modifiche legislative, quali, ad esempio, la necessità di includere con chiarezza nella fattispecie di reato, o quantomeno quale circostanza aggravante, la dimensione online dell'odio.

Allo stesso modo, la dimensione intersezionale del discorso d'odio contro le donne è praticamente assente [16]. L'intersezionalità è raramente riconosciuta nella dottrina giuridica e a livello giurisdizionale. Lungi, tuttavia, dall'essere un mero fronzolo femminista, il riconoscimento dell'intersezione di diversi fattori dell'odio – il genere, la condizione sociale, la disabilità, l'età, l'origine etnica, ecc. – avrebbe delle conseguenze interessanti non soltanto per quanto attiene l'identificazione degli elementi del discorso d'odio contro le donne e delle ragioni sottese alla moltiplicazione dello stesso, ma anche in termini di definizione delle riparazioni conseguenti all'accertamento della commissione del reato[17].

[15] Comitato dei Ministri, Raccomandazione agli Stati membri, *sulla prevenzione e la lotta al sessismo*, del 27 marzo 2019, CM/Rec(2019)1, p. 18.

[16] Sull'intersezionalità, si veda il lavoro cardine di K. CRENSHAW, *Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color*, in *Stanford Law Review*, 1991, vol. 43, n. 6, pp. 1241-1299. Cfr., altresì, *inter alia*, D. MORONDO TARAMUNDI, *Un caffè da Starbucks. Intersezionalità e disgregazione del soggetto nella sfida al diritto antidiscriminatorio*, in *Ragion pratica*, 2011, n. 2, pp. 365-383; L. SOSA, *Intersectionality in the Human Rights Legal Framework on Violence against Women*, Cambridge, 2017; B.G. BELLO, *Intersezionalità. Teorie pratiche tra diritto e società*, Milano, 2020. Su discorso d'odio e intersezionalità, v. N. GHANEA, *Intersectionality and the Spectrum of Racist Hate Speech: Proposals to the UN Committee on the Elimination of Racial Discrimination*, in *Human Rights Quarterly*, 2013, n. 4, pp. 935-954, e tra i recenti AMNESTY INTERNATIONAL, *Barometro dell'odio. Sessismo da tastiera*, 2020, p. 14, disponibile su https://d21zrvtkxtd6ae.cloudfront.net/public/uploads/2020/03/15212126/Amnesty-Barometro-odio-aprile-2020.pdf.

[17] È quanto si sostiene in S. DE VIDO, *Violence against Women's Health in Interna-*

Anche le Nazioni Unite hanno riconosciuto che le tecnologie dell'informazione e della comunicazione contribuiscono al raggiungimento della parità di genere e all'*empowerment* delle donne e delle ragazze[18]. Il mondo virtuale, in altri termini, apre le porte dell'informazione, dell'educazione, dei mercati, del lavoro e delle comunità, che, nel passato, "*would have been completely inaccessible to most people, particularly girls and women*"; ecco allora che "*social media, information and communication technologies are vital tools for women*"[19]. Se dunque da un lato i media online e le piattaforme social hanno aperto grandi possibilità di esprimere la propria opinione, dall'altro lato questi stessi strumenti sono diventati il mezzo per trasmettere messaggi odiosi. Il discorso d'odio online (e offline) nei confronti delle donne e di altre minoranze sessuali è emerso come nuova forma di violenza di genere nei confronti delle donne. Ne sono vittime le donne che vengono attaccate in quanto donne, ovvero sulla base di caratteristiche personali quali il genere – e altre intersezionali ragioni di discriminazione – mentre gli uomini se attaccati sul web lo sono per le opinioni espresse. Donne in politica[20], giornaliste e bloggers[21] sono tra i target principali, ma anche donne che nella loro sfera privata, nel loro profilo, su Twitter o altri social, manifestano idee che sfidano i tradizionali ruoli

tional Law, Manchester, 2020. V. anche intersezionalità L. SOSA, R.M. MESTRE, *The Istanbul Convention from an Intersectional Perspective*, in S. DE VIDO, M. FRULLI (a cura di), *op. cit*.

[18] Nazioni Unite, *Gender Equality and Empowerment of Women through ICT*, 2005, disponibile su www.un.org/womenwatch/daw/public/w2000-09.05-ict-e.pdf; Council on Human Rights, Risoluzione n. 41/11, *New and emerging digital technologies and human rights*, A/HRC/RES/41/11, dell'11 luglio 2019, disponibile su https://undocs.org/A/HRC/RES/41/11.

[19] D. GING, E. SIAPERA (eds.), *Gender Hate Online*, Cham, 2019, prefazione.

[20] European Institute for Gender Equality, *Cyber violence against women and girls*, 2017, disponibile su https://eige.europa.eu/publications/cyber-violence-against-women-and-girls; Council of Europe, *Combating sexist hate speech*, Council of Europe Gender Equality Strategy, 2016, disponibile su https://edoc.coe.int/en/gender-equality/6995-combating-sexist-hate-speech.html.

[21] European Union Agency for Fundamental Rights, *Violence, threats and pressures against journalists and other media actors in the European Union*, 2016, disponibile su https://fra.europa.eu/en/publication/2016/violence-threats-and-pressures-against-journalists-and-other-media-actors-european.

di genere[22]. È stato osservato che "*being present in online spaces alone often means being present in a hostile, sexist environment*"[23]. Le conseguenze del discorso d'odio online sono devastanti per la vittima, perché la silenziano, inducendola all'auto-censura. È in questo contesto che si deve comprendere la portata della disposizione nella direttiva VAW, che richiede agli Stati membri di criminalizzare "la condotta intenzionale consistente nell'istigare alla violenza o all'odio nei confronti di un gruppo di persone o di un membro di detto gruppo definito con riferimento al genere, diffondendo al pubblico tramite TIC materiale contenente tale istigazione" (art. 8). È evidente innanzitutto il limite derivante dal solo uso della parola "genere" e non "sesso", decisione avvenuta in sede al Consiglio e che si discosta dalla proposta della Commissione di marzo 2022. In secondo luogo, al secondo paragrafo, si legge che gli Stati membri "possono decidere di configurare come reato soltanto le condotte atte a turbare l'ordine pubblico o che sono minacciose, offensive o ingiuriose", il che potrebbe aprire ad un gioco al ribasso in sede di trasposizione in ambito interno.

Se, da un lato, il discorso d'odio non può dirsi completamente reato sconosciuto al sistema UE[24], dall'altro lato il c.d. *deepfake* è del tutto nuovo. Il *deepfake* descrive "*both the technology and the resulting bogus content, and is a portmanteau of deep learning and fake*"[25]. Esso consiste in manipolazioni digitali in cui volti o corpi di individui vengono sovrapposti a immagini o video esistenti, senza il loro consenso. Può trattarsi di un video, un'immagine o un suono creato utilizzando l'Intelligenza Artificiale (IA) e gli algoritmi di apprendimento automa-

[22] Sulla persistenza degli stereotipi nel mondo digitale, si veda Eurobarometer Survey, *Flash Eurobarometer 544 Gender stereotypes - Violence against women* (-fieldwork: 21 to 28 April 2024, 25 835 online interviews with EU citizens, aged 18 years and over, in the 27 EU Member States), novembre 2024: il 43% delle persone intervistate concordano sulla seguente affermazione "*if women share intimate pictures of themselves with someone, they are at least partially responsible if the image is shared online without their consent*", disponibile su https://europa.eu/eurobarometer/surveys/detail/3252.

[23] European Institute for Gender Equality, *op. cit.*, p. 9. Si veda altresì A. VAN DER WILK, *Protecting Women and Girls from Violence in the Digital Age*, cit.

[24] Si veda sul punto, *infra*.

[25] K. YASAR, N. BARNEY, Y. WIGMORE, *Whats deepfake technology?*, in *TechTarget*, disponibile su https://www.techtarget.com/whatis/definition/deepfake.

tico così realistico da renderne impossibile la distinzione con il prodotto originale. Benché il *deepfake* possa essere utilizzato a vari scopi, inclusa ad esempio la contraffazione nel mondo dell'arte, nella maggior parte dei casi, come dimostrano gli studi[26], si tratta di pornografia non consensuale ed è espressione di una "violenza di genere generata dall'IA contro le donne", che colpisce le donne, specialmente coloro all'intersezione di diverse forme di discriminazione, in modo sproporzionato. La direttiva VAW colloca il *deepfake* all'interno del crimine di condivisione non consensuale di materiale intimo o manipolato (art. 5) e lo definisce come l'atto intenzionale di "produrre, manipolare o alterare e successivamente rendere accessibile al pubblico, tramite TIC, immagini, video o analogo materiale in modo da far credere che una persona partecipi ad atti sessualmente espliciti, senza il consenso della persona interessata, qualora tali condotte possano arrecare un danno grave a tale persona". Si nota immediatamente un limite a questa definizione dato dall'elemento dell'arrecare grave danno alla persona, aggiunto in sede di negoziati al Consiglio. Nella direttiva VAW, l'elemento del danno grave nella definizione di crimini informatici potrebbe sembrare compromettere la protezione delle vittime di tali crimini. Si deve, tuttavia, enfatizzare il potere di una interpretazione sistematica. Gli atti che soddisfano i requisiti della violenza nel mondo digitale coperti dalla direttiva generalmente causano un danno grave alla vittima di per sé. Nel considerando 18, la direttiva spiega che "nel valutare se il comportamento possa causare un danno grave, si dovrebbe tener conto delle circostanze specifiche del caso, senza pregiudicare l'indipendenza della giustizia. La probabilità di causare un danno grave può essere dedotta da circostanze di fatto oggettive". Un'interpretazione *victim-oriented* di questa disposizione potrebbe (e dovrebbe) attenuare i rischi di un linguaggio giuridico non così attento alla complessità del fenomeno. Le circostanze di fatto oggettive sono piuttosto evidenti: il *deepfake* è manipolazione, nella maggior parte dei

[26] C. McGlynn, E. Rackley, R. Houghton, *Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse,* in *Feminist Legal Studies*, 2017, n. 25, pp. 25-46; C. Okolie, *Artificial Intelligence-Altered Videos (Deepfakes): Image-Based Sexual Abuse, and Data Privacy Concerns*, in *Journal of International Women's Studies,* 2023, n. 2, Article 11.

casi a sfondo sessuale, che riproduce sul web forme di oppressione e oggettivazione del corpo della donna che non può che condurre ad un danno grave, di natura psicologica, ma anche fisica. In tal senso, l'aggravante prevista dalla direttiva VAW, all'art. 11 lett. i) – la condotta ha causato la morte della vittima o arrecato un grave danno fisico o psicologico alla vittima – ci pare essere un importante passo avanti nell'apprezzare la portata devastante di un crimine compiuto nel mondo digitale. Considerato che la direttiva pone norme "minime", gli Stati restano tuttavia liberi di intervenire anche in ipotesi in cui il quadro non soddisfi tali requisiti di gravità.

3. *Gli strumenti preesistenti rispetto alla direttiva 2024/1385 e in particolare quelli relativi al corretto uso delle nuove tecnologie: dalla direttiva sui servizi di media audiovisivi al* Digital Services Act

La cyberviolenza di genere può avvenire mediante, tra gli altri, come si è visto, la condivisione non consensuale di materiale audiovisivo o di materiale manipolato e la diffusione di messaggi che incitano odio e violenza. Il primo strumento da valutare per prendere atto della relazione con la direttiva VAW è quindi la direttiva sui servizi di media audiovisivi, approvata nel 2010 (direttiva (UE) 2010/13) nella versione da ultimo rivista nel 2018[27], che si occupa anche delle piattaforme per

[27] Direttiva (UE) 2010/13 del Parlamento europeo e del Consiglio, *relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi)*, del 10 marzo 2010, in GUUE L 095 del 15 aprile 2010, pp. 1-24, testo modificato dalla direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, *recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato*, del 14 novembre 2018, in GUUE L 303, 69 del 28 novembre 2018, pp. 69-92. Per approfondimenti sulle piattaforme di *videosharing* nella direttiva audiovisivi e sulla disciplina relativa agli *hate speech* v. O. POLLICINO, M. BASSINI, G. DE GREGORIO, *Internet Law and Protection of Fundamental Rights*, Milano, 2022, in particolare pp. 150-158. Più in generale sull'attuazione v. M. MOSOREANU, V. PODOBEA, M. NUNU, A. ZAGONI-BOGSCH, O. JARVI, I. KORONTHALYOVA, A. INNESTI, C. JACOB, T. RAATS, C-M. IORDACHE, M.

la condivisione di video e immagini. Tale direttiva pone in capo agli Stati l'obbligo di far sì che i servizi di media audiovisivi proteggano il pubblico da contenuti che trasmettano incitazione alla violenza o all'odio verso gruppi di persone o membri di un gruppo con determinate caratteristiche comuni, quali ad esempio il genere, in base a quanto previsto dall'art. 21 della Carta dei diritti fondamentali sul generale divieto di discriminazioni[28]. Gli Stati membri e la Commissione europea devono altresì promuovere, ai sensi degli artt. 4-*bis* e 6-*bis* della direttiva (UE) 2010/13, l'autoregolamentazione attraverso codici di condotta adottati a livello nazionale o anche a livello dell'Unione, codici che ben possono intervenire a rafforzare la protezione rispetto a contenuti che rappresentino episodi di cyberviolenza di genere o incitino alla stessa.

Se in origine il tentativo di responsabilizzare le piattaforme online passava necessariamente attraverso i limitati strumenti offerti dalla direttiva sul commercio elettronico (direttiva 2000/31/CE)[29], oggi il riferimento è necessariamente al regolamento sui servizi digitali 2022/2065 (più noto come *Digital Services Act,* DSA[30]) che si applica a

KOMOROWSKI, C. H. BENGESSER, *Study on the implementation of the provisions of the revised AVMSD concerning the promotion of European works in audiovisual media services – Final report*, European Commission: Directorate-General for Communications Networks, Content and Technology, Publications Office of the European Union, 2024.

[28] Art. 6, direttiva (UE) 2010/13, cit.

[29] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)*, dell'8 giugno 2000, in GUCE L 178 del 17 luglio 2000, pp. 1-16. Sulle previsioni di tale direttiva e l'evoluzione che ha poi portato al *Digital Services Act* in rapporto anche con la direttiva audiovisivi sopra citata v. E. PSYCHOGIOPOULOU, *The Fight Against Digital Hate Speech: Disentangling the EU's Regulatory Approach and Hurdles*, in *German law journal*, 2024, n. 9, pp. 1-15. Sul punto v. anche L. WOODS, W. PERRIN, *Online Harm Reduction - A Statutory Duty of Care and Regulator*, pp. 5, vol. 21, n. 28, 2019, https://carnegieuktrust.org.uk/publications/online-harm-reduction-a-statutory-duty-of-care-and-regulator/

[30] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, *relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)*, del 19 ottobre 2022, in GUUE L 277 del 27 ottobre 2022, pp. 1-102. Per un commento a questo e agli altri strumenti correlati vedi M. INGLESE,

tutte le piattaforme digitali dal 17 febbraio 2024 e obbliga i fornitori di servizi digitali ad eliminare i contenuti illegali, prevedendo all'art. 18 la necessità di notificare alle autorità giudiziarie degli Stati interessati le informazioni che "fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato che comporta una minaccia per la vita o la sicurezza di una o più persone". Questo significa che il coordinamento fra la direttiva VAW e il DSA implica che i contenuti qualificabili come cyberviolenza di genere (condivisione non consensuale di materiale intimo o manipolato, *stalking* online, molestie online, istigazione alla violenza o all'odio online) comportano la necessità per le piattaforme di intervenire per rispettare le previsioni del regolamento DSA, regolamento che obbliga altresì le piattaforme e motori di ricerca di dimensioni molto grandi ad effettuare periodicamente, almeno una volta all'anno, la valutazione del rischio di effetti negativi, attuali o prevedibili, anche relativi alla violenza di genere (art. 34 par. 1) e a prendere misure per attenuare tali rischi (art. 35 par. 1). Al fine di rendere più facile l'individuazione di tali fattispecie possono venire in aiuto gli strumenti di Intelligenza Artificiale che abbiano come obiettivo quello di monitorare e individuare i contenuti illeciti da eliminare[31].

È bene sottolineare però che, per quanto il DSA sia applicabile

Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?, in *Quaderni AISDUE*, 2024, fascicolo speciale n. 2, p. 9 ss. Più in generale vedi G. CAGGIANO, *Il quadro normativo del mercato unico digitale*, in F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, in *Eurojus*, 2020, numero speciale, pp. 13-49; F. FERRI (a cura di), *La nuova disciplina UE sull'intelligenza artificiale*, in *Quaderni AISDUE*, 2024, fascicolo speciale n. 2; e i vari contributi in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021.

[31] Come segnalato da C. MURPHY, I. ZAMFIR in *Cyberviolence against women in the EU*, briefing dello EPRS (European Parliament Research Service), PE 767.146, pubblicato online il 4 dicembre 2024, disponibile su https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI(2024)767146_EN.pdf, una società spin-off dell'Università di Anversa sta sviluppando CaLICO, uno strumento di IA che avrebbe lo scopo di individuare le ipotesi di *hate speech* online aiutando così a procedere in maniera efficiente alla relativa eliminazione. Per informazioni v. https://www.brusselstimes.com/1140252/the-belgian-company-building-the-worlds-first-ai-model-to-track-hate-speech-online.

anche alle fattispecie di cyberviolenza di genere, le sue previsioni non sono state pensate con l'obiettivo principale della tutela delle vittime, tanto che il considerando 87 sottolinea come i fornitori di piattaforme online di dimensioni molto grandi finalizzate alla diffusione di contenuti pornografici (e pertanto focalizzando l'obbligo, se di obbligo si può parlare, solo in capo ad una categoria specifica di piattaforme) "dovrebbero adempiere diligentemente a tutti i loro obblighi ai sensi del presente regolamento in relazione ai contenuti illegali che costituiscono violenza online" garantendo che le vittime possano ottenere la rimozione senza ritardo dei "contenuti che rappresentano la condivisione non consensuale di materiale intimo o manipolato", lasciando così ampio margine per una interpretazione restrittiva delle previsioni di cui sopra.

Al fine di minimizzare i rischi la definizione di Piattaforme di grandi dimensioni (VLOP, ossia *Very Large Online Platforms*[32]) è effettuata dalla Commissione europea e comprende, a seguito dell'ultimo aggiornamento del 20 dicembre 2023, anche colossi che hanno come obiettivo la distribuzione di materiale pornografico quali XNXX, Pornhub, Stripchat, XVideos, che potrebbero essere utilizzati come strumenti per la commissione di *gender-based cyberviolence* tramite la distribuzione di materiale manipolato o comunque senza che vi sia il consenso delle parti interessate[33].

La sfida per l'Unione europea e ancora più per i legislatori nazionali è quindi data dalla necessità di coordinare il funzionamento degli strumenti in essere dotati di diretta applicabilità come il DSA, con la direttiva 2024/1385 ancora in attesa di attuazione da parte degli Stati, al fine di evitare che l'IA sia utilizzata per mettere maggiormente a ri-

[32] I VLOP sono quelle piattaforme che raggiungono la soglia dei 45 milioni di utenti mensili nell'Unione europea. Si trovano nell'elenco anche piattaforme e motori di ricerca "generalisti", quali ad esempio Facebook, X, Google, Instagram, Wikipedia, TikTok e siti di vendita online.

[33] Le piattaforme Pornhub, XVideo e Stripchat, inserite per ultime, hanno impugnato davanti al Tribunale dell'Unione europea le decisioni C(2023) 8842 final, C(2023) 8850 final e C(2023) 8844 final della Commissione, del 20 Dicembre 2023, che hanno determinato la loro inclusione nelle VLOP, le tre cause T-138/24, T 39/24 (del 1 marzo 2024) e T-134/24 del 29 febbraio 2024 sono alla data di questo scritto tuttora pendenti.

schio le donne quali potenziali vittime di cyberviolenza (manipolando, ad esempio, le immagini ai fini di una divulgazione che ne violi i diritti), anziché essere usata per identificare e fermare gli episodi di violenza tramite strumenti tecnologici di individuazione delle fattispecie criminali come sopra descritto. Il coordinamento è espressamente indicato nella direttiva VAW, all'art. 23, che fa "salvo" appunto il regolamento (UE) 2022/2065 e prevede che gli Stati membri adottino "le misure necessarie per garantire che il materiale online accessibile al pubblico", incluso quello relativo al *deepfake* e al discorso d'odio, "sia prontamente rimosso o che l'accesso a tale materiale sia disattivato". In tal senso, le misure possono includere anche la possibilità per le autorità competenti di "emanare ordini giuridici vincolanti per rimuovere tale materiale o disabilitare l'accesso al medesimo".

Anche il regolamento sulla protezione dei dati personali adottato nel 2018 (più noto come cd. GDPR)[34] assume un rilievo in relazione alla direttiva VAW in quanto prevede il diritto per gli utenti di Internet a richiedere alle piattaforme la cancellazione di dati inaccurati e/o irrilevanti (compreso il c.d. diritto all'oblio) con previsioni che sono state però ritenute inadeguate per la lotta alla *gender based violence*. Infatti, la procedura per ottenere la cancellazione di dati da parte di vittime di *cyberviolence* appare troppo lunga a complessa, in quanto legata all'identificazione da parte delle vittime stesse delle piattaforme *host* sulle quali il materiale offensivo è stato caricato, oltre a poter essere applicata solo nei confronti di piattaforme poste all'interno dello spazio giudiziario europeo[35].

[34] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, del 27 aprile 2016, in GUUE L 119 del 4 maggio 2016, pp. 1-88.

[35] Per maggiori dettagli e dati esemplificativi si veda il briefing del Parlamento europeo del 4 dicembre 2024, *Cyberviolence against women in the EU*, cit., in particolare p. 6.

4. *Uno strumento quasi contemporaneo rispetto alla direttiva 2024/1385: l'*AI Act

Pur essendo di poco successivo – benché la proposta fosse precedente alla direttiva VAW – il regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'Intelligenza Artificiale (c.d. *AI Act*)[36] non affronta in maniera soddisfacente il fenomeno della cyberviolenza perdendo così una importante occasione per completare al meglio il quadro creato dalla direttiva VAW e lasciando aperti il problema dell'uso (e abuso) dell'IA, che può generare violenza di genere nei confronti delle donne. Il *deepfake* è definito all'art. 3 par. 60 *AI Act*, come segue: "un'immagine o un contenuto audio o video generato o manipolato dall'intelligenza artificiale che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero ad una persona". Ciò che l'*AI Act* non riconosce è il fatto che la maggior parte dei *deepfake* abbia come obiettivo le donne, specialmente coloro che si trovano all'intersezione di diverse forme di discriminazione. I regolamenti delle piattaforme non forniscono spesso un rimedio adeguato e la rimozione delle immagini e dei video potrebbe richiedere troppo tempo. In prospettiva femminista, i *deepfake* riproducono modelli di discriminazione contro le donne nella società, le sminuiscono, le banalizzano, usano i loro corpi come oggetti sessuali e le portano al silenzio. L'*AI Act* richiede l'etichettatura dei *deepfake* come *deepfake* e introduce standard minimi per i modelli fondamentali, ma omette la moderazione dei contenuti. Così, all'art. 50 par. 7:

> L'ufficio per l'IA incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione per facilitare l'efficace attuazione degli obblighi relativi alla rilevazione e all'etichettatura dei contenuti generati o manipolati artificialmente. La Commissione può adottare atti di esecuzione per approvare tali codici di buone pratiche secondo la procedura di cui all'articolo 56,

[36] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, *che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*, del 13 giugno 2024, in GUUE L, 2024/1689 del 12 luglio 2024.

paragrafo 6. Se ritiene che il codice non sia adeguato, la Commissione può adottare un atto di esecuzione che specifichi norme comuni per l'attuazione di tali obblighi secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Secondo l'atto, i *deepfake* dovrebbero indicare in modo chiaro e distinguibile che il contenuto è stato creato o manipolato artificialmente, etichettando di conseguenza l'*output* dell'Intelligenza Artificiale e rivelandone l'origine artificiale, senza intaccare il diritto alla libertà di espressione e il diritto alla libertà delle arti e delle scienze garantiti dalla Carta dei diritti fondamentali dell'UE. Non c'è alcun riferimento tuttavia all'impatto sproporzionato della violenza di genere generata dall'Intelligenza Artificiale su donne e ragazze, ad eccezione di un brevissimo riferimento nel preambolo, dove si legge che: "Se progettati e utilizzati in modo inadeguato, tali sistemi possono essere particolarmente intrusivi e violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale" (considerando n. 56). Riconoscere nel preambolo il rischio che i sistemi di IA perpetuino modelli di discriminazione nei confronti delle donne è importante ma non sufficiente per incorporare una dimensione di genere richiesta dalla stessa Convenzione di Istanbul al suo art. 6: "promuovere ed attuare politiche efficaci volte a favorire la parità tra le donne e gli uomini e l'emancipazione e l'autodeterminazione delle donne".

Il diritto UE, cui si deve riconoscere un importante sviluppo nel senso di tutelare le donne vittime di violenza di genere, non ha colto l'opportunità di fare propria una politica che trasversalmente comprenda, e contribuisca a sradicare, schemi di discriminazione nei confronti delle donne. Così, la mancanza di riferimenti incrociati alla direttiva VAW è sicuramente un'occasione mancata dell'*AI Act*. È importante sottolineare come i considerando 17 – 24 della direttiva VAW siano stati formulati proprio per sottolineare come la violenza online sia quella "intrinsecamente connessa all'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC)" in relazione alla qua-

le le tecnologie vengono "utilizzate per amplificare in modo significativo la gravità dell'impatto dannoso del reato, modificando in tal modo le caratteristiche dello stesso".

5. *Gli strumenti in corso di approvazione: le proposte della Commissione europea in materia di cooperazione giudiziaria penale per la protezione di vittime di VAW*

Un altro profilo interessante è dato dall'interazione fra la direttiva VAW e vari strumenti di cooperazione giudiziaria penale che sono al momento in corso di revisione proprio alla luce della necessità di adeguarli per i reati commessi mediante l'utilizzo di nuove tecnologie.

Un primo esempio è dato dalla direttiva sulla protezione delle vittime (direttiva 2012/29/UE)[37], tuttora in vigore quale strumento generale di cui la direttiva VAW rappresenta una specificazione. Negli ultimi anni è emersa in maniera chiara la necessità di tutelare in maniera specifica le vittime di crimini commessi online o comunque favoriti dall'utilizzo di nuove tecnologie, compresi quindi i casi di *cyberviolence*[38] e alla luce di ciò la Commissione europea ha presentato una proposta di revisione nel 2023[39]. Tale proposta da un lato offre alla vittime la possibilità di avvalersi delle nuove tecnologie per migliorare l'accesso alla giustizia, ma dall'altro propone di introdurre una disposizione che richieda agli Stati membri di garantire il recepimento dei loro obblighi di cui alla presente proposta senza pregiudicare quelli

[37] Direttiva (UE) 2012/29/UE del Parlamento europeo e del Consiglio, *che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI*, del 25 ottobre 2012, in GUUE L 315 del 14 novembre 2014, pp. 57-73.

[38] V. Commission Staff Working Document *Evaluation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA*, del 28 giugno 2022, SWD/2022/0179 final, in particolare p. 33 ss..

[39] Proposta di Direttiva del Parlamento europeo e del Consiglio, *recante modifica della direttiva 2012/29/UE che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI*, del 12 luglio 2023, COM/2023/424 final.

previsti dalla direttiva VAW (art. 27-*bis* della proposta) e allinea l'uso terminologico effettuato dai due strumenti precisando che il riferimento alle vittime di violenza di genere deve includere le vittime di violenza contro le donne e di violenza domestica, così garantendo una tutela rafforzata, con assistenza mirata e integrata per le vittime di VAW. Pur non affrontando direttamente il tema della cyberviolenza di genere, la riforma impatterà in maniera rilevante sulla tutela delle vittime della stessa, a condizione che si proceda ad una corretta attuazione combinata dei due strumenti.

Una situazione simile si rileva anche in relazione alla direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile[40], altro strumento in corso di revisione per il quale il rapporto con la direttiva VAW porterà alla necessità di inserire delle modifiche atte a coordinare i due strumenti.

In particolare, tale direttiva si sta dimostrando non più efficace proprio perché incapace di fronteggiare l'evoluzione tecnologica intervenuta, nell'ultimo decennio in particolare.

La Commissione europea ha presentato una proposta di modifica il 6 febbraio 2024[41] finalizzata a prevenire e combattere l'abuso sessuale su minori che avvenga utilizzando le nuove tecnologie, imponendo ai servizi di comunicazione online (comprese le applicazioni e le piattaforme di messaggistica) di identificare, segnalare e rimuovere il materiale pedopornografico. In realtà la proposta di riforma presentata dalla Commissione è stata duplice: un primo strumento "provvisorio" *proposal for a Regulation on a temporary derogation from certain provi-*

[40] Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, *relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio*, del 13 dicembre 2011, GUUE L 335 del 17 dicembre 2011, pp. 1-14.

[41] Proposal for a Directive of the European Parliament and of the Council, *on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast)*, del 6 febbraio 2024, COM(2024)060. Sul punto v. K. BARTZ, I. GAGLIO, F. LINZ, A. SORRENTI, *et al.*, *Study supporting the evaluation of the EU Directive 2011/93 and the impact assessment of possible options for its amendment – Final report*, European Commission: Directorate-General for Migration and Home Affairs, Publications Office of the European Union, 2024.

sions of the e-Privacy Directive for the purpose of combating child sexual abuse online è stato adottato il 14 luglio 2021 ed è entrato in vigore il 2 agosto 2021[42]. Tale strumento avrebbe dovuto essere sostituito ad agosto 2024 ma, vista l'impossibilità di trovare un accordo in tempi brevi per il secondo strumento (quello definitivo), la sua applicazione è stata prorogata al 3 aprile 2026.

Quanto alla proposta di riforma definitiva, la Commissione ha presentato il testo il 6 febbraio 2024,[43] e l'*iter* sulla base della procedura legislativa ordinaria è ancora in fase di svolgimento: vale la pena sottolineare, per quanto qui di interesse, che oltre ad inserire una serie di previsioni circa i reati contro minori commessi in un contesto online o mediante il supporto di piattaforme e nuove tecnologie, le modifiche degli artt. 3 e 4 dell'originaria direttiva 2011/93/UE avranno l'obiettivo di garantire la coerenza tra il livello delle sanzioni previste per i reati di abuso sessuale e sfruttamento sessuale nei confronti di un minore con quelle previste per reati analoghi dalla direttiva VAW, innalzando il livello delle pene precedenti e coordinando così in maniera efficace e sinergica i due strumenti proprio in relazione alla cyberviolenza.

Sempre sotto il profilo degli strumenti di cooperazione giudiziaria penale vale la pena sottolineare che la Commissione europea aveva anche proposto, già nel 2021, di estendere la lista di eurocrimini sulla base dell'art. 83 par. 1 TFEU[44] per includervi l'incitamento all'odio (*hate*

[42] Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio, *relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori*, del 14 luglio 2021, in GUUE L 274 del 30 luglio 2021, pp. 41-51.

[43] Proposta di Direttiva del Parlamento europeo e del Consiglio, *relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e il materiale pedopornografico, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (rifusione)*, del 6 febbraio 2024, COM(2024) 60 final.

[44] L'art. 83 par. 1 prevede i c.d. eurocrimini per i quali Parlamento europeo e Consiglio possono stabilire norme minime comuni, attribuendo in capo al Consiglio la facoltà di estendere tale lista ad altri crimini gravi che presentino una dimensione transnazionale con decisione assunta all'unanimità, in modo da creare una base giuridica per l'approvazione di norme armonizzate con l'obiettivo di combatterli.

speech) e i reati generati dall'odio (*hate crimes*), con particolare attenzione verso l'uso di Internet come strumento per porre in essere le fattispecie, ma la necessità di raggiungere l'unanimità in sede di Consiglio ha portato all'impossibilità di concretizzare l'iniziativa, iniziativa che avrebbe consentito di avere un ulteriore fondamento per rafforzare e integrare la base giuridica su cui si fonda la direttiva VAW[45]. In assenza di uno strumento di *hard law* che armonizzi la criminalizzazione di tali fattispecie all'interno degli Stati membri, continua a rivestire un ruolo essenziale sul punto il Codice di condotta sul contrasto all'incitamento all'odio online, redatto dalla Commissione europea a maggio 2016[46], al quale hanno aderito buona parte delle VLOP (a titolo esemplificativo Facebook, X, YouTube e, successivamente, Instagram, Snapchat, TikTok). Infine, come annunciato nella Strategia per la parità di genere 2020-2025, la Commissione faciliterà un quadro di cooperazione tra le piattaforme Internet per affrontare specificatamente la violenza online contro le donne, sotto forma di un altro codice di condotta, che, pur essendo un atto di *soft law*, potrebbe cogliere alcuni di questi collegamenti "mancanti".

[45] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Un'Europa più inclusiva e protettiva: estendere l'elenco dei reati riconosciuti dall'UE all'incitamento all'odio e ai reati generati dall'odio*, del 9 dicembre 2021, COM(2021) 777 def. La Commissione affermava in particolare che l'estensione dell'elenco degli eurocrimini avrebbe creato "un'ulteriore base giuridica per contrastare le forme specifiche di grave violenza contro le donne e le ragazze che possono anche essere definite come incitamento all'odio misogino o reati generati dall'odio misogino il cui motivo è oggettivamente riconducibile al pregiudizio di genere".

[46] Commissione europea, *Codice di condotta per lottare contro le forme illegali di incitamento all'odio online,* 30 giugno 2016. Le originarie partecipanti (Facebook, Microsoft, Twitter e YouTube, che partecipano anche al Forum dell'UE su Internet, hanno accettato di estendere la tutela al di là di quanto reso obbligatorio dalla decisione quadro 2008/913/GAI, *sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale*, del 28 novembre 2008, in GUUE L 328 del 6 dicembre 2008, pp. 55-58. In tale codice di condotta non si prevede però un riferimento all'odio basato sul genere ma i rapporti di monitoraggio danno atto che anche il *gender-based hate speech* rientra tra le ragioni d'odio che vengono monitorate (rappresentando, nel 2022, data del settimo, e per ora ultimo monitoraggio, il 4.1% delle ragioni di odio, percentuale aumentata rispetto ai primi monitoraggi, ma più bassa di quello immediatamente precedente (5,1%)).

6. *Gli strumenti di* soft law

Agli strumenti legislativi già approvati o in corso di approvazione all'interno dell'Unione europea si affianca inoltre l'utilizzo da parte dell'Unione europea stessa di interventi di *soft law.*

D'altronde l'Unione europea ha una lunga tradizione sul punto: basti pensare al programma Daphne, lanciato nel 1997 con stanziamento di milioni di risorse per sensibilizzare alla necessità di combattere la violenza di genere e creare reti che la affrontino – una strategia che si è dimostrata un modo efficace per l'UE di promuovere la questione negli Stati membri e nei paesi candidati. L'impegno dell'UE a combattere la violenza di genere, sostenendo e proteggendo le vittime e responsabilizzando i carnefici, è stato più recentemente rafforzato da altri strumenti *soft law* come la comunicazione 2021 della Commissione europea sugli *hate speech* già citata sopra, e la strategia per la parità di genere 2020-2025 "Un'Unione dell'uguaglianza" approvata dalla Commissione europea a marzo 2020[47]. In tale documento si sottolinea la necessità di integrare la dimensione di genere nelle varie politiche dell'Unione europea rafforzando il quadro giuridico esistente, promuovendo la lotta alla violenza di genere e affermando che chiunque dovrebbe essere al sicuro non solo nella propria casa e negli spazi pubblici, ma anche online. La Commissione ha già raggiunto alcuni degli obiettivi che si proponeva in tale strategia (si pensi all'adozione di regole uniformi sui servizi digitali "per chiarire le responsabilità delle piattaforme online per quanto riguarda i contenuti diffusi dagli utenti" concretizzatasi nel DSA e nell'adesione alla Convenzione di Istanbul), altri però sembrano ancora lontani come lo sviluppo di un nuovo quadro di cooperazione tra le piattaforme Internet, che non può dirsi pienamente raggiunto e il riferimento alla necessità di "contrastare [la diffusione] di contenuti lesivi e oltraggiosi che non sempre sono considerati illegali, ma che possono avere effetti devastanti"[48].

[47] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un'Unione dell'uguaglianza: la strategia per la parità di genere 2020-2025*, del 5 marzo 2020, COM(2020) 152 final.

[48] S. DE VIDO, L. SOSA, *Criminalisation of Gender-Based Violence against Women in European States, Including ICT Facilitated Violence. A Special Report*, cit., p. 135.

Anche gli Stati hanno spesso introdotto strumenti di *soft law* ad affiancare le proprie previsioni normative nazionali in tema di *cyber-violence*, spesso carenti sotto il profilo della correlazione al genere. Purtroppo, non tutti gli strumenti di *soft law* nazionali si sono dimostrati sufficienti a supplire alle carenze normative e pertanto un intervento dell'Unione europea appare sempre più necessario[49].

7. *La direttiva 2024/1385: la* digital literacy *come strumento di prevenzione*

Nell'osservare le relazioni tra strumenti giuridici in vigore o in corso di approvazione, si nota come la direttiva VAW sia innovativa anche per la forte matrice preventiva di molte delle sue disposizioni. È del tutto evidente che la criminalizzazione di comportamenti che ricadono sotto la definizione di violenza nel mondo digitale non è sufficiente per andare alle radici del fenomeno. La prevenzione per il tramite di programmi educativi, campagne di sensibilizzazione e formazione diviene quindi un aspetto cruciale, spesso sottovalutato. In particolare, ai sensi dell'art. 34 della direttiva VAW, le misure preventive riguardano specificamente i reati informatici. Gli Stati membri assicurano che tali misure preventive includano lo sviluppo di competenze digitali (*digital literacy*), compreso il pensiero critico per consentire agli utenti di identificare e affrontare i casi di violenza informatica, di cercare sostegno e di prevenirne la perpetrazione. In una comunità, in un gruppo di persone (famiglia, amici, vicini, colleghi), l'identificazione delle forme di violenza digitale rappresenta uno stru-

[49] Sul punto si veda S. DE VIDO, L. SOSA, *Criminalisation of Gender-Based Violence against Women in European States, Including ICT Facilitated Violence. A Special Report*, cit., p. 55 ss. Per una valutazione delle normative dei singoli Stati membri in materia si veda anche C. WALKEY, K. MANTOUVALOU, N. MEURENS, O. KOUAYA, I. PAVLOVAITE, *The legislative frameworks for victims of gender-based violence (including children) in the 27 Member States*, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, October 2022. Più di recente si veda anche la ricostruzione effettuata da European Women's Lobby, *Report on Cyber Violence Against Women: Policy Overview and Recommendations*, settembre 2024, in particolare p. 67 ss..

mento per prevenire questi fenomeni. L'educazione dovrebbe anche essere finalizzata a spiegare come reagire come spettatore, nel pieno rispetto della vittima, ma anche senza chiudere gli occhi di fronte a quanto si compie nel mondo digitale. Per quanto riguarda la formazione, la direttiva VAW specifica che, nel rispetto della libertà e del pluralismo dei media, gli Stati membri sono tenuti a "incoraggiare e sostenere la creazione di attività di formazione sui media" da parte di organizzazioni di professionisti dei media, di organismi di autoregolamentazione dei media e di rappresentanti dell'industria o di altre organizzazioni indipendenti pertinenti, al fine di "fine di combattere le rappresentazioni stereotipate di donne e uomini, le raffigurazioni sessiste delle donne e la colpevolizzazione delle vittime nei media, così da ridurre il rischio di violenza contro le donne e di violenza domestica" (art. 36 par. 8).

La preparazione degli operatori e la predisposizione di unità specifiche che si occupino di crimini informatici anche di genere è fondamentale. Ciò è stato rilevato anche dal GREVIO nei primi rapporti del secondo *round*. Così, ad esempio, nel rapporto tematico sull'Austria, il GREVIO ha apprezzato che centri di competenza per il crimine informatico fossero stati istituiti negli uffici del Procuratore e che gli ufficiali di polizia preposti avessero ricevuto un *training* specifico[50]. Ha altresì osservato che "*these legislative changes came at a timely point, as a recent analysis by the Fundamental Rights Agency (FRA) of posts and comments on large social media platforms found that women are the main targets of online hate speech, including abusive language, harassment and incitement to sexual violence*"[51].

8. *Considerazioni conclusive*

La combinazione data dagli articoli della direttiva VAW in tema di *cyberviolence* e gli strumenti di diritto dell'Unione europea che la

[50] GREVIO, *First thematic evaluation report Building trust by delivering support, protection and justice Austria*, 10 settembre 2024, https://rm.coe.int/first-thematic-evaluation-report-building-trust-by-delivering-support-/1680b18c17, par. 3.

[51] *Ibidem*.

affiancano sembra lasciare aperti alcuni problemi. Innanzitutto, in nessuno di questi strumenti si trova una definizione di cyberviolenza di genere, quale definizione contenitore alla quale ricondurre le fattispecie di reato previste dalla direttiva VAW. Un tentativo di sistematizzare una definizione comune e condivisa è stato tentato da parte dell'EIGE (European Institute for Gender Equality) nello studio del 2022[52] che suggerisce di utilizzare l'espressione "*cyberviolence against women and girls*". Sarebbe stato sufficiente aggiungere un paragrafo all'art. 2 della direttiva VAW, che riprenda il considerando 17 della medesima: una violenza "intrinsecamente connessa all'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC)", dove le tecnologie sono utilizzate per amplificare in modo significativo la gravità dell'impatto dannoso del reato, modificando in tal modo le caratteristiche dello stesso.

Inoltre, i sistemi posti in essere dalle piattaforme, direttamente o indirettamente in attuazione delle previsioni di diritto dell'Unione europea, non sembrano sufficientemente efficaci per moderare l'uso da parte degli utenti in violazione del divieto di cyberviolenza di genere e rimuovere efficacemente le informazioni incriminate. Tutto ciò senza tralasciare il fatto che alcune piattaforme, quelle maggiormente correlate ad episodi di violazione in quanto pensate per condividere materiale pornografico, si stanno dimostrando restie a collaborare nell'attuazione degli strumenti esistenti, come dimostrato dall'impugnativa avvenuta della decisione di considerarle VLOP, o si stanno muovendo sempre più nel *dark web*. Da questo punto di vista non si può che auspicare un intervento efficace da parte della Commissione europea nell'ambito dei poteri alla stessa attribuiti dal *Digital Services Act*, sezione 3.2, che comprendono la possibilità di sanzionare econo-

[52] EIGE, *Combating cyber violence against women and girls*, 2022, https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en, p. 35. Per altre definizioni v., K. PARK, D. GING, S. MURPHY, C. MCGRATH, *The impact of the use of social media on women and girls*, European Parliament: Directorate-General for Internal Policies of the Union European Parliament, 2023, p. 28. Per approfondimenti v. anche E. L. BACKE, P. LILLESTON, J. MCCLEARY-SILLS, *Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence*, in *Violence and Gender*, September 2018, n. 5(3), pp. 135–146.

micamente le piattaforme che non rispettano gli obblighi derivanti dal regolamento e in particolare dai suoi art. 34 e 35.

Inoltre, manca un forte collegamento, che è stato realizzato in parte dall'art. 23 della direttiva VAW con riferimento al DSA, tra strumenti diversi. In particolare, come si è detto, l'*AI Act* non ha colto l'impatto sproporzionato della violenza generata dall'Intelligenza Artificiale sulle donne e le minori.

Spetterà quindi agli Stati membri procedere a dare attuazione alla direttiva VAW cercando di colmare le lacune esistenti circa queste fattispecie particolarmente insidiose di reato, tenendo presente l'obiettivo fondamentale di prevenire e tutelare le vittime che deve sempre affiancare quello di sanzionare il colpevole, considerando altresì l'opportunità di qualificare come tale non solo chi commette materialmente il crimine in prima battuta ma anche chi agevola, non reprime e non pone in essere tutte le misure necessarie per tutelare i diritti delle vittime.

Abstract

L'obiettivo di questo contributo è affrontare le previsioni della direttiva 2024/1385 in materia di cyberviolenza di genere collocandole a confronto con gli altri strumenti esistenti e in corso di approvazione o modifica nell'ordinamento dell'Unione europea al fine di valutare se e come la direttiva si ponga in continuità e coordinamento con tali strumenti e se il lavoro congiunto fra gli stessi possa rappresentare un risultato soddisfacente per proteggere le vittime nei confronti della cyberviolenza di genere. A tale fine ci si soffermerà, quanto agli strumenti esistenti, sulla direttiva sui servizi di media audiovisivi (direttiva 2010/13), sul *Digital Services Act e AI Act,* nonché sul GDPR. Con riguardo agli strumenti in corso di revisione, il contributo si focalizzerà sulla direttiva 2011/93 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, senza tralasciare il riferimento agli strumenti di *soft law*. Con riferimento ai comportamenti coperti dalla direttiva VAW, il capitolo approfondisce il discorso d'odio sulla base del genere e il c.d. *deepfake*. Si proporrà altresì una breve riflessione sull'importanza delle misure di prevenzione nella direttiva VAW per concludere quindi con alcune osservazioni sulla necessità di maggiore coordinamento tra strumenti giuridici dell'UE presenti e futuri.

KEYWORDS: cyberviolenza di genere – Digital Services Act – donne vittime di violenza – violenza domestica – direttiva 2024/1385

LA CIBERVIOLENCIA DE GÉNERO EN LA RELACIÓN ENTRE LA DIRECTIVA 2024/1385 Y OTROS INSTRUMENTOS DEL DERECHO COMUNITARIO

El objetivo de esta contribución es afrontar las disposiciones de la Directiva 2024/1385 en materia de ciberviolencia de género, poniéndola en comparación con otros instrumentos existentes, o en proceso de aprobación o modificación en el ordenamiento de la Unión Europea con el fin de valorar si, y cómo la Directiva continua o/y se pone en coordinación con tales instrumentos y si el trabajo conjunto entre ellas pueda representar un resultado satisfactorio para proteger a las víctimas frente a la ciberviolencia de género. Con este propósito se pone atención en los instrumentos existentes, la directiva de Servicios de Medios Audiovisuales (Directiva 2010/13), el *Digital Services Act* y *AI Act*, así como el GDPR. En cuanto a los instrumentos objeto de revisión, el capítulo se centra en la Directiva 2011/93 relativa a la lucha contra los abusos sexuales y la explotación sexual de los niños y la pornografía infantil, sin olvidar la referencia a los instrumentos de *soft law*. En relación con las conductas contempladas en la Directiva VAW, se profundiza en el discurso de odio basado en el género y en el denominado *deepfake*. También se realiza una breve reflexión sobre la importancia de las medidas preventivas en la Directiva VAW, y se concluye con algunas observaciones sobre la necesidad de una mayor coordinación entre los instrumentos jurídicos de la UE, actuales y futuros.

PALABRAS CLAVE: ciberviolencia de género – Digital Services Act – mujeres víctimas de violencia – violencia doméstica – directiva 2024/1385

DALLA STRATEGIA PER LA PARITÀ DI GENERE ALL'INSERIMENTO DELLA VIOLENZA DIGITALE TRA GLI "EUROCRIMINI": L'APPROCCIO OLISTICO DELL'UNIONE EUROPEA AL FENOMENO DELLA VIOLENZA CONTRO LE DONNE E DI GENERE

Angela Festa[*]

1. *Introduzione*

La violenza contro le donne e di genere, nelle sue molteplici e multiformi manifestazioni[1], è intesa come una forma di violenza atta a colpire le donne in quanto tali o in modo sproporzionato[2].

[*] Ricercatrice in Diritto dell'Unione europea, Università della Campania. Email: angela.festa@unicampania.it.

[1] La violenza contro le donne basata sul genere si può manifestare in via diretta sottoforma di violenza fisica, sessuale (stupri, molestie), psicologica (minacce, umiliazioni, scherno, forme di controllo), economica (negazione dell'accesso alle risorse finanziarie, alla proprietà, al mercato del lavoro, etc.). Rientrano tra le forme di violenza diretta contro le donne la tratta, lo sfruttamento sessuale, i matrimoni forzati, i delitti d'onore, le mutilazioni genitali, nonché le emergenti forme di violenza online, come lo *stalking* online o il cyberbullismo. La violenza contro le donne può, inoltre, manifestarsi anche in via indiretta sottoforma di atteggiamenti, stereotipi, norme e modelli culturali tradizionali rispetto al genere che possono causare forme di violenza basata sul genere.

[2] Sulla scorta della definizione contenuta all'art. 3 della Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne

Si tratta di una violazione dei diritti umani tra le più gravi e diffuse al mondo: limitando il campo di osservazione esclusivamente al panorama dei paesi membri dell'Unione europea, secondo un recentissimo studio condotto congiuntamente dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA), dall'Istituto europeo per l'uguaglianza di genere (EIGE) e dall'Ufficio statistico dell'Unione europea (EUROSTAT)[3] sulla base di dati raccolti tra il 2020 e il 2024[4], a livello UE, una donna su tre è colpita da violenza fisica, sessuale o minacce in età adulta; una su cinque ha avuto esperienza di violenza fisica da parte del proprio partner o da parte di conoscenti stretti[5]; una su tre è stata vittima di molestie sessuali sul luogo di lavoro. L'indagine conferma anche che nonostante la sua pervicacia, tale forma di violenza rimane spesso invisibile perché l'80% di donne che ne ha esperienza non cerca l'aiuto dei professionisti e soltanto il 20% circa denuncia i fatti alle autorità.

Le cause del fenomeno sono senza dubbio complesse, ma larga parte degli studi e dei rapporti internazionali sul tema[6] riconosce che le principali siano da rintracciare in una radicata discriminazione ai danni del sesso femminile, che riflette una disuguaglianza strutturale

e la violenza domestica, c.d. Convenzione di Istanbul del 2011.

[3] Cfr. European Union Agency for Fundamental Rights, European Institute for Gender Equality, Eurostat, *EU gender-based violence survey – Key results. Experiences of women in the EU-27*, Publications Office of the European Union, Luxembourg, 2024. Il report è stato pubblicato il 25 novembre 2024, in una data che ha valore fortemente simbolico. È, inoltre, significativo che sia stato realizzato in stretta collaborazione dall'Agenzia dell'Unione europea che si occupa di diritti fondamentali, dall'Istituto europeo per l'uguaglianza di genere e dall'Ufficio statistico dell'UE. Il precedente report sul tema, considerato una pietra miliare in ambito europeo, era stato realizzato dieci anni prima dall'Agenzia dell'UE per i diritti fondamentali su un campione rappresentativo sia a livello europeo che a livello nazionale di 42.000 donne europee. Cfr. European Union Agency for fundamental rights, *Violence against women: an EU-wide survey. Main results report*, 5 march 2014.

[4] L'intervista ha coinvolto 114023 donne: un numero quasi due volte superiore rispetto a quello delle intervistate nell'indagine dell'Agenzia FRA del 2014.

[5] Quella che è stata definita "violenza di prossimità". Cfr. I. BARTHOLINI, *Violenza di prossimità. La vittima, il carnefice, lo spettatore e il "grande occhio"*, Milano, 2013.

[6] Basti pensare ai rapporti stilati dai diversi Special Rapporteur delle Nazioni Unite sulla violenza di genere.

tra donne e uomini e che vede le prime, in quanto tali, in una posizione subordinata rispetto ai secondi.

Norme, attitudini e stereotipi di genere – diffusi ancora oggi nei più ampi contesti sociali e istituzionali – concorrendo alla costruzione delle identità e delle relazioni sociali, contribuirebbero a riprodurre quelle disuguaglianze e, in ultima analisi, ad alimentare e "normalizzare" gli episodi di violenza contro le donne[7].

Con l'adozione della direttiva (UE) 2024/1385[8], l'Unione europea si è finalmente dotata di un quadro normativo unitario e generale, diretto a contrastare la violenza contro le donne e la violenza domestica[9].

L'approvazione dell'atto giunge, peraltro, parallelamente all'adesione dell'UE alla Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e contro la violenza domestica, c.d. Convenzione di Istanbul[10], a cui l'atto di diritto derivato largamente si ispira, se non altro perché originariamente teso a "surrogare" quella ratifica che tardava ad arrivare[11].

[7] Un ruolo rilevante è certamente svolto anche dalla rappresentazione mediatica. In tema, cfr. T. ALESCI, *Violenza di genere e rappresentazione mediatica*, in *Il Processo*, 2022, n. 2, pp. 399-421; L. BAINOTTI, *Violenza contro le donne e violenza delle donne nello specchio dei media*, in *Problemi dell'informazione*, 2018, n. 1, pp. 160-161.

[8] Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio del 14 maggio 2024 *sulla lotta alla violenza contro le donne e alla violenza domestica*, in GUUE del 24 maggio 2024, pp. 1-36.

[9] Cfr. M. FERRARI, *Violenza contro le donne: l'Unione europea adotta finalmente la direttiva (UE) 2024/1385*, in *Eurojus*, 17 giugno 2024, pp. 1-5; B. PEZZINI, *Una Direttiva in materia di lotta alla violenza contro le donne e alla violenza domestica*, in *Quaderni costituzionali*, 2024, n. 3, pp. 730-733.

[10] Per approfondimenti sulla Convenzione cfr. il commentario: S. DE VIDO, M. FRULLI (eds.), *Preventing and combating violence against women and domestic violence – A Commentary on the Istanbul Convention*, Northampton, 2023.

[11] L'Unione europea ha firmato la Convenzione nel 2017, ma la ratifica è stata perfezionata soltanto il 28 giugno 2023, dopo che nel 2021, su richiesta del Parlamento europeo, la Corte di giustizia aveva emesso un parere consultivo ai sensi dell'art. 218 TFUE. La Convenzione è entrata in vigore per l'Unione il 1° ottobre 2023. Sul tema della lenta e faticosa adesione dell'UE alla Convenzione di Istanbul, cfr. C. MORINI, *La questione dell'adesione dell'Unione europea alla Convenzione di Istanbul alla luce del parere 1/19 della Corte di giustizia*, in *Freedom Security and Justice: European legal Studies*, 2021, n. 3, pp. 136-162. Cfr. anche S. DE VIDO, *La convenzione di Istanbul quale strumento interpretativo del diritto derivato dell'Ue in situazioni di violenza*

Dotandosi di "norme minime" comuni per il contrasto alla violenza di genere, con la direttiva, l'Unione europea mira ad armonizzare le legislazioni dei suoi Stati membri in materia di prevenzione, protezione delle vittime e criminalizzazione di alcune forme di violenza di genere, inclusa tra queste anche la violenza digitale, non espressamente contemplata nella Convenzione del Consiglio d'Europa.

Nell'economia del presente Volume, il contributo mira innanzitutto ad inquadrare l'atto *de quo* nell'ambito dell'ordinamento giuridico dell'Unione europea e, in particolare, all'interno della Strategia per la parità di genere 2020-2025, di cui costituisce uno dei frutti più rilevanti.

Successivamente, dopo aver illustrato le principali tappe che hanno segnato la genesi dello strumento, passa ad illustrarne i maggiori contenuti, soffermando l'attenzione sui reati connessi alla violenza online.

Svolgendo alcune considerazioni sui punti più controversi del testo normativo adottato, ne individua il principale merito: quello di occuparsi "olisticamente" del tema della violenza di genere, inducendo gli Stati membri ad affrontare il fenomeno attraverso misure non solo punitive ma anche preventive.

2. *La parità di genere tra i valori e gli obiettivi dell'Unione europea: alcune coordinate di diritto primario*

Come anticipato nelle premesse, il fenomeno della violenza contro le donne affonda le sue radici nella disuguaglianza e nella mancanza di equilibrio nei rapporti tra generi.

Non è un caso che a permeare la Convenzione di Istanbul – che resta una pietra miliare in argomento – sia l'idea che "il raggiungimento dell'uguaglianza di genere *de jure* e *de facto*" costituisca "un elemento chiave per prevenire la violenza contro le donne"[12].

contro le donne: la sentenza c-621/21 della CGUE, disponibile su www.sidiblog.org.

[12] Cfr. Preambolo della Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica. Sulle cause etniche e culturali della violenza di genere dalla prospettiva del diritto internazionale, cfr. S. ANGIOI, *Le radici etniche e culturali della violenza di genere: un approccio di diritto internazionale*, in A. DI STASI, R. CADIN, A. IERMANO, V. ZAMBRANO (a cura di),

Ebbene, considerando la violenza di genere e l'uguaglianza uomo-donna come tematiche strettamente connesse, se per un verso è vero che la direttiva (UE) 2024/1385 può essere considerata il primo atto di diritto derivato giuridicamente vincolante volto specificamente a contrastare la violenza contro le donne, per altro verso, non può dirsi che l'impegno dell'Unione europea a favore dell'uguaglianza di genere sia così recente[13].

Al contrario, è ben noto che i riferimenti alla parità uomo-donna nel diritto primario siano presenti sin dai Trattati fondativi. Certamente, l'introduzione dell'art. 119 nel Trattato di Roma del 1957, istitutivo della Comunità economica europea, posto a garanzia della parità salariale fra lavoratori e lavoratrici, poteva dirsi rappresentativa di una preoccupazione di matrice soprattutto economica[14]. Tuttavia, per via pretoria, la Corte di giustizia arrivò a dichiarare ben presto che la norma aveva una vocazione sociale e doveva dirsi espressione di un principio fondamentale della Comunità[15].

Donne migranti e violenza di genere nel contesto giuridico internazionale ed europeo, Napoli, 2023, pp. 33-70.

[13] Cfr. A. SCIORTINO, *L'uguaglianza di genere nell'UE: categorie giuridiche e tutele*, in *Rivista AIC*, 2020, n. 4, pp. 20-58; K. FIORENZA, *L'impegno dell'UE nel contrasto alla violenza di genere: iniziative internazionali e riforme interne*, in *Comparazione e diritto civile*, 2023, n. 2, pp. 753-789.

[14] Ai sensi dell'allora art. 119: "Ciascuno Stato membro assicura durante la prima tappa, e in seguito mantiene, l'applicazione del principio della parità delle retribuzioni fra i lavoratori di sesso maschile e quelli di sesso femminile per uno stesso lavoro. Per retribuzione deve essere inteso, ai sensi del presente articolo, il salario o trattamento normale di base o minimo, e tutti gli altri vantaggi pagati direttamente o indirettamente, in contanti o in natura, dal datore di lavoro al lavoratore in ragione dell'impiego di quest'ultimo. La parità di retribuzione, senza discriminazione fondata sul sesso implica: a) che la retribuzione accordata per uno stesso lavoro pagato a cottimo sia fissata in base a una stessa unità di misura, b) che la retribuzione corrisposta per un lavoro pagato a tempo sia uguale per un posto di lavoro uguale".

[15] L'art. 119 del Trattato CEE contiene il principio della parità nelle condizioni d'impiego ed il principio di non-discriminazione in base al sesso è, nelle materie disciplinate dal Trattato – fra cui la materia del lavoro –, un principio di diritto comunitario applicato dalla Corte di giustizia in ragione delle finalità sociali ed economiche del Trattato. Cfr. Corte di giustizia, sentenza dell'8 aprile 1976, *Gabrielle Defrenne contro Société anoyme belge de navigation aérienne Sabena*, p. 1369.

Per la cristallizzazione di tale apertura giurisprudenziale nel diritto primario si dovette comunque attendere poco più di un ventennio: è stato il Trattato di Amsterdam ad aver introdotto la parità uomo-donna tra gli obiettivi della Comunità[16] e ad aver fornito all'art. 13 TCE[17] la base giuridica per l'adozione di atti di diritto derivato destinati a contrastare le discriminazioni di genere in tutte le politiche comunitarie, al di là dei settori dell'occupazione e del mercato[18].

Purtuttavia, quello che si intende rimarcare è che nel corso dell'evoluzione normativa e della costruzione della "Comunità di diritto" che l'Unione europea ambisce a rappresentare, l'impianto di diritto primario in materia di parità di genere si è notevolmente consolidato.

All'interno del Trattato attualmente vigente, la parità tra donne e uomini è assurta, infatti, ai sensi dell'art. 2 TUE, ad uno dei valori fondanti e identitari dell'Unione, comune agli Stati membri[19]. Inoltre, ai sensi dell'art. 3, par. 3 TUE la lotta alle discriminazioni e la promozione della parità tra donne e uomini sono obiettivi dell'Unione che, ai sensi dell'art. 8 TFUE, vanno impressi, secondo un vincolo di integrazione normativa orizzontale, in tutte le azioni dell'Organizzazione[20]. Ciò non diversamente da quanto richiedono altre disposizioni di ap-

[16] Attraverso una modifica degli artt. 2 e 3 TCE.

[17] Tale norma è oggi contenuta nell'art. 19 TFUE che ammette nei casi in cui non ci siano norme più specifiche (per esempio gli artt. 25 e 157 TFUE) e nei limiti delle competenze dell'UE, l'adozione di provvedimenti legislativi per combattere tutte le forme di discriminazione, incluse quelle fondate sul sesso. È rilevante notare che la norma preveda ancora oggi per tali provvedimenti il ricorso alla procedura speciale che richiede che il Consiglio deliberi all'unanimità e previa approvazione del Parlamento.

[18] In tema, O. POLLICINO, *Discriminazione sulla base del sesso e trattamento preferenziale nel diritto comunitario*, Milano, 2005.

[19] Come espressamente chiarito nelle sentenze del 16 febbraio 2022 sulla legittimità del regolamento 2020/2092, tutti gli elementi dell'art. 2 sono valori dell'UE. Per approfondimenti in merito a tale giurisprudenza sia consentito rimandare a A. FESTA, *Le sentenze «gemelle» del 16 febbraio 2022: oltre la questione di legittimità, un «manifesto» sui fondamenti del diritto europeo*, in *Papers di diritto europeo*, 2022, n. 1, pp. 81-110.

[20] Per uno sguardo critico alla prospettiva di genere nel diritto internazionale privato, cfr. R. ESPINOSA CALABUIG, *La (olvidada) perspectiva de género en el Derecho internacional privado (La prospettiva (dimenticata) di genere nel diritto internazionale privato)*, in *Freedom Security and Justice: European Legal Studies*, 2019, n. 3, pp. 44-57.

plicazione generale, come l'art. 10 TFUE, che prevede l'integrazione della lotta alle discriminazioni (fondate, tra l'altro, anche sul sesso) nella definizione e attuazione delle politiche e azioni dell'UE.

Ne consegue che tutt'oggi il legislatore dell'Unione ha l'obbligo di valutare gli effetti che un determinato atto o una data misura possono comportare per gli uomini e per le donne, a prescindere dallo scopo in concreto perseguito dalla natura dell'atto o dalla misura in questione[21], dandosi così attuazione al cosiddetto *gender mainstreaming*, vale a dire il processo di inclusione della prospettiva di genere nelle varie fasi di pianificazione e monitoraggio degli interventi pubblici[22].

In questo quadro normativo, meritano menzione anche l'art. 153 TFUE, che consente all'Unione di intervenire nell'ambito più ampio delle pari opportunità e della parità di trattamento nei settori dell'impiego e dell'occupazione, e l'art. 157 che, riprendendo i contenuti dell'ex art. 119 del Trattato CEE sul principio della parità di retribuzione tra lavoratori di sesso maschile e femminile, contiene una norma dotata di effetto diretto[23] e afferma, al suo par. 4, che gli Stati membri possono mantenere o adottare misure che prevedano vantaggi specifici diretti a facilitare l'esercizio di un'attività professionale da parte del sesso sottorappresentato, ovvero evitare o compensare svantaggi nelle carriere professionali.

Di assoluta rilevanza nel panorama del diritto primario è, infine, la

[21] Oltre che sul piano delle misure di *soft law*, l'art. 8 trova attuazione a livello normativo, attraverso varie tecniche, quali l'adozione di strumenti di tutela specifici, oppure tramite l'inserimento di norme che estendono i vincoli in capo agli Stati, o ancora per mezzo del finanziamento di programmi che hanno come obiettivo la diffusione della parità di genere. Gli obiettivi posti dall'art. 8 coinvolgono tutte le istituzioni europee a vario titolo: la Commissione è propulsore del processo di integrazione normativa della prospettiva di genere, delle attività di *soft law* e promozionali nell'ambito del *gender mainstreaming*, mentre le altre istituzioni sono coinvolte sul piano politico nella fase dell'adozione degli atti normativi in senso conforme all'art. 8 TFUE. In questo ambito, non è meno rilevante il ruolo dei singoli Stati membri, della cui collaborazione non si può fare a meno per l'attuazione delle direttive. Cfr. S. NICCOLAI, *I rapporti di genere nella costruzione costituzionale europea*, in *Politica del diritto*, 2006, n. 4, p. 595 ss.

[22] S. MAZEY, *Gender Mainstreaming strategies in the EU: delivering on an agenda?*, in *Feminist legal studies*, 2022, 10(3), pp. 227-240.

[23] Come riconosciuto dalla Corte di giustizia sin dalla sentenza *Defrenne*.

Carta dei diritti fondamentali dell'Unione europea (CDFUE) che, ponendosi come pienamente vincolante per le istituzioni, gli organi e gli organismi dell'Unione e per gli Stati membri, sia pure nei limiti applicativi dell'art. 51[24], attribuisce grande rilievo al principio di uguaglianza, a cui dedica l'intero titolo terzo (artt. 20-26).

È l'art. 23, par. 1, a sancire più precisamente che "la parità tra donne e uomini deve essere assicurata in tutti i campi, compreso in materia di occupazione, di lavoro e di retribuzione", affermando altresì, al par. 2, che "il principio della parità non osta al mantenimento o all'adozione di misure che prevedano vantaggi specifici a favore del sesso sottorappresentato"[25], richiamando così quanto previsto all'art. 157, par. 4 TFUE e riconoscendo piena legittimità all'adozione di vantaggi specifici e a misure preferenziali, funzionali alla rimozione delle condizioni di svantaggio presenti in un determinato ambito sociale o lavorativo, al fine di garantire una coesistenza armoniosa e una partecipazione equilibrata all'interno della società tanto alle donne quanto agli uomini[26].

L'art. 23 CDFUE denota, quindi, una presa di coscienza circa l'entità del principio della parità di trattamento tra i generi, il cui raggiungimento diventa possibile considerando tanto la dimensione negativa, concernente il divieto di discriminazione, quanto la dimensione positiva delle misure preferenziali.

3. *La Strategia per la parità di genere*

Esaminate, seppur molto sinteticamente, le coordinate di diritto primario entro cui si muove l'ordinamento sovranazionale, l'azione

[24] Sull'ambito di applicazione della Carta, da ultimo, cfr. A. DI STASI, A. IERMANO, A. LANG, A. ORIOLO, R. PALLADINO, *Spazio europeo di giustizia e applicazione giurisprudenziale del Titolo VI della Carta dei Diritti fondamentali dell'Unione europea*, Napoli, 2024.

[25] Cfr. F. SPITALERI (a cura di), *L'eguaglianza alla prova delle azioni positive*, Torino, 2013.

[26] F. SPITALERI, L.M. RAVO, *Trattamenti preferenziali e azioni positive a favore delle donne: punti fermi e linee di sviluppo della giurisprudenza della Corte Europea dei diritti dell'uomo*, in F. SPITALERI (a cura di), *op.cit.*, Torino, 2013, pp. 189-220.

concreta da cui la direttiva (UE) 2024/1385 origina è costituita dalla Strategia per la parità di genere presentata dalla Commissione europea il 5 marzo del 2020, per il periodo 2020-2025[27]. Trattasi di un programma d'azione particolarmente ambizioso volto a fissare gli obiettivi strategici e le azioni da compiere per dare nuovo slancio all'uguaglianza tra donne e uomini e costruire un'Europa garante della parità di genere.

Il fatto che l'atto che si occupa di lotta alla violenza di genere derivi da una strategia per le pari opportunità testimonia ancora una volta che le due dimensioni sono strettamente intrecciate: anzi, la violenza di genere contro le donne può essere considerata tanto causa quanto conseguenza delle disuguaglianze di genere nei vari settori della socialità.

La Strategia parte dalla considerazione che malgrado gli Stati membri dell'Unione siano a livello mondiale considerati "avanzati" nella tutela della parità di genere[28], tuttavia, nessun paese membro raggiunge la "piena" parità[29].

Il piano si propone, quindi, di contribuire alla creazione di uno spazio europeo in cui donne e uomini possano esprimere pienamente le proprie capacità e avere le medesime occasioni di partecipare in modo equo e inclusivo allo sviluppo della società europea. Il tutto sia attraverso azioni mirate che attraverso una migliore integrazione della dimensione di genere in tutte le politiche dell'UE, a rilievo sia interno che esterno.

Il primo degli obiettivi indicati dalla Strategia è proprio quello di "liberarsi della violenza e degli stereotipi". Gli stereotipi sono conside-

[27] Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un'Unione dell'uguaglianza: la strategia per la parità di genere 2020-2025*, del 5 marzo 2020, COM(2020) 152 def., disponibile su https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/gender-equality-strategy_it.

[28] Dalle statistiche risulta infatti che effettivamente 14 tra i primi 20 paesi al mondo per l'attuazione della parità di genere sono Stati membri dell'Unione europea.

[29] In questo campo si registra, tra l'altro, anche quello che viene definito "paradosso nordico": paesi del Nord Europa, come Svezia, Danimarca e Finlandia, da sempre in cima alle classifiche internazionali sull'uguaglianza di genere (v. il *Gender equality index* dell'EIGE o il *Global Gender Gap Report*), accanto a dati particolarmente positivi in termini di pari opportunità, riportano tassi di violenza domestica elevatissimi, con stereotipi e pregiudizi ben radicati.

rati "una delle cause profonde della disparità" in tutti gli ambiti della società[30] e riguardano tutti i settori[31]. È a questo proposito che, in considerazione delle difficoltà di ratifica della Convenzione di Istanbul, la Commissione preannuncia l'intenzione di proporre misure atte ad estendere le sfere di criminalità – c.d. eurocrimini – a forme specifiche di violenza di genere, come le mutilazioni genitali femminili, l'aborto forzato, la sterilizzazione forzata, i matrimoni precoci, il delitto d'onore. La Commissione sottolinea anche la forte necessità di lavorare sul piano dell'educazione e della formazione sin dall'infanzia, per sostenere lo sviluppo di relazioni non violente, impegnandosi a finanziare la formazione, il rafforzamento delle capacità e i servizi di supporto. Si sofferma, dunque, sul tema della violenza e delle molestie in ambito lavorativo e sul fronte della violenza online diventata dilagante,

[30] Già la Risoluzione del Parlamento europeo, *sull'eliminazione degli stereotipi di genere nell'Unione europea*, del 12 marzo 2013, 2012/2116(INI), in GUUE C 36 del 29 gennaio 2016, ma anche la Risoluzione del Parlamento europeo, *sulla strategia dell'UE per la parità di genere*, del 21 gennaio 2021, 2019/2169(INI), in GUUE C 456 del 10 novembre 2021, pp. 208-231, rilevavano che in tutto il mondo sono presenti strutture e stereotipi dannosi che perpetuano la disuguaglianza; "l'abbattimento di tali strutture e stereotipi costituirà un progresso verso la parità di genere"; "promuovere la parità di genere e investire nelle donne e nelle ragazze non solo apporta benefici alla società nel suo complesso, ma è un obiettivo importante di per sé".

[31] Incluso quello giudiziario. L'EIGE ha coniato una vera e propria definizione di stereotipo giudiziario: si tratta di una pratica dei giudici che attribuisce a un individuo attributi, caratteristiche o ruoli specifici sulla base della sua appartenenza a un particolare gruppo sociale. La definizione è ripresa da S. CUSACK, *Eliminare gli stereotipi giudiziari - Parità di accesso per la giustizia alle donne nei casi di violenza di genere*, Documento finale presentato all'Ufficio dell'Alto Commissario delle Nazioni Unite per i diritti umani nel 2014. A proposito di stereotipi giudiziari, il caso italiano è tra l'altro piuttosto emblematico: basti pensare che soltanto pochi anni fa la Corte europea dei diritti dell'uomo, con sentenza resa nel noto caso *J.L. c. Italia* ha condannato il paese per violazione dell'art. 8 CEDU, posto a tutela del diritto al rispetto della vita privata e familiare, perché una sentenza della Corte d'Appello di Firenze, in un processo per stupro, aveva stigmatizzato la vittima attraverso giudizi deplorevoli, non lineari e comunque irrilevanti sulla sua vita privata. Cfr. Corte europea dei diritti dell'uomo, sentenza del 27 maggio 2021, *JL c. Italia*, ricorso n. 5671/16. Per approfondimenti, A. IERMANO, V. TEVERE, *Stereotipi di genere nelle aule di giustizia e vittimizzazione secondaria: analisi del caso J.L C. Italia*, in *Culture e Studi del Sociale*, 2023, n. 8(1), pp. 21-35.

per annunciare una legge sui servizi digitali volta a chiarire le responsabilità delle piattaforme online[32].

Un punto affrontato dalla Commissione nell'analisi che segue riguarda anche l'uso dei mezzi di comunicazione come strumenti per combattere gli stereotipi, in quanto in grado di influenzare convinzioni, valori e percezione della realtà. Interessante a tal proposito è il richiamo all'Intelligenza Artificiale (IA), che rischia di riprodurre e amplificare i pregiudizi di genere qualora gli algoritmi non si rivelino sufficientemente trasparenti.

Il secondo obiettivo indicato dalla Strategia è quello della realizzazione di un'economia basata sulla parità di genere, per raggiungere il quale la Commissione individua degli interventi che incidono sulla partecipazione ai diversi settori economici, sul divario di genere nel mercato del lavoro, sul divario retributivo e pensionistico, nonché sull'assistenza familiare.

Il documento sottolinea quanto la partecipazione delle donne al mercato del lavoro sia importante per l'economia, ai fini dell'accrescimento di forza lavoro e di competenze. Peraltro, dati statistici dimostrano che per le donne avere un lavoro si accompagna anche ad una maggiore probabilità di uscire da relazioni violente e che anche la violenza psicologica da parte del proprio partner sia meno frequente per le coppie paritarie dove lei guadagna quanto lui.

Nonostante si registri un aumento del tasso di occupazione delle donne, queste ultime incontrano ancora molte difficoltà, sia nel trovare lavoro che nel mantenerlo; difficoltà che derivano in larga misura dalla mancanza di un'equa ripartizione delle responsabilità di assistenza tra i genitori e dal difficile equilibrio tra vita professionale e vita familiare.

Con riguardo al rapporto di lavoro, la Commissione punta l'attenzione sul divario retributivo[33] che, di conseguenza, si ripercuote

[32] Il c.d. DSA, poi adottato il 19 ottobre 2022. Cfr. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, *relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)*, del 19 ottobre 2022, in GUUE L 277, del 27 ottobre 2022, pp. 1-102.

[33] In tutti i paesi del mondo e nella maggior parte dei settori lavorativi, le donne guadagnano meno degli uomini e questo divario continua a rappresentare una delle ingiustizie più diffuse a livello globale. Il *gender pay gap* è, nella sua definizione più

sul trattamento pensionistico e che, in ultimo, espone le donne a un rischio maggiore di povertà.

Il terzo obiettivo tracciato nella Strategia riguarda la necessità che i ruoli dirigenziali nella società siano equamente ripartiti. Rispetto al perseguimento di tale obiettivo, la Commissione dichiara il suo impegno per l'adozione della proposta di direttiva del Parlamento europeo (PE) e del Consiglio riguardante il miglioramento dell'equilibrio di genere nei consigli di amministrazione, presentata nel 2012[34], e per fa-

semplice, la differenza nei guadagni orari lordi medi tra donne e uomini, basata sugli stipendi pagati direttamente ai dipendenti prima che intervengano le detrazioni a titolo di contributi dell'imposta sul reddito e della previdenza sociale. Quando per misurare il divario retributivo tra lavoratori e lavoratrici dipendenti viene considerato unicamente il relativo salario medio, il *gender pay gap* è definito *unadjusted*. Nell'Unione europea, il *gender pay gap* calcolato sulla base della differenza del salario lordo, si attestava al 14,8% nel 2021, con picchi particolarmente alti in Estonia (22,7%), Germania (20,9%), Austria (19,6%) e Repubblica Ceca (20,1%) e più bassi in Romania (3,0%), Lussemburgo (4,6%) ed Italia (5%). L'interpretazione dei numeri non è così semplice come sembra, poiché un divario retributivo di genere minore in un paese specifico non significa necessariamente più uguaglianza di genere. Se prendiamo il caso specifico dell'Italia, il divario è molto al di sotto della media europea, ma il dato non tiene conto di fattori peculiari che caratterizzano il nostro mercato del lavoro, come per esempio il tasso di occupazione femminile, le diverse qualifiche professionali e le specificità del settore pubblico e privato. Questi aspetti emergono a pieno misurando contemporaneamente l'insieme di queste caratteristiche strutturali, che determinano il c.d. differenziale salariale di genere "aggiustato". In un paese come il nostro, in cui il tasso di occupazione femminile è estremamente più basso rispetto a quello maschile e dove l'accesso al mercato del lavoro è più facile per le donne con livello di istruzione più alto, si dovrebbe necessariamente utilizzare questo tasso econometrico corretto per ottenere delle stime più precise.

A titolo esemplificativo, secondo l'Eurostat, il divario retributivo orario medio italiano "non aggiustato" nel 2021 era del 5%, ma, correggendo questo divario per il salario orario medio, le ore lavorate e il tasso di occupazione, saliva al 43,7%. È in questo modo che si riesce a comprendere quanto il *gap* salariale sia non solo il frutto delle caratteristiche personali del lavoratore/lavoratrice, ma anche della disuguaglianza di genere.

[34] La proposta di direttiva è stata poi adottata nel 2022. Cfr. direttiva (UE) 2022/2381 del Parlamento europeo e del Consiglio, *riguardante il miglioramento dell'equilibrio di genere fra gli amministratori delle società quotate e relative misure (Testo rilevante ai fini del SEE)*, del 23 novembre 2022, in GUUE L 315 del 7 dicembre 2022, pp. 44-59.

cilitare la circolazione di buone pratiche riguardanti l'equilibrio di genere nei consigli di amministrazione e nelle posizioni dirigenziali[35].

Infine, negli ultimi tre punti, il documento affronta tre questioni trasversali. La prima riguarda tutti i cambiamenti che l'Unione europea si trova ad affrontare, tra i quali la transizione verde e digitale e il cambiamento demografico, che rende essenziale che tutte le politiche e le iniziative adottate dall'UE e dagli Stati membri abbiano una prospettiva di genere. La seconda questione affrontata attiene alla dimensione finanziaria, necessaria per intraprendere azioni efficaci in materia di parità di genere all'interno dell'Organizzazione. In particolare, vengono in rilievo le azioni volte a promuovere la partecipazione delle donne al mercato del lavoro e a sostenere l'equilibrio tra vita professionale e vita privata, a favorire l'imprenditoria femminile, a combattere la segregazione di genere in alcune professioni e ad affrontare il problema della rappresentanza squilibrata di ragazze e ragazzi in alcuni settori dell'istruzione e della formazione.

In ultimo, la Commissione chiarisce che la Strategia per la parità di genere si colloca all'interno di un progetto la cui portata è necessariamente globale e da portare avanti attraverso iniziative e programmi anche congiunti con l'ONU e campagne volte a sostenere la lotta contro stereotipi di genere e violenza contro le donne.

Ritornando alla direttiva (UE) 2024/1385, essa costituisce uno dei frutti più rilevanti della descritta Strategia[36], testimoniando la volontà dell'Unione di perseguire il contrasto alla violenza contro le donne e alla violenza domestica attraverso strumenti di *hard law* e mediante il ricorso all'adozione di fattispecie incriminatrici comuni agli Stati membri, per raggiungere obiettivi non sufficientemente perseguibili mediante atti di *soft law*.

[35] Nell'intento di investire anche le istituzioni e gli organi europei del compito di assicurare l'equilibrio di genere nelle posizioni dirigenziali, la Commissione stessa assumeva l'impegno di raggiungere un equilibrio di genere del 50% a tutti i livelli dirigenziali del suo personale entro la fine del 2024.

[36] Cfr. C. Kasim, *Advancing Gender Equality: The EU's Landmark Directive 2024/1385 on Violence Against Women*, in *EU Law Analysis*, 21 June 2024.

4. *La direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*

La direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica, nella sua formulazione pubblicata il 14 maggio ed entrata in vigore il 13 giugno 2024[37], costituisce l'esito di un *iter* procedimentale complesso, avviato su sollecitazione del PE[38], nel settembre 2021.

Più nello specifico, il PE aveva invitato la Commissione ad annoverare la violenza di genere tra gli eurocrimini, ai sensi dell'art. 83 TFUE, per equipararla a reati particolarmente gravi come il terrorismo, la tratta degli esseri umani, la criminalità informatica, lo sfruttamento sessuale e il riciclaggio di denaro.

La proposta normativa, poi presentata l'8 marzo 2022[39], facendo seguito a sua volta ad un'ampia consultazione pubblica realizzata me-

[37] La direttiva si applica nei confronti di tutti i paesi membri, fatta eccezione che per la Danimarca, a norma del Protocollo 22 al Trattato.

[38] Già con una Risoluzione del 26 novembre 2009, il PE raccomandava agli Stati membri di migliorare la propria legislazione e le politiche nazionali per combattere ogni forma di violenza contro le donne (Parlamento europeo, *Risoluzione sull'eliminazione della violenza contro le donne*, P7_TA(2009)0098, del 26 novembre 2009, in GUUE C 285E del 21 ottobre 2010, pp. 53-58) mentre in una relazione del 2013 del Servizio di ricerca del Segretariato generale del PE veniva proposta l'adozione di quattro direttive: una sullo stupro, una contro le mutilazioni genitali femminili, una contro la violenza domestica ed una, in alternativa alle precedenti, più ampia sulla violenza di genere contro le donne in generale, con base giuridica individuata nell'art. 83 TFUE. Sul tema cfr. V. TEVERE, *Il difficile cammino verso una tutela integrata delle donne vittime di violenza nello spazio di libertà, sicurezza e giustizia: sviluppi normativi e perduranti profili di criticità*, in *Freedom Security and Justice: European Legal Studies*, 2019, n. 2, pp. 184-207.

[39] Anche questa volta, la scelta della data è di per sé significativa, trattandosi del giorno in cui si celebra la Giornata internazionale della donna. Sulla proposta cfr. S. DE VIDO, *A first insight into the EU proposal for a Directive on countering violence against women and domestic violence,* in *EJIL: Talk! Blog of the European Journal of International Law*, 2022; E. BERGAMINI, *La proposta di una direttiva dell'Unione europea sulla lotta alla violenza contro le donne e alla violenza domestica*, in A. DI STASI, R. CADIN, A. IERMANO, V. ZAMBRANO (a cura di), *op. cit.*, pp. 487-510.

diante il portale "Dì la tua"[40], si presentava come particolarmente ambiziosa, soprattutto sotto il profilo culturale.

L'accordo politico raggiunto sul testo definitivo[41] ha, tuttavia, in parte ridimensionato gli scopi iniziali della proposta, deludendo le aspettative di molte associazioni e gruppi impegnati sul fronte della lotta alla violenza contro le donne, che non hanno tardato ad esprimersi in termini critici verso l'operato delle istituzioni europee[42].

Il più deciso arretramento ha riguardato sicuramente l'art. 5 della proposta, relativo alla nozione di stupro. Quest'ultima, nelle intenzioni della Commissione europea, era fondata sul consenso, come elemento centrale e costitutivo del reato ("*only yes means yes*")[43]. Nel testo finale dell'accordo, tuttavia, a causa di frizioni interne al Consiglio, tale impostazione è venuta meno, sicché, sebbene siano previste delle sanzioni minime per lo stupro, permane nella direttiva una lacuna definitoria tanto grave quanto sintomatica del fatto che – nonostante la questione

[40] La consultazione, aperta a organizzazioni della società civile, parti sociali, soggetti operanti nell'ambito delle pari opportunità, ma anche singoli cittadini, dall'8 febbraio 2021 al 10 maggio 2021, prevedeva la partecipazione attraverso la compilazione di un questionario online ed è esitata in 767 risposte: tra i vari Stati membri, quello più rappresentato risulta essere l'Ungheria con il 48% delle risposte. Sul tema cfr. E. STRADELLA, *Partecipazione multilivello alla formazione delle politiche europee, innovazioni tecnologiche, trasformazione dei processi democratici: il caso della direttiva sulla lotta alla violenza contro le donne e alla violenza domestica*, in *Osservatorio sulle fonti*, 2023, n. 2, pp. 291-305. La consultazione è proseguita anche dopo l'adozione della proposta di direttiva, con l'obiettivo di individuare modi e spazi per un'inclusione della giustizia riparativa all'interno della proposta stessa. In argomento, cfr. T. CHAPMAN, *Restorative Justice: offering access to justice for victims of genderbased violence*, in *Diritti Comparati*, 2023, n. 4, pp. 208-227.

[41] Il 9 giugno 2023, il Consiglio ha concordato la sua posizione sulla direttiva proposta; l'accordo tra i legislatori dell'UE si è raggiunto nel febbraio 2024. Il Parlamento europeo ha quindi adottato la direttiva il 24 aprile 2024 con 522 voti a favore, 27 contrari e 72 astensioni. Il testo è stato adottato dal Consiglio il 7 maggio 2024 e, infine, firmato il 14 maggio 2024.

[42] Cfr. L'appello della rete europea WAVE, riportata da DiRe e disponibile online su https://www.direcontrolaviolenza.it/lettera-di-wave-a-tutte-le-relatrici-nel-parlamento-europeo-della-bozza-direttiva-su-violenza-alle-donne/.

[43] Cfr. R. DE PAOLIS, *Il mancato consenso sul consenso: una riflessione alla luce della nuova Direttiva sulla lotta alla violenza contro le donne e la violenza domestica*, in *Rivista di Diritti Comparati*, anteprima, 2024, pp. 209-247.

appaia superata nel diritto internazionale (la Convenzione di Istanbul include una definizione di stupro basata sull'assenza di consenso, ai sensi dell'art. 36) – tra gli Stati membri dell'Unione europea, in realtà, manca ancora una convergenza sul punto[44]. Magra consolazione appare la disposizione dell'art. 35 che, come si vedrà, impone agli Stati di promuovere campagne di sensibilizzazione e di educazione al consenso.

Come anticipato, l'approvazione della direttiva è giunta quasi contestualmente all'adesione dell'Unione europea alla Convenzione di Istanbul, che obbliga l'UE ad approntare misure giuridiche e politiche per prevenire la violenza contro le donne, sostenere le vittime e punire i colpevoli ed a sottoporsi a valutazione periodica da parte del gruppo GREVIO, il comitato di esperti istituito dalla Convenzione.

Non deve, tuttavia, pensarsi che l'adesione alla Convenzione renda superflua la direttiva o viceversa che la presenza della direttiva renda l'adesione alla Convenzione priva di rilievo, giacché i due atti operano su piani diversi[45]: come è stato osservato, la Convenzione promuove l'operato dell'Unione sul fronte della lotta alla violenza di genere e alla violenza domestica, la direttiva quello degli Stati membri. Tra l'altro, se i paesi dell'UE che non hanno ratificato la Convenzione non sono tenuti a rispettarne gli obblighi di criminalizzazione, diversamente essi sono chiamati a rispettare le previsioni di diritto derivato dell'Unione europea contenute nella direttiva.

La direttiva, per come adottata, è volta in definitiva a combattere la violenza contro le donne e la violenza domestica e, in particolare, le forme più gravi di violenza online, tra cui si contemplano la condivisione o la manipolazione non consensuale di materiale intimo, lo *stalking* online e le molestie online. Essa mira a raggiungere tali obiettivi

[44] Dopo mesi di confronto, la maggioranza degli Stati ha votato a favore dell'esclusione della definizione formulata dalla Commissione. Ciò che più sorprende è che tra questi Stati si contino non solo l'Ungheria, sostenitrice della tesi tradizionale, ma anche paesi come la Germania e la Francia. La questione chiaramente non è di scarsa rilevanza, se si considerano soltanto i riflessi negativi che dispiega sul piano processuale, per la necessità di dover provare la resistenza fisica ai fini della configurazione della fattispecie criminosa.

[45] S. DE VIDO, *L'adesione dell'Unione europea alla Convenzione di Istanbul del Consiglio d'Europa: il ruolo delle organizzazioni della società civile a tutela delle donne*, in *Sistema Penale*, 2023, n. 3.

stabilendo standard giuridici omogenei e formulando sanzioni penali minime comuni a tutti gli Stati membri dell'Unione europea.

L'operazione compiuta è, dunque, quella di estendere la lista dei reati europei di cui all'art. 83, par. 1, comma 2 TFUE[46], come voluto dal Parlamento europeo, includendovi la violenza contro le donne e la violenza domestica, mediante un atto che denota un cambiamento di paradigma dato dalla presa di coscienza di avere a che fare con un fenomeno criminale talmente grave e contrastante con i valori ed i diritti fondamentali dell'Unione europea, da rendere necessaria una regolamentazione comune.

Da un punto di vista formale, la direttiva (UE) 2024/1385 è divisa in 7 capi[47] e si pone in linea con i quattro obiettivi della Convenzione di Istanbul, vale a dire: prevenzione, protezione, azione penale e politiche coordinate. Essa, infatti, può essere strutturata in quattro parti fondamentali: prevenzione e intervento precoce; protezione e accesso alla giustizia; sostegno alle vittime; coordinamento e cooperazione.

All'art. 2, la direttiva contiene innanzitutto una definizione di "violenza contro le donne" e "violenza domestica", nonché una definizione di "vittima", "prestatore di servizi di *hosting*", "prestatore di servizi intermediari", "minore", "persona a carico", "autorità competente". A differenza della Convenzione di Istanbul, la direttiva, però, non fornisce una chiara distinzione tra "genere" e "sesso", usando i termini in modo intercambiabile nella maggior parte dei casi e rischiando così di minare buona parte dei progressi raggiunti sul piano internazionale. Una prospettiva di genere genuina avrebbe permesso, forse, una migliore comprensione delle cause e della natura socialmente strutturata e storicamente radicata di detta forma di violenza.

Seguono, poi, all'art. 3 definizioni di taluni reati, tra i quali quello delle mutilazioni genitali femminili, dei matrimoni forzati, della condivisione non consensuale di materiale intimo o manipolato, dello *stalking* online, delle molestie online, dell'istigazione alla violenza o all'odio online.

[46] Per un'analisi completa dell'art. 83 TFUE, cfr. C. AMALFITANO, *Art. 83 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, 2014, p. 896 ss.

[47] Denominati rispettivamente: Disposizioni generali; Reati concernenti lo sfruttamento sessuale delle donne e dei minori e crimini informatici; Tutela delle vittime e accesso alla giustizia; Supporto alle vittime; Prevenzione ed intervento precoce; Coordinamento e cooperazione; Disposizioni finali.

Un aspetto rilevante del punto è l'introduzione dell'obbligo per i paesi membri di criminalizzare le mutilazioni genitali femminili (art. 3) e il matrimonio forzato (art. 4), a dimostrazione del fatto che tali questioni non possono essere intese come il prodotto di convinzioni etnico-culturali, ma devono essere piuttosto considerate crimini legati al genere.

La direttiva prevede poi disposizioni relative alle sanzioni minime da applicare, alle circostanze aggravanti, alla giurisdizione e ai termini di prescrizione, presentandosi, talora, come sufficientemente dettagliata e, talaltra, riconoscendo un certo margine di discrezionalità in capo agli Stati membri (ad esempio, il termine di prescrizione dei reati non è stato deciso a livello UE ma è disposto dai singoli Stati in relazione alla gravità del reato in questione).

I capi successivi della direttiva (capo 3-4) sono relativi alla protezione e al sostegno alle vittime, a cui deve essere garantito l'accesso alla giustizia, a cure mediche complete e a servizi di salute sessuale e riproduttiva. Gli Stati membri sono tenuti a fornire una formazione adeguata ai professionisti che potrebbero interagire con le vittime, comprese le forze dell'ordine, i pubblici ministeri e la magistratura. La necessità sottolineata è, dunque, quella di prevedere o rafforzare "percorsi di formazione specifica e permanente rivolti a tutte le autorità e agli organismi competenti affinché svolgano celermente e adeguatamente la valutazione individuale del rischio, necessaria per preservare l'incolumità della vittima e fornire un'assistenza su misura, ed evitino il perpetuarsi di stereotipi sessisti che portano ad una vittimizzazione secondaria o ripetuta in tutte le fasi del procedimento"[48]. Per quanto ri-

[48] Il legislatore italiano all'atto di recepimento sarà chiamato a rafforzare e integrare gli strumenti con cui l'autorità giudiziaria dispone misure urgenti di allontanamento, ordinanze restrittive e/o ordini di protezione al fine di tutelare efficacemente le vittime e le persone a loro carico. Si veda a questo proposito il caso *Talpis v. Italia* (ricorso n. 41237/14), in cui la Corte europea dei diritti dell'uomo ha condannato l'Italia per non aver assicurato una tutela effettiva alla ricorrente, vittima di ripetute violenze da parte del marito, a causa dei ritardi nella procedura e della mancata adozione di misure idonee a prevenire il ripetersi delle aggressioni denunciate dalla donna. Sul caso *Talpis* cfr. A. DI STASI, *Il diritto alla vita e all'integrità della persona con particolare riferimento alla violenza domestica (artt. 2 e 3 CEDU)*, in A. DI STASI (a cura di), *CEDU e ordinamento italiano. La giurisprudenza della Corte europea dei diritti dell'uomo e*

guarda l'assistenza alle vittime, la direttiva predispone l'istituzione di centri antistupro e di case rifugio ed introduce una linea di assistenza telefonica rosa attiva 24/24[49].

Il capo 5 è, invece, relativo alla prevenzione, legata alle campagne e ai programmi di sensibilizzazione che devono essere svolti nelle scuole e nelle Università per contrastare gli stereotipi di genere, promuovere l'uguaglianza di genere, il rispetto reciproco e il diritto all'integrità personale e a incoraggiare tutte le persone, in particolare gli uomini e i ragazzi, a fungere da modelli di riferimento positivi per agevolare cambiamenti comportamentali in tutta la società[50].

In ogni caso, si richiede agli Stati membri di adottare politiche globali e coordinate (art. 38) e di introdurre piani d'azione nazionali (art. 39) che dovrebbero essere attuati con la cooperazione a livello sindacale (art. 43). Questi sforzi dovrebbero essere rafforzati dalla collaborazione con organizzazioni non governative. Gli Stati membri sono a tal uopo invitati a considerare le competenze delle organizzazioni femminili e dei servizi specializzati in donne, come attori cruciali nell'affrontare tutte le forme di violenza di genere.

Il capo 7 della direttiva contiene, in ultimo, le disposizioni finali. Tra queste è inserita la clausola di non regressione: pertanto, se gli Stati membri dispongono di norme più avanzate di quelle contenute nella direttiva, essi sono tenuti a mantenere il quadro normativo esistente più protettivo. Quelle della direttiva sono, infatti, concepite come norme "minime" che segnano il *threshold* al di sotto del quale non è consentito scendere.

5. Segue. *La violenza digitale nella nuova direttiva*

Una delle operazioni più riuscite nella direttiva è probabilmente quella di ricomprendere nel concetto di violenza contro le donne e di

l'impatto nell'ordinamento interno (2016-2020), Vicenza, 2020, pp. 1-32.

[49] Si tratta del numero "116 016".

[50] A tale proposito può segnalarsi che l'Unione europea già da tempo riserva dei fondi specifici a tali obiettivi: si pensi al Programma europeo Daphne, varato nel maggio 1997, e volto a prevenire e combattere la violenza contro i bambini, i giovani e le donne e per proteggere le vittime e i gruppi a rischio.

genere anche una serie di condotte che abitualmente non vengono accostate alla nozione in questione.

Quando si parla di violenza di genere, infatti, si pensa soprattutto alle forme più estreme della violenza fisica. Ma, come già accennato, la violenza di genere può assumere manifestazioni multiformi e il contesto della Rete non ne è affatto esente[51]. Al contrario, quest'ultima può essere capace di rendere ancora più evidente lo stretto legame intercorrente tra forme di disuguaglianza e violenza e di amplificare gli effetti della violenza stessa.

Quando è rivolta contro le donne, la violenza in Rete è spesso declinata in aggressioni verbali, insulti, retoriche sessiste stereotipate, ricerca e pubblicazione online di informazioni personali e private (cd. *doxing*), pornografia indesiderata, stigmatizzazione a sfondo sessuale, intimidazioni, minacce di aggressione e di morte, atteggiamenti misogini "punitivi", *cyberstalking*, *revenge porn*, offese e molestie basate sul genere, trasmissione online di atti di aggressione sessuale e stupro[52] che, per le potenzialità del mezzo tecnologico (dove i contenuti possono rimanere online per molto tempo, essere visibili per un pubblico particolarmente ampio ed essere riprodotti e ricondivisi *ad libitum*), possono avere effetti dirompenti sulla persona della vittima.

Come osservato dall'Avvocato generale Spunar che all'uopo cita, in alcune delle sue Conclusioni, il film *The Social Network*: "su internet si scrive con l'inchiostro, non a matita"[53].

[51] Cfr. tra gli altri, S. POZZOLO, R. BENCIVENGA, F. BOSCO, *Genere e tecnologia: nuove capacitazioni o antichi pregiudizi mascherati?*, in *About Gender – Rivista internazionale di studi di genere*, 2016, n. 9, pp. 1-14; P. GRIMALDI, *"Stalking" e bullismo nell'era dei "social network"*, in *Familia*, 2019, n. 6, pp. 719-734; A. BARBIERI, *Violenza di Genere e Nuove Tecnologie: Cyberbullismo, Sexting e Revenge Porn*, Milano, 2020; BARKER KIM, JURASZ OLGA, *Online Misogyny as a Hate Crime: An Obstacle to Equality?*, in *GenIUS*, 2021, n. 1, pp. 51-66; A. SCHIAVON, *La cyber-violenza maschile contro le donne: una nuova sfida per il diritto penale*, in *Studi sulla questione criminale*, 2019, n. 1-2, pp. 207-222; F. CERQUOZZI, *Non è un web per donne: hate speech, cyberstalking e altre forme di violenza on line*, in *Aggiornamenti sociali*, 2020, n. 6-7, pp. 493-502.

[52] Cfr. S. VANTIN, *La lama della rete. Forme della violenza contro le donne sul web*, in *Rivista italiana di informatica e diritto*, 2020, n. 2, pp. 27-33.

[53] Cfr. Conclusioni dell'Avvocato generale Maciej Szpunar, presentate il 4 giugno 2019, causa C-18/18, *Eva Glawischnig-Piesczek contro Facebook Ireland Limited*.

Già nel 2017 l'Istituto europeo per l'eguaglianza di genere aveva sollevato il problema della violenza "virtuale" contro donne e ragazze, denunciando la difficoltà nel reperimento di dati disaggregati rispetto al genere ma anche enfatizzando l'altissima percentuale di vittime, nonché la significativa gravità dei danni che ne derivano. Lo stesso aveva, inoltre, messo in evidenza che la violenza in Rete deve essere intesa come un "*continuum*" rispetto a quella fisica, da cui non va dissociata, anche perché capace di provocare ripercussioni "reali" sulla vita delle persone coinvolte[54], assumendosi come ormai superata la distinzione tra mondo fisico e mondo virtuale, per effetto del cd. "*on-life*" in cui siamo perennemente immersi[55].

Anche il Parlamento europeo, pochi anni più tardi, con una Risoluzione del 14 dicembre 2021, aveva espresso raccomandazioni alla Commissione europea sulla lotta alla violenza di genere, soffermandosi in particolare sulla violenza online[56]. Per non citare le suggestioni sul punto provenienti sul piano regionale europeo dalle raccomandazioni del GREVIO e dalla giurisprudenza della Corte europea dei diritti umani[57].

Su questo sfondo e tesaurizzando le sollecitazioni ricevute, la direttiva pone, dunque, un'enfasi particolarmente significativa sulla lotta alla violenza informatica, disciplinando anche la violenza di genere commessa in Rete e considerando i relativi reati come appartenenti alla sfera di criminalità particolarmente grave, con ciò innovando rispetto alla Convenzione di Istanbul che, anche in ragione del tempo in cui fu negoziata, non contiene riferimenti espliciti alla violenza online[58].

[54] Cfr. European Institute for Gender Equality, *Cyber Violence against Women and Girls*, 2017.

[55] Cfr. L. FLORIDI, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Berlino, 2014.

[56] Parlamento europeo, Risoluzione del Parlamento europeo, *recante raccomandazioni alla Commissione sulla lotta alla violenza di genere: violenza online*, del 14 dicembre 2021, 2020/2035(INL), in GUUE C 251 del 30 giugno 2022, p. 2-22.

[57] Cfr. GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women*, adottata il 20 ottobre 2021; Corte europea dei diritti dell'uomo, sentenza dell'11 febbraio 2020, *Buturugă c. Romania*, ricorso n. 56867/15.

[58] A. IERMANO, *Violenza digitale e Convenzione di Istanbul: una dimensione distinta ma non separata dalla violenza contro le donne*, in *Freedom Security and Justice: European Legal Studies*, 2024, n. 1, pp. 64-95.

D'altra parte, non si può dubitare del carattere transazionale delle fattispecie[59] nonché della necessità di combatterli su basi comuni[60].

Così, già nel Preambolo, la direttiva considera la violenza online come corollario della violenza subita dalle vittime nella vita reale, evidenziando che può ridurre le donne al silenzio, impedendone la partecipazione alla vita sociale su un piano di parità con gli uomini; essa può avere effetti devastanti sulla salute mentale, sul proseguimento degli studi, può causare esclusione sociale, ansia, induzione all'autolesionismo e, in casi estremi, portare al suicidio. Si osserva, inoltre, che la violenza online prende di mira e colpisce soprattutto le donne politiche, le giornaliste e le difensore dei diritti umani.

In questo contesto, la direttiva si occupa di prevedere norme minime per le forme più gravi di violenza online e, più precisamente, per la condivisione non consensuale di materiale intimo o manipolato (art. 5), lo *stalking* online (art. 6), le molestie online (art. 7), l'istigazione alla violenza o all'odio online (art. 8). Per ciascuna fattispecie è offerta una definizione e sono previste delle sanzioni minime (art. 10), che si richiedono essere in ogni caso effettive, proporzionate e dissuasive.

Senza entrare nel merito delle definizioni delle varie fattispecie, quello che può sorprendere in questa sede è forse l'indicazione contenuta nel Preambolo, alla stregua della quale, per il caso dei crimini commessi sul web e connessi all'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC), la responsabilità penale dovrebbe essere limitata a condotte che possono provocare danni gravi o un grave danno psicologico alla vittima, oppure a condotte che possono indurre la vittima a temere seriamente per la propria incolumità o per quella delle persone a suo carico.

In buona sostanza, nell'interpretazione offerta nel Preambolo, la responsabilità dell'autore non può considerarsi *in re ipsa* per il fatto

[59] Si pensi ai reati di *hate speech* online su cui cfr. I. ANRÒ, Online hate speech*: la prospettiva dell'Unione europea tra regolamentazione della condotta dei prestatori di servizi intermediari e ricorso al diritto penale*, in *Osservatorio delle fonti*, 2023, n. 1, pp. 13-39.

[60] A. VERZA, *El mundo cibernético y las nuevas formas de violencia contra las mujeres*, in J.M. LÓPEZ ULLA, J. SÁEZ GONZÁLES (eds.), *Combatiendo la violencia contra la mujer: experiencias europeas y americanas*, Cizur Menor, 2020, pp. 235-274.

della condotta, ma occorrerebbe dimostrare il danno per la vittima, soggetto a valutazione secondo le circostanze del caso.

Inoltre, altro aspetto della disciplina che potrebbe forse sottendere una certa sottovalutazione del fenomeno è la sanzione minima prevista per i reati di condivisione non consensuale di materiale intimo o manipolato, *stalking* online e molestie online, individuata nella pena della reclusione nel limite non inferiore ad un anno, ai sensi dell'art. 10. Attesi i possibili effetti della cyberviolenza sulle vittime, ci si sarebbe potuti aspettare, forse, un'ambizione maggiore su questi fronti.

Diversamente, può considerarsi positivamente sia la previsione contenuta all'art. 23, ai sensi della quale almeno per i reati informatici gli Stati membri sono tenuti a disporre di canali accessibili e prontamente disponibili per denunciare atti di violenza, compresa la possibilità di sporgere denuncia e di presentare prove online, sia l'imposizione dell'obbligo per gli Stati di prevedere tutte le misure necessarie per garantire che il materiale online sia prontamente rimosso o che l'accesso a tale materiale sia disattivato.

La direttiva, pur tacendo in punto di responsabilità delle piattaforme online, prospetta la possibilità per le autorità giudiziarie competenti di emanare su richiesta della vittima ordini giuridici vincolanti a carico dei pertinenti prestatori di servizi intermediari di rimuovere uno o più elementi specifici o di disabilitarne l'accesso, considerando che la rimozione alla fonte può non essere sempre fattibile, a causa di difficoltà giuridiche o pratiche di esecuzione di un ordine di rimozione[61].

In ultimo, altro aspetto positivo del testo è che, anche nel caso della cyberviolenza, la direttiva non manca di precisare quanto sia necessario far leva sulle misure preventive, ovvero sull'educazione, includendo lo sviluppo di competenze di alfabetizzazione digitale, per permettere agli utenti di sviluppare competenze critiche del mondo digitale, individuare e affrontare i casi di violenza online, cercare assistenza e prevenire detta violenza.

[61] Cfr. art. 23 della direttiva in esame.

6. *Considerazioni conclusive: l'approccio olistico dell'Unione europea alla violenza contro le donne e di genere*

La direttiva oggetto di esame, alla quale gli Stati membri dovranno conformarsi entro il 14 giugno 2027 con le disposizioni legislative, regolamentari e amministrative necessarie, costituisce certamente un tassello significativo nell'ambito della Strategia europea per la parità di genere.

Volta a garantire la tutela delle vittime e a potenziare l'uguaglianza di genere nell'Unione europea, non solo attraverso la criminalizzazione di molti reati, ma anche richiedendo agli Stati membri di adottare misure preventive volte a promuovere la parità, essa rappresenta un simbolo significativo dell'impegno dell'UE a raggiungere l'uguaglianza di genere non solo *de jure* ma anche *de facto*.

Certamente, il risultato politico raggiunto resta il frutto di un compromesso che, sotto vari aspetti, può aver deluso molti. L'assenza di convergenza tra gli Stati membri attorno alla definizione del reato di stupro è soltanto uno degli elementi più emblematici che testimoniano quanta strada ci sia ancora da fare.

Ma la direttiva appare lacunosa anche su altri fronti, nella misura in cui, ad esempio, pur riconoscendo che le vittime di discriminazione intersezionale sono esposte a un maggiore rischio di violenza, manca di dedicare norme apposite a gruppi particolarmente vulnerabili, come quello delle donne migranti[62]. Queste ultime, trovandosi, per una pluralità di fattori, ad essere maggiormente esposte allo sfruttamento e alla violenza ed essendo, per la loro condizione, meno propense a denunciare gli abusi subiti, avrebbero evidentemente meritato una più ampia attenzione nel testo della direttiva[63].

[62] In tema, cfr. A. DI STASI, R. CADIN, A. IERMANO, V. ZAMBRANO (a cura di), *Donne migranti e violenza di genere nel contesto giuridico internazionale ed europeo*, cit.; S. DE VIDO, *Donne, violenza e diritto internazionale delle migrazioni*, in N. PESARO, A. FAVARO (Edición), *Viajes y escrituras: migraciones y cartografías de la violencia*, Parigi, 2019, pp. 51-57; I. BOIANO, *Le persecuzioni nei confronti delle donne e il sistema di protezione internazionale: quale Paese può dirsi "sicuro" per le donne?*, in *Questione Giustizia*, 2022, n. 4.

[63] Recentemente, la Corte di giustizia, nel caso *WS c. Bulgaria* (sentenza del 16 gennaio 2024, causa C-621/21,), si è spinta a riconoscere il diritto alla protezione in-

Allo stesso modo, sarebbe stato auspicabile un intervento più incisivo a proposito della violenza di genere nel mondo del lavoro, anche vista la portata del fenomeno, testimoniata da ultimo dall'indagine già citata e pubblicata alla fine del 2024 dalla FRA, da Eurostat e da EIGE. La proposta iniziale dell'art. 4 si riferiva, in realtà, espressamente alle "molestie sessuali sul posto di lavoro" fornendone una definizione, ma quella sua formulazione è stata respinta ed espunta dal testo definitivo.

Pur con i limiti evidenziati, si ritiene, tuttavia, che in ogni caso l'intervento in commento vada celebrato. Il fatto che l'Unione sia finalmente intervenuta attraverso un atto giuridicamente vincolante sul tema ha, infatti, un pregio indiscutibile: quello di imporre agli Stati membri di prendere in carico il contrasto alla violenza di genere e di assumere come centrale il tema della sensibilizzazione e prevenzione del fenomeno a livello sociale.

Riconoscendo la responsabilità condivisa degli Stati membri nella lotta alla violenza contro le donne e la violenza domestica, la direttiva induce gli ordinamenti nazionali ad una necessaria presa di coscienza dell'urgenza di intervenire rispetto ad un fenomeno strutturale ancora pericolosamente radicato.

Risultano particolarmente rilevanti in questo quadro tutte le disposizioni della direttiva che impongono agli Stati membri, non solo di criminalizzare certe condotte, incluse quelle di violenza cibernetica, ma anche di investire nella sensibilizzazione, nell'educazione, nella formazione di figure professionali adeguate alla sfida e nella previsione di una rete di servizi integrati di assistenza specializzata a supporto delle vittime. L'approccio "sanzionatorio/normativo" della direttiva è, infatti, affiancato e bilanciato a quello "costruttivo/riflessivo" che, rivelando l'impegno olistico dell'Unione europea a favore della lotta alla

ternazionale, alla luce della Convenzione di Istanbul, anche alle donne provenienti da paesi in cui la violenza domestica è quasi endemica, e ciò sebbene questa circostanza non sia contemplata dalla direttiva n. 2011/95 tra i motivi per il riconoscimento della protezione internazionale. Cfr. sul tema M.F. ANGORI, *Migrazioni femminili: la Corte di giustizia dell'Unione europea riconosce lo status di rifugiato alle donne vittime di violenza di genere*, in *ADiM Blog*, Osservatorio della Giurisprudenza, febbraio 2024, pp. 1-8. Cfr. anche Corte di giustizia, sentenza dell'11 giugno 2024, causa C-646/21, *K, L v Staatssecretaris van Justitie en Veiligheid*.

violenza di genere e della costruzione della parità, mira a generare nei suoi Stati membri un mutamento culturale nei rapporti sociali.

Intervenendo sulle cause, le norme della direttiva puntano, quindi, a toccare quel substrato culturale da cui la violenza origina, per creare una dinamica favorevole ad un'evoluzione positiva delle politiche di genere, dando nuovo slancio alla sensibilizzazione pubblica nei confronti del fenomeno.

Naturalmente la violenza di genere, inclusa la violenza online, costituisce un tema rispetto al quale il diritto, compreso quello sovranazionale, rappresenta soltanto una delle possibili risposte.

Probabilmente nessun meccanismo giuridico riuscirà da solo a garantire l'uguaglianza di fatto tra i sessi[64]. Ciononostante, la nuova normativa ha il pregio di responsabilizzare sul tema ciascun ordinamento giuridico nazionale dell'Unione europea e di indurre gli Stati membri a considerare la lotta per il contrasto e la prevenzione della violenza di genere, anche nelle sue articolazioni virtuali, tra le priorità politiche, spingendoli ad adottare una strategia uniforme e a dare maggiore organicità alla propria legislazione non sempre incline a cogliere le specificità del fenomeno indagato[65].

Abstract

Il contributo mira ad inquadrare la direttiva (UE) 2024/1385 nell'ambito dell'ordinamento giuridico dell'Unione europea e, segnatamente, all'interno della Strategia per la parità di genere 2020-2025. Ne illustra, dunque, i maggiori contenuti, soffermando l'attenzione sui reati connessi alla violenza online. Svolgendo alcune considerazioni sui punti più controversi del testo normativo adottato, ne individua il principale merito: quello di affrontare olisticamente il tema della violenza di genere, inducendo gli Stati membri ad affrontare il fenomeno attraverso misure non solo punitive ma anche preventive.

[64] Cfr. L. FERRAJOLI, *Manifesto per l'uguaglianza*, Roma, 2019.

[65] Per una disamina recente del contesto normativo italiano, cfr. P. DI NICOLA TRAVAGLINI, F. MENDITTO, *Il nuovo codice rosso. Il contrasto alla violenza di genere e ai danni delle donne nel diritto sovranazionale e interno*, Torino, 2024.

KEYWORDS: direttiva (UE) 2024/1385 – Strategia europea per la parità di genere – non-discriminazione – violenza di genere – eurocrimini

DE LA ESTRATEGIA DE IGUALDAD DE GÉNERO A LA INCLUSIÓN DE LA VIOLENCIA DIGITAL ENTRE LOS "EUROCRÍMENES": EL ENFOQUE HOLÍSTICO DE LA UNIÓN EUROPEA ANTE EL FENÓMENO DE LA VIOLENCIA CONTRA LAS MUJERES Y DE GÉNERO

El capítulo sitúa a la directiva (UE) 2024/1385 en el ordenamiento jurídico de la Unión Europea y, en particular, en la Estrategia para la Igualdad de Género 2020-2025. Se exponen sus principales contenidos, centrándose en los delitos relacionados con la violencia en línea. Luego de exponer las observaciones sobre los puntos más controvertidos del texto legislativo adoptado, se identifica su principal mérito: el de abordar holísticamente la cuestión de la violencia de género, induciendo a los Estados miembros a enfrentar el fenómeno a través de medidas no sólo punitivas, sino también preventivas.

PALABRAS CLAVE: directiva (UE) 2024/1385 – Estrategia Europea para la Igualdad de Género – no discriminación – violencia de género – eurocrímenes

ORDINAMENTO ITALIANO
ORDENAMIENTO ITALIANO

LA "RISPOSTA PENALISTICA" ALLA VIOLENZA CONTRO LE DONNE E ALLA VIOLENZA DOMESTICA PREVISTA DALLA DIRETTIVA 2024/1385: VERSO L'EMANAZIONE DI NUOVE FATTISPECIE INCRIMINATRICI?

Mariangela Telesca[*] *- Elio Lo Monte*[**]

SOMMARIO: 1. Premessa metodologica. – 2. Le singole figure criminose "delineate" dalla direttiva: le mutilazioni genitali femminili (art. 3). – 3. Il matrimonio forzato (art. 4). – 4. La condivisione non consensuale di materiale intimo o manipolato (art. 5). – 5. Lo *stalking* online (art. 6). – 6. Le molestie online (art. 7). – 7. L'istigazione alla violenza o all'odio online (art. 8). – 8. Istigazione, favoreggiamento, concorso e tentativo (art. 9). – 9. Regime sanzionatorio e circostanze.

1. *Premessa metodologica*

La recente direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio, del 14 maggio 2024, *sulla lotta alla violenza contro le donne e alla violenza domestica*, si apre con il dichiarato scopo "di prevenire e combattere efficacemente la violenza contro le donne e la violenza domestica in tutta l'Unione. A tal fine essa rafforza e introduce misure in relazione a: la definizione dei reati e delle pene irrogabili, la protezione delle vittime e l'accesso alla giustizia, l'assistenza alle vittime, una migliore raccolta di dati, la prevenzione, il coordinamento e la cooperazione"[1].

Per il conseguimento di tali condivisibili obiettivi la direttiva (sotto lo specifico profilo del diritto penale sostanziale), nel prendere atto

[*] Ricercatrice di Diritto penale, Università degli Studi di Salerno. Email: mtelesca@unisa.it. È autrice dei parr. 1, 2, 3, 7, 8, 9.

[**] Professore ordinario di Diritto penale, Università degli Studi di Salerno. Email: elomonte@unisa.it. È autore dei parr. 4, 5, 6.

[1] Considerando 1 della direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio, *sulla lotta alla violenza contro le donne e alla violenza domestica*, del 14 maggio 2024, in GUUE L, del 25 maggio 2024, pp. 1-36.

che "le disposizioni vigenti a livello dell'Unione e nazionale si sono rivelate insufficienti a combattere e prevenire efficacemente la violenza contro le donne e la violenza domestica"[2] prevede una serie di interventi che possono essere così sintetizzati:

a) emanazione di specifiche fattispecie di reato (artt. 3-9 – capo 2 della direttiva dedicato ai "reati di sfruttamento sessuale femminile e minorile e criminalità informatica");

b) previsione di sanzioni effettive, dissuasive e proporzionate (considerando n. 28, art. 10);

c) punibilità delle condotte offensive poste in essere attraverso Tecnologie dell'Informazione e della Comunicazione (TIC) in quanto "l'uso delle TIC comporta il rischio di un'amplificazione facile, rapida e diffusa di alcune forme di violenza online, con l'evidente rischio di provocare o aggravare danni profondi e a lungo termine per la vittima";

d) previsione di misure per la rimozione di materiale online (art. 23);

e) attivazione di forme di protezione immediata e di assistenza specifica (considerando n. 38 e succ.) per evitare il rischio di intimidazione, di ritorsione e di vittimizzazione secondaria e ripetuta e, dunque, protezione della dignità e l'integrità fisica delle vittime (considerando n. 7, artt. 14-24) nonché previsione di misure di protezione, assistenza, prevenzione e interventi precoci (art. 1 lett. c);

f) attivazione di interventi mirati per prevenire e ridurre al minimo il rischio che sia commessa violenza contro le donne o violenza domestica e il rischio di recidiva (art. 37).

Con riferimento alla emanazione di specifiche figure incriminatrici – su cui soffermeremo le nostre attenzioni – la direttiva stabilisce che gli Stati membri debbano incriminare le condotte intenzionali[3], per le ipotesi di:

[2] *Ivi*, considerando 5.

[3] Il concetto di "intenzionalità" viene utilizzato dal legislatore sovranazionale come mera volontà in contrapposizione alla negligenza e, quindi, non racchiude una particolare tipologia di dolo (appunto quello intenzionale); ciò per un duplice ordine di ragioni: a) l'uso del dolo intenzionale finirebbe per limitare il campo di azione dell'intervento laddove l'intera direttiva è strutturata per ampliare al massimo l'intervento sanzionatorio; b) in altre direttive (ad esempio come quella sulla tutela

1) mutilazioni genitali femminili (art. 3);
2) matrimonio forzato (art. 4);
3) condivisione non consensuale di materiale intimo o manipolato (art. 5);
4) *stalking* online (art. 6);
5) molestie online (art. 7);
6) istigazione alla violenza o all'odio online (art. 8);
7) istigazione, favoreggiamento, concorso e tentativo (art. 9).

Il capo 2 si completa con le disposizioni relative: all'entità delle sanzioni (art. 10); alle circostanze aggravanti (art.11); alla giurisdizione (art. 12); alla prescrizione (art. 13).

In realtà, si tratta di condotte in linea di massima già punite dal nostro ordinamento, ora con norme specifiche altre volte con disposizioni ricavabili all'interno del codice penale, che vanno, tutt'al più, adeguate alle indicazioni della direttiva; non mancano, sotto altri profili, aspetti problematici che rendono difficoltoso il recepimento della direttiva come, ad esempio, nel caso delle "molestie online"[4]. Solo in tali casi, potrebbe pervenirsi all'idea di introdurre altre fattispecie di reato; ma, è noto, qualunque occasione è utile per un legislatore affetto, da sempre, da nomorrea legislativa – per utilizzare una formula di carrariana memoria[5] – per "arricchire" l'ordinamento di nuove figure criminose. Occorre evitare, però, la tentazione di implementare, ulteriormente, il sistema penalistico con una serie di "nuovi" tipi criminosi per fatti in verità già sanzionati, laddove lo sforzo del legislatore dovrebbe indirizzarsi sulle varie misure funzionali ad assicurare reale protezione alle vittime di violenza. Il legislatore deve prendere atto che

penale dell'ambiente, che sostituisce le direttive 2008/99/CE e 2009/123/CE del Parlamento europeo e del Consiglio dell'11 aprile 2024) il concetto di "intenzionalità" racchiude anche il "nostro" dolo eventuale. Si stabilisce, infatti, che: "l'"intenzione" potrebbe essere intesa come intenzione diretta a provocare il decesso di una persona o potrebbe comprendere anche una situazione in cui l'autore del reato, nonostante non volesse provocare il decesso di una persona, accetti comunque la probabilità di provocarlo, e agisca, o si astenga dall'agire, volontariamente e in violazione di un particolare obbligo, causando pertanto il decesso di una persona".

[4] V. *infra* par. 6.

[5] F. CARRARA, *Un nuovo delitto*, in *Opuscoli di diritto criminale,* 3 ed., Prato, 1889, IV, p. 522.

la mera risposta penalistica da sola non risolve il problema come, del resto, dimostra il dato empirico nell'evidenziare un fenomeno in continua crescita[6] e, conseguentemente, attivarsi per assicurare una risposta di più ampio respiro che ruoti, essenzialmente, su meccanismi preventivi[7]; e ciò ancora non basta. Il rischio, da evitare, è quello di rimpinguare la "fabbrica di illusioni"[8] affidando all'intervento repressivo compiti che da solo non è in grado di risolvere; non v'è alcun dubbio che il diritto penale debba svolgere la sua parte ma non può essere caricato di aspettative la cui soluzione richiede risposte di natura multiagenziale che vede impegnati tutti gli attori sociali.

Da un punto di vista metodologico, verranno evidenziate alcune caratteristiche – senza riproporre considerazioni già svolte (per evitare il rischio di inutile ripetitività) – delle fattispecie già presenti nel sistema per valutare il grado di soddisfazione delle "richieste" sovranazionali di cui alla direttiva 2024/1385.

Quest'ultima, va pure segnalato, presenta molteplici passaggi che rendono la comprensione del testo alquanto complessa con conseguenti difficoltà attuative; si pensi, ad esempio, alle disposizioni di cui all'art. 7 in tema di molestie online per il riferimento ai comportamenti minacciosi.

Il recepimento della direttiva, da altro punto di vista, potrebbe rappresentare un'opportunità per il legislatore interno per operare degli "aggiustamenti" del dato normativo esistente, intervenendo sulle questioni problematiche evidenziate dal dibattito scientifico e dall'applicazione giurisprudenziale. In altri termini, le singole fattispecie incriminatrici – dopo anni di applicazione – hanno evidenziato alcune criticità che potrebbero essere risolte con interventi di *maquillage* funzionali al raggiungimento di quell'effettività della risposta statuale che il settore lamenta e che rappresenta, a ben vedere, la connotazione di fondo non solo della direttiva ma di ogni intervento normativo connotato da razionalità politico-criminale.

[6] Si vedano alcuni dati sul sito *https://www.salute.gov.it.*

[7] Si vedano, ad esempio, le indicazioni di cui ai considerando nn. 1, 59, 73, 74, 78, 86 e il capo V, solo per i riferimenti alla prevenzione.

[8] E. MUSCO, *L'illusione penalistica*, Milano, 2004, p. 125.

2. Le singole figure criminose "delineate" dalla direttiva: le mutilazioni genitali femminili (art. 3)

La direttiva obbliga i vari Stati ad incriminare i fatti concernenti le mutilazioni genitali femminili cercando di arginare un fenomeno di estrema diffusione, che genera conseguenze gravissime sulla salute fisica e psichica della persona[9].

L'art. 3 della direttiva stabilisce, infatti, che siano punite come reato le condotte concernenti:

a) "l'escissione, l'infibulazione o altra mutilazione della totalità o di parte delle grandi labbra o delle piccole labbra vaginali o del clitoride;

b) il costringere o l'indurre una donna, ragazza o bambina a subire uno degli atti di cui alla lettera a)".

Si tratta, come si anticipava, di comportamenti già sanzionati dall'ordinamento interno attraverso l'art. 583-*bis*; la disciplina di settore si completa con le disposizioni dell'art. 583-*ter* c.p. che prevede la pena accessoria per l'esercente una professione sanitaria per i fatti di

[9] Secondo il World Health Organization, disponibile su *https://www.who.int*, (5 febbraio 2024), più di 230 milioni di donne viventi oggi hanno subito mutilazioni genitali femminili (MGF) nei 30 paesi dell'Africa, del Medio Oriente e dell'Asia in cui viene utilizzata la pratica. Lo stesso organismo distingue tra conseguenze a breve (forte dolore, emorragia, infiammazione dei tessuti genitali, febbre, infezioni come il tetano, problemi urinari e di guarigione, lesioni dei tessuti genitali limitrofi, morte) e a lungo termine (problemi urinari, minzione dolorosa, infezioni delle vie urinarie); problemi vaginali (leucorrea, prurito, vaginosi batterica e altre infezioni); problemi mestruali (mestruazioni dolorose, passaggio difficile del sangue mestruale, ecc.); tessuto cicatriziale e cheloide; problemi sessuali (rapporti dolorosi, riduzione della soddisfazione, ecc.); aumento del rischio di complicanze nel parto (parto difficile, emorragia, taglio cesareo, necessità di rianimazione del bambino, ecc.) e mortalità neonatale; disturbi psicologici (depressione, ansia, disturbo da stress post-traumatico, bassa autostima, ecc.). Secondo il Parlamento europeo, *Mutilazioni genitali femminili: dove e perché vengono ancora praticate*, disponibile su *https://www.europarl.europa.eu* (11 febbraio 2020), sebbene sia internazionalmente riconosciuta come violazione dei diritti umani, si calcola che siano circa 68 milioni le ragazze in tutto il mondo che rischiano di subire questa pratica prima del 2030.

cui all'art. 583-*bis* c.p.; entrambe le norme sono state introdotte dall'art. 6, co. 1, Legge n. 7/2006[10].

L'art. 583-*bis* c.p. è strutturato in due distinte fattispecie incriminatrici: le mutilazioni genitali femminili (comma 1) e le lesioni agli organi genitali femminili (comma 2).

La figura criminosa di cui al primo comma punisce la "mutilazione degli organi genitali femminili" (primo alinea) specificando (secondo alinea) che per mutilazione degli organi genitali femminili si intendono "la clitoridectomia, l'escissione e l'infibulazione e qualsiasi altra pratica che cagioni effetti dello stesso tipo".

La tutela approntata dalla fattispecie di cui all'art. 583-*bis* c.p. – anche sotto il profilo sanzionatorio[11] – risulta più ampia di quella ipotizzata dalla direttiva e ciò per molteplici ragioni che possono essere così sintetizzate:

a) per la previsione incriminatrice non solo dell'escissione, dell'infibulazione o di altra mutilazione della totalità o di parte delle grandi labbra o delle piccole labbra vaginali o del clitoride (come richiesto dalla lett. a dell'art. 3 della direttiva) ma anche delle lesioni agli organi genitali femminili;

b) per la formulazione strutturale della fattispecie incriminatrice che si connota per essere un reato:

1) comune (anche se di solito le mutilazioni sono effettuate da specifici operatori, sanitari o non; da qui la possibilità di compartecipazione criminosa materiale o morale, in particolare dei genitori)[12], di

[10] I delitti di cui agli artt. 583-*bis* e *ter* c.p. sono stati introdotti in attuazione di molteplici atti internazionali emanati a decorrere dalla seconda metà del secolo scorso: Convenzione dei diritti del fanciullo, New York, 1989; Dichiarazione sull'eliminazione delle violenze nei confronti delle donne, ONU, 1993; Dichiarazione finale della conferenza internazionale su popolazione e sviluppo, Cairo, 1994; Dichiarazione e Piattaforma d'azione, Pechino, 1995; Dichiarazione congiunta OMS, UNICEF, UNFPA sulle mutilazioni genitali femminili, 1997; Quinta conferenza sulle donne, 2005; Risoluzione di messa la bando delle mutilazioni genitali femminili, 2012. In ambito regionale possono essere richiamate le Raccomandazioni del Consiglio d'Europa, 1998, 2000; la Risoluzione del Parlamento europeo, 2001; la Carta africana dei diritti e del benessere del fanciullo, Addis Abeba, 1990; la Dichiarazione afro-araba sui mezzi per prevenire le mutilazioni genitali femminili, 2003.

[11] V. *infra* par. 9.

[12] F. MANTOVANI, *Diritto penale. Parte speciale*, I, *Delitti contro la persona*, 8 ed.,

danno, a dolo generico (coscienza e volontà di cagionare una mutilazione in assenza di esigenze terapeutiche) a forma libera (comma 1)[13];

2) che prevede l'assenza di esigenze terapeutiche (si pensi ad interventi svolti nell'interesse della salute della persona come, ad esempio, l'asportazione tumorale o di cisti ostruttive) quale presupposto negativo della condotta (da cui discende la legittimità – con esclusione della tipicità del fatto – dell'attività medico chirurgica);

3) di tipo commissivo ma anche omissivo, in presenza di un obbligo giuridico di evitare l'evento (art. 40 co. 2 c.p.), come nel caso della madre che rimane inerte di fronte all'iniziativa del padre di sottoporre a mutilazione la figlia[14];

4) che individua l'oggetto materiale della condotta negli organi genitali femminili esterni (grandi e piccole labbra, prepuzio del clitoride, vestibolo della vagina, bulbi del vestibolo, ghiandole vestibolari) e non interni (gonadi e vie genitali interne quali tube uterine e utero)[15];

5) di tipo plurioffensivo, funzionale a salvaguardare l'incolumità individuale costituzionalmente prevista (art. 32, venendo in rilievo l'integrità anatomica e funzionalità sessuale), la dignità della donna (offesa per ragioni di discriminazioni sessuali) e l'integrità allo sviluppo fisico-psichico del minore (art. 2 Cost., 13 e 29 della Convenzione dei diritti del fanciullo);

Padova, 2022, p. 163.

[13] Per maggiori approfondimenti cfr. G. FORNASARI, *Mutilazioni genitali femminili e multiculturalismo: premesse per un discorso giuspenalistico*, in A. BERNARDI, B. PASTORE, A. PUGGIOTTO (a cura di), *Legalità penale e crisi del diritto oggi*, Milano, 2008, p. 179 ss.; F. BASILE, *Commento all'art. 583-bis*, in E. DOLCINI, G.L. GATTA, (a cura di), *Codice penale commentato*, 5ed, Milano, 2021, III, pp. 1019-1036; ID., *Società multiculturali, immigrazione e reati culturalmente motivati (comprese le mutilazioni genitali femminili)*, in *Rivista italiana di diritto e procedura penale*, 2007, n. 4, p. 1296-1345; ID., *La nuova incriminazione delle pratiche di mutilazione degli organi genitali femminili: Legge 9 gennaio n. 7*, in *Diritto penale e processo*, 2006, n. 6, pp. 678-691.

[14] F. MANTOVANI, *op.cit.*, p. 164.

[15] *Ibidem*, p. 164; sulle motivazioni "culturali" cfr. tra gli altri, L. BELLUCCI, *Consuetudine, diritti e immigrazione. La pratica tradizionale dell'escissione nell'esperienza francese*, Milano, 2012, p. 3 ss., in part. p. 77 ss.; A. BERNARDI, *Il "fattore culturale" nel sistema penale*, Torino, 2010, p. 3 ss.; C. DE MAGLIE, *I reati culturalmente motivati. Ideologie e modelli penali*, Pisa, 2010, p. 30 ss.; F. BASILE, *Immigrazione e reati culturalmente motivati. Il diritto penale nelle società multiculturali*, Milano, 2010, p. 41 ss.

6) in cui l'evento è dato dalla mutilazione, permanente (anche se la funzionalità sessuale può essere ripristinata con successivi interventi chirurgici) che deve comportare una diminuzione funzionale e anatomica dell'apparato genitale[16];

c) per la presenza della locuzione "qualsiasi altra pratica che cagioni effetti dello stesso tipo": tale formula comporta un'estensione della tutela ben oltre le previsioni dell'art. 3 della direttiva trattandosi di una formula di chiusura che abbraccia qualunque fatto, diverso da quelli elencati in precedenza, funzionale a menomare gli organi femminili e, quindi, idoneo a comprendere tutte le tipologie di mutilazioni previste dal Tipo 4 della classificazione del WHO[17] (si pensi ad esempio, alla cauterizzazione attraverso bruciatura del clitoride). In sintesi: la locuzione amplia le possibilità di configurare la fattispecie, perché consente l'incriminazione di condotte alternative a quelle elencate nei casi precedenti;

d) per la presenza della seconda figura delittuosa che, sanzionando la lesione degli organi genitali femminili, permette di estendere la tutela della donna svolgendo una funzione sussidiaria e ponendosi in rapporto di incompatibilità con la fattispecie di cui al co. 1. Il tipo criminoso in parola pur presentando le stesse caratteristiche della figu-

[16] F. MANTOVANI, *op.cit.*, p. 164.

[17] Il World Health Organization classifica le mutilazioni genitali femminili in quattro tipi principali. Tipo 1: si tratta della rimozione parziale o totale del glande clitorideo (la parte esterna e visibile del clitoride, che è una parte sensibile dei genitali femminili) e/o del prepuzio/cappuccio clitorideo (la piega della pelle che circonda il glande clitorideo). Tipo 2: si tratta della rimozione parziale o totale del glande clitorideo e delle piccole labbra (le pieghe interne della vulva), con o senza rimozione delle grandi labbra (le pieghe esterne della pelle della vulva). Tipo 3: conosciuta anche come infibulazione, è il restringimento dell'apertura vaginale attraverso la creazione di un sigillo di copertura. La tenuta si forma tagliando e riposizionando le piccole labbra, o grandi labbra, a volte attraverso cuciture, con o senza rimozione del prepuzio clitorideo/cappuccio clitorideo e del glande. Tipo 4: ciò include tutte le altre procedure dannose per i genitali femminili per scopi non medici, ad esempio puntura, piercing, incisione, raschiamento e cauterizzazione dell'area genitale. Nel 2008, l'Assemblea Mondiale della Sanità ha approvato la risoluzione WHA61.16 sull'eliminazione delle MGF, sottolineando la necessità di un'azione concertata in tutti i settori: salute, istruzione, finanza, giustizia e affari delle donne.

ra precedente in relazione ad oggetto materiale, al bene giuridico, all'offesa, al soggetto passivo, si differenzia:

1) per la condotta, consistente nel menomare gli organi genitali femminili con modalità diverse da quelle indicate nel co. 1 (lesioni, cioè, che finiscono per menomare la funzionalità sessuale ma non in modo permanente come forare o trapassare il clitoride, poiché "nella permanenza e nella non permanenza della menomazione sembra rinvenibile l'unico criterio per la non facile individuazione della differenza tra i due reati"[18]; trattandosi di interventi non demolitori e, dunque, con effetti rimovibili[19], risulta spiegata la pena minore per il delitto di lesione rispetto a quello di mutilazione;

2) per l'evento consistente nella malattia del corpo o della mente (con esclusione degli effetti permanenti) come nell'ipotesi di emorragie o alterazioni dell'apparato genitale poi guariti;

3) per il dolo specifico caratterizzato dal fine di menomare le funzioni sessuali;

4) per la perfezione del reato che si verifica nel tempo e nel luogo dell'insorgenza della malattia.

Il delitto di mutilazione (co. 1) è un reato a consumazione istantanea ad effetti permanenti: la consumazione si verifica nel momento in cui si produce la mutilazione. Il delitto di lesione, invece, a consumazione istantanea ad effetti solo eventualmente permanenti si verifica con l'insorgenza della malattia; il tentativo risulta ammissibile con conseguente anticipazione dell'intervento sanzionatorio[20] (ed anche sotto questo profilo la norma appare in grado di assolvere quanto richiesto dalla direttiva).

In linea con quanto in precedenza anticipato (della tutela più ampia prevista dalle fattispecie di cui all'art. 583-*bis* e *ter* c.p. rispetto a quanto previsto dalla direttiva comunitaria) va rimarcato, come limpidamente sostenuto, che l'eventuale consenso dell'avente diritto, per i limiti previsti dall'art. 5 c.c, non scrimina:

[18] F. MANTOVANI, *op. cit.*, p. 165.

[19] S. SEMINARA, *I delitti contro la persona*, in R. BARTOLI, M. PELISSERO, S. SEMINARA (a cura di), *Diritto penale. Lineamenti di parte speciale*, Torino, 2021, pp. 3-216.

[20] F. BASILE, sub *art. 583*-bis, cit., p. 1030; per ulteriori considerazioni in rapporto a quanto previsto dalla direttiva v. *infra* par. 8.

1) le mutilazioni (art. 583-*bis* co. 1 c.p.) in quanto comportano una menomazione permanente dell'integrità fisica;

2) le lesioni di cui all'art. 583-*bis* co. 2 c.p. poiché trattasi di menomazione delle funzioni sessuali – che seppur non permanente – sono contrarie all'ordine pubblico e ai principi costituzionali della dignità della persona e della non discriminazione.

Allo stesso modo non scrimina l'esercizio di un diritto perché:

1) alcuna legge prevede il diritto di praticare le mutilazioni;

2) tali pratiche non possono considerarsi neppure esercizio del diritto dei genitori di istruire ed educare i figli secondo le proprie convinzioni religiose (si tratta di pratiche appartenenti alla categoria culturale-tribale prive di sentimento religioso)[21].

Le fattispecie codicistiche appena richiamate non contengono disposizioni rapportabili alla lett. b) dell'art. 3 della direttiva ("il costringere o l'indurre una donna, ragazza o bambina a subire uno degli atti di cui alla lettera a))".

Per la "costrizione" potrebbe farsi riferimento all'art. 610 c.p.; per l'induzione, invece, manca nel nostro ordinamento uno specifico riferimento o qualche norma sulla falsariga della fattispecie relativa alla circonvenzione di persone incapace (quest'ultima è strutturata in termini da non poter essere utilizzata in tema di mutilazioni o lesioni genitali).

Il legislatore potrebbe aggiungere, allora, all'art. 583-*bis* c.p., un comma (dopo il secondo) del seguente tenore:

"*Alla stessa pena (o alla pena diminuita fino a…oppure da…a…) soggiace chi, fuori del caso di concorso, costringe o induce taluno a subire i fatti di cui al comma 1; alla stessa pena (o alla pena diminuita fino a…oppure da …a…) chi, fuori del caso di concorso, costringe o induce taluno a subire i fatti di cui al comma 2*".

In sede di modifica dell'art. 583-*bis* c.p. il legislatore potrebbe intervenire anche sul co. 2 ed in particolare eliminando la locuzione "al fine di menomare le funzioni sessuali" e con essa trasformando il dolo specifico in dolo generico. A ben vedere l'attuale conformazione del dolo (specifico)[22] finisce per vanificare la portata della fattispecie in

[21] F. MANTOVANI, *op.cit.*, p. 166.

[22] Sulle perplessità ingenerate dal dolo specifico "certamente incongruo, laddove

tutti i casi in cui la lesione non è finalizzata a "menomare le funzioni sessuali" ma si lega ad altri fattori (religiosi, culturali, discriminatori, ecc.). Non minore difficoltà si verificano sul piano dell'accertamento; paradigmatico è il caso affrontato dalla giurisprudenza di merito che non ha ritenuto sussistente il dolo specifico perché i fatti erano da collocarsi all'interno delle finalità di realizzare una pratica simbolica diretta a soddisfare una "funzione di umanizzazione" (riconoscimento di un individuo come uomo o come donna all'interno della comunità degli umani), una "funzione identitaria" (sancire il vincolo di appartenenza ad una specifica comunità garantendo la possibilità di vivere in libertà all'interno di tale gruppo) e, infine, una "funzione di purificazione" (garantita dalla fuoriuscita di qualche goccia di sangue)[23].

3. *Il matrimonio forzato (art. 4)*

L'art. 4 della direttiva rubricato "matrimonio forzato" stabilisce che:

"Gli Stati membri provvedono a che siano punite come reato le seguenti condotte intenzionali:

a) costringere un adulto o un minore a contrarre matrimonio;

b) attirare un adulto o un minore nel territorio di un paese diverso da quello in cui risiede allo scopo di costringerlo a contrarre matrimonio".

Non diversamente dalle mutilazioni genitali femminili anche queste ipotesi sono già disciplinate – seppure parzialmente – dal c.p. all'art. 558-*bis* introdotto dall'art. 7, co. 1, Legge n. 69/2019 (c.d. "Codice Rosso"), conformandosi il legislatore all'obbligo di incriminazione previsto dall'art. 37 par. 1 della Convenzione del Consiglio

si consideri come gli interventi in esame obbediscano alle più svariate finalità", cfr. S. SEMINARA, *op.cit.*, p. 96.

[23] Cfr. Corte d'Appello di Venezia, 23 novembre 2012 (dep. 21 febbraio 2013), n. 1485, disponibile su *https://dpc-rivista-trimestrale.criminaljusticenetwork.eu*, con commento di F. BASILE, *Il reato di "pratiche di mutilazione degli organi genitali femminili" alla prova della giurisprudenza: un commento alla prima (e finora unica) applicazione giurisprudenziale dell'art. 583 bis c.p.*, *ivi*, 2013, 4, pp. 311-324.

d'Europa sulla prevenzione e il contrasto alla violenza contro le donne e della violenza domestica (cd. Convenzione di Istanbul).

In via di estrema sintesi, va effettuato qualche riferimento alla figura criminosa – protesa a salvaguardare la libertà di autodeterminazione dell'individuo con particolare riguardo alla libertà di compiere liberamente le scelte attinenti alla propria sfera affettiva e sessuale[24] – solo al fine del coordinamento con le indicazioni del legislatore comunitario tenendo presente che la norma codicistica:

1) ha una portata più ampia (sotto questo profilo va evidenziato il dato che accanto al "matrimonio" viene richiamata, alternativamente, l'unione civile);

2) prevede ipotesi di induzione approfittando di determinate condizioni della vittima (vulnerabilità o di inferiorità psichica o di necessità di una persona, con abuso delle relazioni familiari, domestiche, lavorative o dell'autorità derivante dall'affidamento della persona per ragioni di cura, istruzione o educazione, vigilanza o custodia);

3) all'opposto, non disciplina le ipotesi di cui alla lett. b) dell'art. 4 della direttiva.

La fattispecie di cui all'art. 558-*bis* c.p. – collocata nell'ambito dei delitti contro il matrimonio[25] viene fatta rientrare nell'ampia categoria dei c.d. "reati culturalmente orientati"[26] – risulta strutturata nei termini di reato comune (il co. 2 richiede, però, una relazione qualificata e, pertanto, reato proprio[27]), a dolo generico (nel secondo comma, con la conoscenza della condizione di vulnerabilità, inferiorità psichica o necessità della vittima), articolata su due figure delittuose rapportabili alla categoria dei reati di evento a forma vincolata.

La figura delittuosa disciplinata al co. 1 dell'art. 558-*bis* c.p. utiliz-

[24] S. BERNARDI, sub *art. 558*-bis, in E. DOLCINI, G.L.GATTA (a cura di), *Codice penale commentato*, 5ed., Milano, 2021, III, pp. 642-652; A. VALSECCHI, *"Codice Rosso" e diritto penale sostanziale*, in *Diritto penale e processo*, 2020, pp. 168-174.

[25] In senso critico verso tale sistemazione G. PEPE, *I matrimoni forzati presto previsti come reato anche in Italia?*, in *Diritto penale contemporaneo. Archivio 2010-2019*, 2019, pp. 1-2; per una collocazione nella sezione I, capo III, titolo XII, tra i delitti contro la personalità individuale cfr. S. BERNARDI, *op.cit.,* p. 644.

[26] G. PEPE *op. cit.*, p. 644.

[27] A.M. BELTRAME, sub *art. 558*-bis *c.p.*, in G. FORTI, S. RIONDATO, S. SEMINARA, (a cura di), *Commentario breve al codice penale*, 7 ed., Padova, 2024, p. 2077-2081.

za la locuzione "con violenza o minaccia, costringe una persona" mentre la direttiva prevede solo il termine "costringe" specificando un adulto o un minore. In relazione a quest'ultimo aspetto, la disposizione codicistica già recepisce quanto richiesto dalla direttiva in considerazione del fatto che la "persona" è concetto comprensivo anche dell'adulto o del minore.

Ugualmente può dirsi per la costrizione, che nell'art. 558-*bis* c.p. viene precisata con i termini "violenza" o "minaccia" atteso che difficilmente può aversi una costrizione senza qualche forma di violenza o minaccia. Del resto, il concetto di costrizione si concretizza nel forzare o nell'obbligare qualcuno, con la forza o con altro mezzo, a fare qualcosa che sia contraria alla volontà o comunque non spontanea[28]; inoltre, i concetti di violenza e di minaccia (che hanno una collocazione normativa nell'art. 610 e nell'art. 612 c.p.) vantano una marcata applicazione giurisprudenziale che fa rientrare nel loro ambito qualunque atto in grado di "condizionare" o "intimidire" la volontà del destinatario.

Resta fuori dalla portata dell'art. 558-*bis* c.p., come si anticipava, la lett. b) dell'art. 4 della direttiva vale a dire il fatto di "attirare" una persona in un altro paese "allo scopo di costringerlo a contrarre matrimonio".

In proposito, non sono mancate voci che si sono poste l'interrogativo se siano punibili a titolo di tentativo le ipotesi consistenti nell'attirare intenzionalmente con l'inganno un adulto o un bambino sul territorio di un paese o di uno Stato diverso da quello in cui risiede, allo scopo di costringerlo a contrarre matrimonio; a tale quesito è stata data una condivisibile risposta negativa poiché una simile condotta tutt'al più può costituire un atto preparatorio del delitto di cui all'art. 558-*bis* c.p.[29]. Affinché possano sussistere gli estremi del tentativo è necessario, invece, che l'agente intraprenda l'esecuzione del delitto in questione, "ossia, trattandosi di fattispecie a forma vincolata, ponga in essere atti corrispondenti allo specifico modello di comportamento descritto nella norma incriminatrice"[30].

[28] Così il *Vocabolario on line* consultabile sul sito *https://www.treccani.it.*

[29] S. BERNARDI, *op,cit.*, p. 648.

[30] *Ibidem.*

Discende da ciò che per dare copertura incriminatrice ad una tale indicazione significa formulare una fattispecie che sia ancorata:

1) alla condotta di "attirare" (dal significato semantico alquanto ampio) ossia, affascinare, sedurre, allettare, intrigare, invitare, solleticare, adescare un adulto o minore. Il termine oscilla, in ultima analisi, tra le lusinghe e le minacce oppure tra gli artifizi e i raggiri;

2) compiuta con dolo specifico ("allo scopo" di "costringerlo a contrarre matrimonio");

3) di pericolo (perché la finalità è quella di contrarre un matrimonio che può anche non verificarsi nonostante la vittima abbia lasciato il paese di residenza).

Al tal fine potrebbe formularsi un aggravamento di pena qualora il matrimonio o l'unione civile[31] vengano celebrati secondo lo schema del reato aggravato dall'evento.

Va evidenziato, infine, che, per evitare i c.d. matrimoni precoci, il legislatore ha previsto all'art. 558-*bis* c.p. due circostanze aggravanti speciali: la prima (co. 3) ad efficacia comune applicabile nei casi in cui a venire coinvolto sia un minore degli anni diciotto; la seconda, ad effetto speciale (reclusione da due a sette anni), nell'ipotesi in cui il fatto sia commesso in danno di un minore degli anni quattordici.

In considerazione delle riflessioni sinora svolte si potrebbe aggiungere un comma all'art. 558-*bis* c.p. del seguente tenore:

"*Alla stessa pena (di cui al comma 1 oppure ad una pena inferiore) è punito chiunque attira una persona nel territorio di un paese diverso da quello in cui risiede allo scopo di costringerlo a contrarre matrimonio o unione civile; la pena è aumentata se la persona è minorenne; la pena è altresì aumentata se il matrimonio e l'unione civile vengono celebrati*".

[31] Il riferimento all'unione civile va in linea con il considerando n. 16 per un duplice ordine di ragioni: a) perché al pari del matrimonio forzato "è una forma di violenza che comporta gravi violazioni dei diritti fondamentali e, in particolare, dei diritti delle donne e delle ragazze all'integrità fisica, alla libertà, all'autonomia, alla salute fisica e mentale, alla salute sessuale e riproduttiva, all'istruzione e alla vita privata"; b) e perché la direttiva lascia impregiudicate le definizioni di "matrimonio" previste dal diritto nazionale o internazionale.

4. *La condivisione non consensuale di materiale intimo o manipolato (art. 5)*

L'art. 5 della direttiva[32] prevede che gli Stati membri puniscano la condivisione non consensuale di materiale intimo o manipolato.

Si tratta di fatti già puniti dal nostro ordinamento, in modo specifico, attraverso l'art. 612-*ter* c.p. (introdotto dall'art. 10 co. 1 della Legge n. 69/2019) oltre ad una cospicua serie di disposizioni che, seppure indirettamente, possono arricchire la risposta statuale (es. artt. 595, co. 3, c.p., 580 c.p., artt. 612-*bis*, 615-*bis*, 617-*septies* c.p., art. 167 del d.lgs. n. 196/2003, c.d. Codice della privacy).

Sin da ora anticipiamo che appare necessario l'intervento del legislatore sotto un duplice profilo:

1) recepimento di alcuni aspetti espressamente richiesti dalla direttiva, e

2) "aggiustamenti" delle figure criminose delineate dall'art. 612-*ter* c.p.

Gli apprezzabili intenti del legislatore interno di contrastare fatti che possono avere ricadute devastanti sulla vittima si scontrano, come si vedrà nel prosieguo, con i non pochi profili problematici che la nuova fattispecie incriminatrice di cui all'art. 612-*ter* c.p. manifesta, quale naturale effetto di una norma emanata, frettolosamente, sull'impulsività del momento.

[32] La norma così dispone: "1. Gli Stati membri provvedono a che siano punite come reato le condotte intenzionali seguenti: a) rendere accessibile al pubblico, tramite Tecnologie dell'Informazione e della Comunicazione (TIC), immagini, video o analogo materiale ritraente atti sessualmente espliciti o le parti intime di una persona senza il consenso di tale persona qualora tali condotte possano arrecare un danno grave a dette persone; b) produrre, manipolare o alterare e successivamente rendere accessibile al pubblico, tramite TIC, immagini, video o analogo materiale in modo da far credere che una persona partecipi ad atti sessualmente espliciti, senza il consenso della persona interessata, qualora tali condotte possano arrecare un danno grave a tale persona; c) minacciare i comportamenti di cui alle lettere a) o b) al fine di costringere una persona a compiere un determinato atto, acconsentirvi o astenersi dallo stesso. 2. Il paragrafo 1, lettere a) e b), del presente articolo, non pregiudica l'obbligo di rispettare i diritti, le libertà e i principi sanciti dall'articolo 6 TUE e si applica fatti salvi i principi fondamentali connessi alla libertà di espressione e di informazione e alla libertà delle arti e delle scienze, quali recepiti nel diritto dell'Unione o nazionale".

Comune si presenta la *ratio*: sia la fattispecie incriminatrice di cui all'art. 612-*ter* c.p. che la direttiva sono supportate dalle volontà del legislatore di evitare fatti "estremamente dannosi per la vittima"[33] e cercare di arginare un fenomeno in continua espansione che genera conseguenze psicofisiche gravissime sulla vittima (solitamente donna, ma non solo) e, in alcuni casi, porta addirittura al suicidio.

In ordine all'oggettività giuridica tutelata va segnalata la portata plurioffensiva della fattispecie incriminatrice (art. 612-*ter* c.p.), essendo destinata a salvaguardare non solo il complesso delle condizioni che si riassumono nello stato di tranquillità individuale, in quanto presupposto per il normale esercizio dei diritti di libertà, ma anche altri interessi (ad esempio, la reputazione, l'onore, l'immagine, la privacy); non diversa oggettività giuridica si rinviene nei diversi "considerando" della direttiva tutti protesi a contrastare le varie forme di violenza.

La nuova disposizione, utilizzando il pronome indefinito "chiunque" (co. 1) o "chi" (co. 2), descrive un reato comune; mentre la circostanza aggravante (comune) prevista dal co. 3 (primo alinea) delinea un reato proprio per l'uso del sostantivo "coniuge"; il secondo alinea della stessa disposizione, con il riferimento alla "persona" "che è o è stata legata da relazione affettiva alla persona offesa" [34], può essere collocato nel contesto dei c.d. reati di mano propria[35] o ad attuazione personale[36] proprio per la specifica qualità richiesta dalla norma che circoscrive, così, la schiera dei potenziali autori. Sotto questo profilo la fattispecie di cui all'art. 612-*ter* c.p. può dirsi in linea con le indicazioni di cui all'art. 5 della direttiva.

Soggetto passivo è, in primo luogo, la persona ripresa o fotografata che non presta il proprio consenso alla diffusione o pubblicazione delle immagini o dei video (co. 1 e 2); poi, la persona legata da relazione affettiva all'agente (co. 3); e, infine, la persona in condizione di inferiorità fisica o psichica e la donna in stato di gravidanza (co. 4). Soggetto passivo è solitamente la donna ma ciò non esclude che anche al-

[33] Considerando 19 della direttiva (UE) 2024/1385, *cit.*

[34] Sulle difficoltà nell'accertamento della locuzione v. *infra* par. 5.

[35] Su questa categoria nella manualistica corrente cfr. C. FIORE, S.FIORE, *Diritto penale. Parte generale*, 6ed., Torino, 2020, p. 190.

[36] Cfr. F. MANTOVANI, *Diritto penale. Parte generale*, 10ed., Padova, 2017, p. 109.

tri soggetti (uomo, gay, bisessuali, transessuali, *graysexual*, pansessuali, ecc.) possano essere vittime di divulgazione di materiali a contenuto sessualmente esplicito. Entrambe le disposizioni utilizzano il termine "persona" e, dunque, offrono copertura a tutti i soggetti coinvolti; l'art. 612-*ter* c.p. presenta per i richiami ai co. 3 e, soprattutto, 4 un ampliamento della tutela rispetto a quanto previso dal legislatore comunitario.

La direttiva prevede di punire le condotte funzionali a "rendere accessibile al pubblico, tramite Tecnologie dell'Informazione e della Comunicazione (TIC)", immagini, video o analogo materiale ritraente atti sessualmente espliciti; l'art. 612-*ter* c.p. prevede la medesima copertura con la circostanza aggravante comune descritta al co. 3: "se i fatti sono commessi attraverso strumenti informatici o telematici"[37].

Ugualmente può dirsi per quanto concerne l'assenza di consenso; l'art. 5 della direttiva e l'art. 612-*ter* c.p. stabiliscono, infatti, che sia punita la divulgazione ("senza il consenso" della persona interessata) avente ad oggetto "immagini, video o analogo materiale ritraente atti sessualmente espliciti o le parti intime di una persona senza il consenso".

Diversamente si verifica, invece, con la locuzione "immagini, video o analogo materiale ritraente atti sessualmente espliciti o le parti intime di una persona" utilizzata in sede comunitaria, laddove l'art. 612-*ter* c.p. adopera l'inciso "immagini o video a contenuto sessualmente esplicito". Entrambe le formule hanno in comune il riferimento alle "immagini" e ai "video"; la direttiva aggiunge come formula di chiusura l'inciso "analogo materiale". Tale locuzione ha il merito di ampliare la portata del tipo criminoso fino ad abbracciare tutto ciò che non rientra nei concetti di "immagine" e di "video"; l'inserimento nell'art. 612-*ter* c.p. della locuzione "o analogo materiale" (oppure una formula equipollente) comporterebbe una migliore descrizione della condotta evitando operazioni interpretative funzionali a far rientrare

[37]In una eventuale operazione di aggiornamento dell'art. 612-*ter* il legislatore potrebbe sostituire la locuzione "strumenti informatici o telematici" (in qualunque altra disposizione compare) con quella della direttiva "tecnologie dell'informazione e della comunicazione" avendo portata più ampia in quanto comprensiva di strumenti come telefono, Internet, computer, Reti, radio e televisione, nonché servizi come videoconferenza, formazione a distanza e banche dati.

nel concetto di "immagini" o "video", ad esempio, anche le fotografie[38]. Del resto, il considerando n. 19 reca: "il pertinente reato definito nella presente direttiva dovrebbe riguardare tutti i tipi di tale materiale, ad esempio immagini, fotografie e video, comprese le immagini sessualizzate e i clip video e audio"[39].

La direttiva presenta, ancora, l'inciso "o le parti intime di una persona" posta in alternativa (per la presenza della congiunzione 'o') agli "atti sessualmente espliciti". L'art. 612-*ter* c.p. utilizza la formula "contenuto sessualmente esplicito"; si tratta di una formula alquanto indeterminata che riesce a dire tutto e il suo contrario ed è fonte di notevoli difficoltà interpretative: ad esempio l'immagine della vittima che gira per casa nuda o mentre fa la doccia è immagine a contenuto sessualmente esplicito? In una prospettiva di riforma, proprio al fine di dotare – sul punto – la fattispecie incriminatrice di maggiore precisione è stato ipotizzato (anche dopo un'analisi comparata della normativa), l'inserimento di un comma aggiuntivo che stabilisca cosa s'intende per "contenuto sessualmente esplicito" non diversamente da come si è

[38] Il "video" indica il dispositivo elettronico di cui ci si serve, a vari fini, per analizzare, elaborare, registrare ed eventualmente trasmettere immagini, fisse o in movimento e accompagnate o meno da suoni. In ordine alle "immagini" va segnalato, preliminarmente, che il legislatore non ha utilizzato il termine "fotografia" né tanto meno l'ha affiancato al sostantivo "immagini" (ad esempio immagini fotografiche), con la conseguenza che, *prima facie*, la disposizione escluderebbe le fotografie. Una tale conclusione appare poco sostenibile perché non si comprende per quali ragioni solo le immagini, a differenza delle fotografie, integrerebbero la fattispecie incriminatrice in considerazione del fatto che entrambe hanno la stessa capacità di immagazzinare un dato oggetto o, come nel caso di specie, la persona. Più correttamente il termine "immagine" racchiude anche la fotografia; il fatto che il legislatore non abbia usato il termine "foto" ma quello di "immagine" evidentemente ha voluto riconoscere alla norma la precisa capacità di ampliare la portata della fattispecie incriminatrice. Del resto, escludere dalla figura delittuosa le fotografie che ritraggono parti intime di una persona non pare sostenibile sul piano politico-criminale. Una conferma si ricava da un punto di vista linguistico: l'immagine viene descritta in termini di figura esteriore percepita con la vista oppure di rappresentazione grafica, fotografica o plastica di cosa o di persona, reale o fantastica; in proposito si v. E. LO MONTE, *Art. 613-ter c.p. "Diffusione illecita di immagini o video sessualmente espliciti". Tra buoni propositi, denegato "diritto all'oblio" e morti "social",* Torino, 2021, p. 72.

[39] Conclusioni queste a cui si era pervenuti precedentemente nell'analisi dell'art. 612-*ter* c.p.; si v. in proposito, E. LO MONTE, *op.cit.*, p. 73 ss. e p. 167 ss.

verificato, ad esempio, con la fattispecie di cui all'art. 603-*bis* c.p.[40]. Occorre, in sostanza, fornire strumenti dai quali far discendere delle linee guida che diano all'ambiguo costrutto sintattico un itinerario lungo sul quale fondare una prassi costante priva di ondeggiamenti funzionali a chiarire situazioni di oggettiva incertezza del dato normativo e, dunque, evitare anfibologie applicative[41]. L'inciso "o le parti intime di una persona" rappresenta un "passo in avanti" sul piano della intellegibilità del comando perché maggiormente specificativa della norma penalistica attuale; ma ancora è poco.

La direttiva utilizza alle lett. a) e b) dell'art. 5 la formula "rendere accessibile al pubblico"; diversamente ha operato il legislatore dell'art. 612-*ter* c.p. con la formula "invia, consegna, cede, pubblica o diffonde"[42]. L'inciso adoperato dal legislatore comunitario riesce ad assorbi-

[40] Con l'accortezza, però, di non utilizzare spiegazioni più generiche del testo che si vuole chiarire come si è verificato proprio con la fattispecie in tema di "Intermediazione illecita e sfruttamento del lavoro" (art. 603-*bis*, co. 3, c.p.). In proposito E. LO MONTE, *Osservazioni sull'art. 603*-bis *c.p. di contrasto al caporalato: ancora una fattispecie enigmatica*, in A. CASTALDO, V. DE FRANCESCO, M. DEL TUFO, S. MANACORDA, L. MONACO (a cura di), *Scritti in onore di Alfonso M. Stile*, Napoli, 2013, pp. 955-968.

[41] E. LO MONTE, *Art. 612*-ter, cit., p. 103.

[42] La fattispecie incriminatrice si configura quando, in assenza del consenso delle persone rappresentate, l'agente "invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati" (co. 1 e 2). Le condotte di cui ai co. 1 e 2 hanno però un diverso presupposto che nel primo caso consiste nella realizzazione o nella sottrazione (co. 1), e nella seconda ipotesi risulta, invece, dall'aver ricevuto o (comunque) acquisito (co. 2) le immagini o i video a contenuto sessualmente esplicito.

All'interno delle condotte vietate è possibile operare una distinzione tra invio/consegna/cessione da un lato e pubblicazione/diffusione dall'altro.

I vocaboli utilizzati dal legislatore possono sembrare equipollenti e, nel linguaggio comune, vengono solitamente adoperati in modo equivalente, ma il fatto che siano stati previsti in modo alternativo (lo conferma la congiunzione "o") obbliga l'interprete alla ricerca, sebbene non semplice, di una soluzione che escluda un rapporto di sinonimia. Invio, consegna e cessione evidenziano modalità diverse che possono essere raggruppati, da un punto di vista etimologico, sotto il verbo "rivelare". Infatti, *inviare* può essere letto come "mandare a qualcuno"; *consegnare* implica il fatto di "recapitare", "portare"; *cedere* coinvolge l'azione di operare un "trasferimento". Tutti e tre i termini, come si accennava, hanno in comune il fatto di comunicare la notizia ad un ristretto numero di soggetti, verificandosi, in tal modo, un ampliamento della portata della fattispecie incriminatrice sanzionando addirittura il comportamento

re tutte le ipotesi previsti dall'art. 612-*ter* c.p. anche se quest'ultima ha il merito di accordare una maggiore tutela alla vittima perché consente di configurare il tipo criminoso anche se la "divulgazione" non è indirizzata al "pubblico" ma ad un solo soggetto; circostanza questa che non risulta coperta dalla direttiva per l'esplicito riferimento al "pubblico"[43].

Differenze si rinvengono, ancora, in tema di: a) elemento soggettivo e b) qualificazione del fatto;

a) la fattispecie di cui all'art. 612-*ter* c.p. richiede al co. 1 il semplice dolo generico [44] essendo irrilevanti le finalità perseguite dall'agente; scopi particolari perseguiti dall'agente sono richiesti, invece, dal co. 2 dell'art. 612-*ter* c.p.; invero, la formula adoperata dal legislatore "al fine di recare loro nocumento" fa sì che per l'integrazione della figura criminosa sia necessario il dolo specifico. Per cui il comportamento di colui che trasmette il file dai contenuti sessualmente espliciti senza la volontà di recare nocumento alla vittima ma solo, ad esempio, per mostrarlo agli amici non integrerà la fattispecie di reato; va da sé che la prova del dolo (specifico) presenta non poche difficoltà e finisce per svuotare le possibilità di applicazione della fattispecie;

b) il tipo criminoso disciplinato dall'art. 612-*ter* c.p. risulta strutturato nei termini di reato di pericolo astratto/presunto[45], mentre la

di chi invia anche ad una sola persona il materiale sessualmente esplicito e in qualunque modalità questo avvenga. Diversamente deve dirsi per i lemmi "pubblicazione" e "diffusione", ampiamente adoperati nel codice, anche in modo alternativo – come avviene ad esempio con l'art. 656 c.p. La "diffusione" ha un fondamento nell'art. 4, co. 1, lett. m) del Codice della privacy e individua "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione", oppure "implica una comunicazione ad un numero indeterminato di persone"; la pubblicazione (che di fatto costituisce una forma di diffusione) risulta connotata dall'utilizzo del mezzo della stampa.

[43] A conferma di quanto sostenuto nel testo va richiamato il considerando n. 18 che afferma: "Le espressioni "accessibile al pubblico" e "pubblicamente accessibile" dovrebbero rinviare al concetto di potenziale raggiungimento di un certo numero di persone".

[44] Il legislatore comunitario utilizza il termine "intenzionalmente"; sul punto si rinvia a quanto anticipato nel par. 1.

[45] Ai fini della sussistenza della fattispecie è necessario, relativamente ad evento e nesso eziologico: a) che un'immagine o un video abbia "contenuto sessualmente espli-

direttiva, richiedendo che le "condotte possano arrecare un danno grave a dette persone", ipotizza un reato di danno. Entrambe le scelte non appaiono soddisfacenti: la disposizione interna per le note questioni di rilevanza costituzionale connesse al rapporto tra pericolo presunto e principio di offensività; la norma della direttiva richiedendo il danno – in particolare "grave" – rischia di vanificare la risposta statuale alla luce della prova del danno e, ancor di più, della gravità dello stesso. Inoltre – ed è forse l'aspetto meno condivisibile della direttiva – l'inciso, per l'uso della congiunzione "qualora", può fondare l'idea che in assenza di danno grave (o in altri termini, in presenza di un danno "semplice") sia lecito rendere accessibile al pubblico il materiale sessualmente esplicito. La soluzione potrebbe essere quella di utilizzare il pericolo concreto che, seppur non privo di problemi sul terreno dell'accertamento, può contare su un ricco dibattito scientifico e su una nutrita applicazione giurisprudenziale.

In ordine alla consumazione, con riferimento all'art. 612-*ter* c.p., dai verbi utilizzati (inviare, consegnare, cedere) essendo la fattispecie strutturata nei termini di reato di pericolo astratto/presunto, discende che è sufficiente il semplice invio, consegna o cessione, con il risultato che si configura il reato anche nel caso in cui il destinatario non abbia cognizione dell'immagine o del video. Per la pubblicazione o la diffusione, invece, basta che l'agente abbia inviato ad un giornale la foto o il video. Allo stesso modo, integra il requisito della comunicazione con più persone il mero inserimento del messaggio offensivo in un sito Internet senza che vi sia l'effettiva percezione dello stesso da parte di più soggetti. La direttiva richiama le "tecnologie dell'informazione e della

cito"; b) che sia stato inviato, consegnato, ceduto, pubblicato o diffuso il materiale intimo destinato a rimanere privato; c) e che non vi sia stato il consenso della persona ritratta o rappresentata. Il giudice deve "limitarsi", pertanto, a verificare la sussistenza di questi tre elementi senza ulteriori accertamenti. Altro il giudice non è tenuto a fare; non deve, quindi, indagare se la persona ritratta abbia o meno "risentito" delle conseguenze, e se sia stata limitata la sua libertà psichica, oppure offesa la sua reputazione, l'onore, la privacy, ecc. Ugualmente può dirsi in ordine al pericolo per l'oggettività giuridica, che non viene evocato neppure attraverso qualche sinonimo e, dunque, non è elemento del tipo, con l'ulteriore conseguenza che la fattispecie incriminatrice di cui all'art. 612-*ter* c.p. risulta strutturata secondo le connotazioni del pericolo astratto/presunto.

comunicazione" e dunque l'uso del web, deve ritenersi che il tempo e il luogo della consumazione vada rinvenuto – non diversamente dalla diffamazione a mezzo Internet – secondo i canoni di cui agli artt. 8 e 9 c.p.p.[46].

La lett. b) della direttiva reca l'inciso "produrre, manipolare o alterare e successivamente rendere accessibile al pubblico, tramite TIC, immagini, video o analogo materiale in modo da far credere che una persona partecipi ad atti sessualmente espliciti, senza il consenso della persona interessata". La produzione di materiale intimo senza consenso risulta coperta da altre fattispecie codicistiche in base al comportamento dell'agente (si pensi ad esempio all'art. 617-*septies* c.p.); la manipolazione e/o l'alterazione dei contenuti sessualmente espliciti non sono coperti dalla fattispecie di cui all'art. 612-*ter* c.p., così come la stessa non racchiude altre immagini come ad esempio l'autoritratto che rappresenti atti sessualmente espliciti inviati dalla vittima e poi pubblicati dal partner senza il consenso. "Fatti" questi che, insieme alle c.d. *deepfake*, andrebbero inseriti nel tipo criminoso di cui all'art. 612-*ter* c.p.[47].

[46] Corte di Cassazione, sentenza del 5 febbraio 2009 n. 8513 (dep. 25 febbraio 2009), secondo la quale l'immissione di scritti lesivi dell'altrui reputazione nel sistema Internet integra il reato di diffamazione aggravata (art. 595 c.p., comma 3, cfr. Corte di Cassazione, sentenza del n. 217745. Anche la diffamazione telematica è, naturalmente, reato di evento. Essa si consuma nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa, che, nel caso in cui le frasi offensive siano state immesse sul web, sono quelli in cui il collegamento viene attivato, cfr. Corte di Cassazione sentenza del 21 giugno 2006 n. 234528. Orbene, non risultando, nel caso in esame, il luogo in cui il reato è stato consumato (non potendo, in altre parole, applicarsi la regola di cui all'art. 8 c.p.p., comma 1), deve farsi ricorso ai criteri suppletivi di cui all'art. 9 c.p.p. Ed in tal senso, a norma del co. 2 di detto articolo, la competenza va attribuita al giudice della residenza dell'imputato, non essendo noto il luogo indicato nel co. 1, vale a dire "l'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione".

[47] In un precedente scritto (E. LO MONTE, *Art. 612*-ter, cit., p. 73 ss.) veniva fatto rientrare nel concetto di immagine l'eventuale autoritratto esplicitamente sessuale, qualora in grado di identificare la persona, fatto a mano con matita o con dei colori da parte della vittima e poi inviato al partner e da questi postato su Internet. Si concludeva che il termine "immagine", così come adoperato dal legislatore, ha l'idoneità di comprendere non solo le fotografie o gli scritti ma anche l'immagine digitale, e cioè la rappresentazione di un'immagine sul computer. Per una migliore chiarezza del "comando legislativo" sarebbe stato opportuno inserire accanto alle immagini e al video

In ultimo, la direttiva all'art. 5 co. 2 fa "salvi i principi fondamentali connessi alla libertà di espressione e di informazione e alla libertà delle arti e delle scienze" con la conseguenza che non assurge a condotta punibile la divulgazione di materiale con contenuti sessualmente espliciti nel caso in cui si tratti di attività "coperta" da motivazioni, ad esempio, artistiche.

5. *Lo* stalking *online (art. 6)*

L'art. 6 della direttiva prevede una particolare forma di "*stalking*"[48] consistente nella sorveglianza e nel monitoraggio dei movimenti e delle attività della vittima, attraverso TIC, nelle ipotesi in cui tali comportamenti "possano arrecare un danno grave alla persona".

Si tratta di una previsione criminosa che poco o nulla ha in comune con la fattispecie degli atti persecutori di cui all'art. 612-*bis* c.p. (il c.d. *stalking*). Quest'ultima (reato a forma libera, plurioffensivo, a dolo generico), infatti, si discosta dalla direttiva per le seguenti ragioni:

anche gli "scritti" e le "fotografie". Allo stesso modo veniva evidenziato che l'art. 612-*ter* c.p. non menzionava i "colloqui" con contenuto sessualmente esplicito registrati con il consenso della vittima e poi utilizzati nei termini di ritorsione sessuale. Le singole disposizioni che compongono la fattispecie incriminatrice di cui all'art. 612-*ter* c.p. non operano alcun richiamo ai colloqui; l'omesso riferimento sollecita un duplice ordine di osservazioni. In primo luogo, occorre chiarire se anche i colloqui possono essere un mezzo idoneo a limitare la libertà morale della vittima; si pensi all'esempio di colui che posta in rete una registrazione dal forte contenuto sessuale nella quale la persona offesa, con la promessa – esplicitamente richiesta e ottenuta – di non diffondere il contenuto della registrazione, abbia raccontato le sue fantasie libidinose o abbia commentato i particolari intimi di esperienze sessuali vissute. Si concludeva che anche una tale tipologia di dialoghi fosse in grado di incidere negativamente sulla libertà morale della vittima e che, pertanto, andava inserita nella fattispecie incriminatrice; attualmente, in ossequio al principio di tassatività-determinatezza dell'illecito penale, l'eventuale pubblicazione di conversazioni esplicitamente sessuali non consente di integrare il tipo delittuoso descritto dal legislatore.

[48] Art. 6: "Gli Stati membri provvedono affinché siano punite come reato le condotte intenzionali consistenti nel sottoporre ripetutamente o continuamente un'altra persona a sorveglianza tramite TIC, senza il suo consenso o un'autorizzazione legale a tal fine, per seguirne o monitorarne i movimenti e le attività, qualora tali condotte possano arrecare un danno grave alla persona in questione".

a) per la previsione di tre eventi alternativi (il perdurante e grave stato di ansia o di paura; il fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva; l'alterazione delle abitudini di vita) nessuno dei quali richiesti dalla direttiva;

b) per il riferimento al danno (che nella direttiva è qualificato dalla "gravità" diversamente da quanto disposto nell'art. 612-*bis* c.p. che non contiene alcun richiamo al danno; ciononostante la fattispecie viene ricostruita, tranne voci isolate[49], da dottrina e giurisprudenza nei termini di reato di danno);

c) per l'assenza di alcuni presupposti previsti dalla direttiva, vale a dire, la "mera" sorveglianza e le finalità di "seguire" e "monitorare" i movimenti e le attività della vittima.

Si tratta, in conclusione, di norme completamente diverse che in comune hanno solo il titolo e, ciononostante, la fattispecie di cui all'art. 612-*bis* c.p. potrebbe essere di aiuto nella redazione dell'eventuale nuova figura criminosa – come delineata dall'art. 6 della direttiva – non fosse altro per evitare i vistosi errori commessi dal legislatore.

La *ratio* dell'art. 6 della direttiva – che dovrebbe caratterizzare anche l'*emananda* figura delittuosa – è quella di evitare una "forma moderna di violenza spesso perpetrata nei confronti di familiari o persone che convivono con l'autore del reato, ma anche ad opera di ex partner o conoscenti"[50]: in sintesi si tratta di evitare le possibilità di "controllare una persona"[51]. Per meglio cogliere le finalità perseguite dal legislatore eurounitario occorre tenere presente, ancora, le ulteriori indicazioni del considerando n. 23 secondo cui: "Nella definizione del reato di *stalking* online, il concetto di "tracciamento" dovrebbe rinviare al fatto di rintracciare la posizione di una persona e di seguirne gli spostamenti, mentre il concetto di "monitoraggio" dovrebbe riferirsi alla

[49] Ritiene si tratti di fattispecie di pericolo E. LO MONTE, *Una nuova figura criminosa: lo "stalking" (art. 612-bis c.p.). Ovvero l'ennesimo, inutile, "guazzabuglio normativo",* in *Indice Pen*ale, 2010, n. 2, pp. 479-508.

[50] Considerando 21 della direttiva (UE) 2024/1385, *cit.*

[51] *Ivi*, considerando 23.

sorveglianza di una persona più in generale, compresa l'osservazione delle sue attività".

Il compito che attende il legislatore interno nella redazione della nuova fattispecie, alla luce delle "indicazioni" appena richiamate, non è assolutamente facile; a nostro avviso, il legislatore dovrebbe tenere nel giusto rilievo, alla luce della *ratio* prima evocata, che sul piano strutturale:

a) l'art. 6 utilizza, in ordine alla condotta, la locuzione "sottoporre ripetutamente o continuamente un'altra persona a sorveglianza" con il risultato che non possono essere utilizzate formule, senza alcuna specificazione con riferimento alla durata, come si è verificato con l'art. 612-*bis* con l'inciso "atti persecutori" interpretato dalla giurisprudenza nella sufficienza di due semplici atti[52]. L'avverbio "ripetutamente" e il concetto di "monitoraggio" implicano, il primo (riflettendo sui sinonimi), "molte volte", "a più riprese", "frequentemente", "reiteratamente", "spesse volte", ecc.; il secondo, è dato da uno "studio sistematico" di un fenomeno sociologico, economico, ecc.[53] e, dunque, attività che non possono esaurirsi in due sole condotte; del resto, appare difficile che l'attività di monitoraggio dei "movimenti" e delle "attività" possa essere realizzato con un "controllo" non affidato ad una serie di momenti. Il legislatore potrebbe indicare un arco temporale entro il quale vanno racchiuse le condotte di sorveglianza o monitoraggio o potrebbe specificarne il numero. Ciò ancora non è sufficiente a dare seguito alla direttiva perché la "continuità" della sorveglianza può avvenire anche con una sola azione (si pensi a colui che inserisca un virus nel computer oppure nello smartphone della vittima) ed anche tali ipotesi andrebbero disciplinate;

b) la formula "senza il suo consenso o un'autorizzazione legale a tal fine" può anche essere omessa per il semplice fatto che il dissenso è *in re ipsa* mentre il consenso scrimina (art. 50 c.p.); non c'è alcuna uti-

[52] Cfr. la nota presa di posizione della Corte di Cassazione sentenza del 17 febbraio 2010 n. 6417; conclusione questa ben lontana dall'attività "persecutoria" che richiede, di per sé, una serie di comportamenti che non può essere racchiusa nei due atti come ritenuto dalla giurisprudenza sufficienti a configurare la figura delittuosa si cui all'art. 612-*bis* c.p.; sul punto cfr. E. LO MONTE, *Una nuova figura criminosa*, cit., p. 481 ss.

[53] Vocabolario online Treccani, consultabile sul sito *https://www.treccani.it.*

lità nel prevedere – come è stato fatto con la fattispecie di cui all'art. 612-*ter* c.p. – l'assenza di consenso e, dunque, l'inutile capovolgimento del normale funzionamento del sistema penale. Lo stesso vale per l'eventuale autorizzazione legale che giustifica la condotta ai sensi dell'art. 51 c.p.;

c) in relazione all'inciso "possano arrecare un danno grave alla persona" valgono le osservazioni prima svolte con riferimento alla condivisione non consensuale di materiale intimo o manipolato;

d) l'art. 6 richiama le "condotte intenzionali" e, dunque, in tema di elemento psicologico – per le considerazioni prima svolte sul punto – è sufficiente il semplice dolo generico.

Il legislatore dovrebbe emanare una nuova fattispecie che renderebbe punibili le condotte di "controllo" e "monitoraggio" dei movimenti e delle attività di una persona, qualora sussisterebbe il pericolo di danno grave alla persona.

Da altro punto di vista va rilevato che se le attività di "tracciamento" e "monitoraggio", svolte tramite TIC, risultano punibili allorché siano in grado di arrecare un nocumento alla vittima (se "*possano* – corsivo aggiunto – arrecare un danno grave alla persona" nell'art. 6 della direttiva) ne consegue che le stesse possono essere lette anche come una sorta di anticipazione della tutela rispetto alla vigente fattispecie di cui all'art. 612-*bis* c.p. Si tratterebbe in questi casi di "atti idonei diretti in modo non equivoco" (in grado di cagionare un danno che ancora non si è verificato) e, dunque, (in assenza di uno dei tre eventi previsti dall'art. 612-*bis* c.p.) di un tentato delitto di atti persecutori.

6. *Le molestie online (art. 7)*

L'art. 7 della direttiva persegue il dichiarato scopo di contrastare le molestie online; se ciò si presenta come un'aspirazione del tutto condivisibile, sul piano concreto problemi di non poco momento sorgono quando si vanno a leggere le singole disposizioni che compongono l'evocato articolo; la norma, in verità, è scritta a dir poco in modo enigmatico per non dire incomprensibile.

Né, tanto meno, ad apportare miglioramenti sul terreno della

chiarezza dell'art. 7 può essere richiamato il disposto del considerando n. 24 della direttiva che, anzi, finisce per complicare ulteriormente, perché, come si vedrà, finisce per "trasformare" le molestie online in atti persecutori.

Una fattispecie incriminatrice che racchiuda tutte le varie ipotesi previste nell'art. 7 della direttiva appare un'operazione difficilmente attuabile per le ragioni che espliciteremo nel prosieguo.

In primo luogo, vanno evidenziate le asserzioni svolte nel considerando n. 24 laddove si afferma che le "molestie online (…) dovrebbero includere il fatto di attuare, in modo ripetuto o continuativo, comportamenti minacciosi nei confronti di una persona, almeno qualora tali comportamenti comportino il rischio di commettere reati tramite TIC, e se tali comportamenti *possono indurre tale persona a temere seriamente per la propria incolumità o per l'incolumità delle persone a carico* (corsivo aggiunto)".

L'art.7 riprende tale impostazione e richiede che gli Stati membri provvedano a punire una "quadriade" di condotte poste in essere intenzionalmente (e, dunque, per le ragioni prima avanzate, con dolo generico); in modo più specifico per il legislatore comunitario devono essere sanzionati:

- i comportamenti minacciosi che possono indurre la persona a temere per la propria incolumità (o quella di altre persone a carico della vittima) (lett. a);
- i comportamenti minacciosi o ingiuriosi (…) qualora tale comportamento possa arrecare un grave danno psicologico alla persona (lett. b)[54];

[54] La *ratio* di tale previsione si coglie richiamando, ancora una volta, il considerando n. 24 laddove afferma che: "Questo tipo di attacchi di ampia portata, compresi gli attacchi di gruppo coordinati online, possono trasformarsi in vere e proprie aggressioni offline o causare gravi danni psicologici e in casi estremi portare al suicidio della vittima". Il considerando richiama, poi, le varie categorie delle vittime e gli ambiti di lavoro; si sostiene, infatti, che tali attacchi spesso prendono di mira importanti donne politiche, giornaliste e tutte coloro che difendono i diritti umani; in siffatte categorie vengono fatte rientrare anche le donne che operano in contesti diversi, ad esempio nei campus universitari, nelle scuole e sul luogo di lavoro.

- l'inviare a una persona (…) un'immagine, un video o altro materiale analogo raffigurante i genitali qualora tale condotta possa arrecare un grave danno psicologico alla persona in questione (lett. c).
- il rendere accessibile al pubblico (…) materiale contenente i dati personali di una persona (…) al fine di istigare altre persone ad arrecare un danno fisico o psicologico grave alla persona (lett. d).

Tutte le condotte richiamate devono avvenire tramite TIC; la prima condotta richiede ripetitività e continuazione del comportamento e, ancora, che la persona sia indotta a temere "seriamente" per la propria incolumità.

Da un siffatto "quadro" possono aversi varie soluzioni, ma prima va sgomberato il campo da un possibile equivoco di fondo.

Tralasciando i requisiti della ripetizione e della continuazione per i quali vale quanto sostenuto a proposito dello *stalking* online, il primo aspetto problematico che viene in evidenza è il rapporto tra la rubrica dell'art. 7 "molestie online" e i comportamenti minacciosi (lett. a) e i comportamenti minacciosi o ingiuriosi (lett. b); quasi che le molestie online siano equiparate ai due tipi di comportamento appena ricordati. Non si comprende, con i "normali" principi che governano il diritto penale interno, l'uso della locuzione "molestie online" – utilizzata nella rubrica dell'art. 7 e nel considerando n. 24 – e i comportamenti minacciosi, trattandosi di ambiti completamente diversi; non a caso il codice penale dedica a tali fatti differenti fattispecie incriminatrici (art. 660 e art. 612 c.p.).

L'art. 7 prevede, inoltre, che la punibilità di siffatte condotte minacciose sia subordinata alla sussistenza di determinate condizioni: "indurre la persona in questione a temere seriamente per la propria incolumità o per l'incolumità delle persone a carico", lett. a); "arrecare un grave danno psicologico alla persona", lett. b). Da tali formule discende che si è in presenza di vere e proprie minacce e, dunque, in una prospettiva di accoglimento della direttiva occorre confrontarsi (nel senso di raccordarsi) con la disciplina prevista dall'art. 612 c.p.; in secondo luogo , l'uso dell'avverbio "seriamente", art. 7 lett. a) – se implica, sotto il profilo dell'offensività, l'idea che vanno sanzionati comportamenti "credibili" o "gravi" idonei a suscitare un timore "serio" con esclusione di paure lievi – comporta, all'opposto, "seri" problemi di ricezione in una disposizione incriminatrice.

Allo stesso modo di non semplice intellegibilità si presenta l'inciso "almeno qualora tali comportamenti comportino il rischio di commettere reati"; la formula parrebbe sottintendere che la punibilità, anche alla luce del rigore sanzionatorio sollecitato dalla direttiva[55], si riferisca a "fatti gravi" commessi mediante l'uso di TIC che si caratterizza per l'ampia diffusività.

Alla luce delle considerazioni appena svolte il legislatore interno potrebbe, in astratto, innovare le disposizioni di cui agli artt. 660 e 612 c.p.

Nel prima caso si tratterebbe di introdurre un nuovo comma che faccia riferimento alle molestie (anche "ingiuriose") poste in essere con strumenti telematici e informatici o, meglio, con le tecnologie dell'informazione e della comunicazione (TIC, come affermato nella direttiva) e prevedere una sanzione rapportata alle indicazioni di cui all'art. 10 della direttiva (pena non inferiore nel massimo ad un anno) e conseguente incremento sanzionatorio. Tale strada, però, non sembra percorribile atteso che l'art. 10 della direttiva fa riferimento alla *reclusione* e, quindi, inapplicabile alla contravvenzione disciplinata dall'art. 660 c.p.

Nella seconda ipotesi, si potrebbe aggiungere un comma all'art. 612 c.p. che richiami espressamente le minacce ("gravi" o in grado di suscitare un grave pregiudizio) a mezzo TIC[56].

La strada più semplice, però, è data dal fatto che le condotte di cui alle lett. a) e b) finiscono per configurare la più grave fattispecie degli atti persecutori nella forma aggravata (dall'uso di strumenti telematici o informatici, art. 612-*bis* co. 2 c.p.). L'avverbio "seriamente" o un suo sinonimo non è utilizzato nella fattispecie degli atti persecutori ma ciò non osta ai sensi del considerando n. 91 che "abilita" gli Stati membri ad attivare misure maggiormente stringenti se finalizzati a tutelare la vittima di violenza.

La lett. b) richiede, inoltre, che vengano sanzionate le condotte

[55] V. *infra* par. 9.

[56] La giurisprudenza di legittimità ha precisato, recentemente, che il reato di molestie può ben essere commesso anche con l'inoltro di messaggi di posta elettronica e, quindi, non solo attraverso l'uso del telefono come previsto dalla norma; si tratta, secondo i giudici di legittimità (Corte di Cassazione, sentenza del 10 ottobre 3023 n. 34171) di interpretazione estensiva e non di analogia, vietata nel diritto penale.

minacciose o ingiuriose adottate "pubblicamente"; il riferimento alla diffusività pare del tutto ridondante in presenza dell'uso delle Tecnologie dell'Informazione e della Comunicazione (i.e. Internet).

Da altro punto di vista l'uso del termine "pubblicamente" esclude la possibilità di configurare la fattispecie qualora il comportamento minaccioso sia indirizzato non ad una fascia indeterminate di persone ma solo ad una, seppure attraverso l'uso delle tecnologie informatiche. Ora se il legislatore sovranazionale ha inteso esplicitare il concetto di diffusione riferendosi non al singolo ma ad una cerchia indeterminata di soggetti, la presenza del termine nella sussunzione eventuale nella fattispecie incriminatrice degli atti persecutori esclude la configurabilità del fatto rispetto ad un solo destinatario. L'eventuale omissione della "pubblicità" amplia le possibilità applicative, ed anche tale soluzione si pone in linea con il considerando n. 91. La stessa norma prevede, diversamente dalla lett. a), che le condotte arrechino un danno (grave) psicologico; si tratta di una specificazione del tutto ultronea atteso che il concetto di "danno alla persona" implica anche le conseguenze di natura psichica. Infine, sull'espresso richiamo alla "gravità" valgono le considerazioni svolte con riferimento alla lett. a). L'inciso "insieme ad altre persone" risulta coperto dalle disposizioni in tema di compartecipazione criminosa (artt. 110 e ss. c.p.) e, pertanto, non solleva alcuna questione;

La lett. c) prevede che siano punite le condotte di inviare a una persona senza che questa lo richieda, tramite TIC, un'immagine, un video o altro materiale analogo raffigurante i genitali qualora tale condotta possa arrecare un grave danno psicologico alla persona in questione.

In ordine all'invio di materiale raffigurante gli organi genitali (o altro materiale simile), c.d. *cyberflashing*, occorre distinguere se la trasmissione:

1) concerne la diffusione e, allora, la condotta risulta già coperta dalle disposizioni di cui all'art. 5 della direttiva in tema di condivisione non consensuale di materiale intimo o manipolato;

2) se è rivolta alla vittima, in tal caso la norma è finalizzata a coprire eventuali momenti di natura "estorsiva" o certamente di coazione della libertà di autodeterminazione della vittima. Tali ipotesi potrebbero trovare copertura nelle disposizioni in tema di minaccia o violen-

za c.d. impropria[57] (612 c.p.), violenza privata[58] (art. 610 c.p.), estorsione (629 c.p. atteso che – ai fini della configurabilità della fattispecie – oltre a venire in rilievo ogni forma di prevaricazione, l'ingiustizia del profitto racchiude ogni vantaggio e non solo quello di tipo patrimoniale, Corte di Cassazione, sentenza del 4 maggio 2006 n. 29563). Conclusione questa che risulta in linea con il considerando n. 24 ove si fa espresso riferimento al fatto che il "*cyberflashing* è una forma comune di intimidazione che mira a ridurre le donne al silenzio" e, dunque, le immagini o i video prima ottenuti – con il consenso della vittima – vengono utilizzati per ridurre la stessa al silenzio. Il limite della disposizione va rinvenuto nella condizione del "grave danno psicologico"; in altri termini, il concetto di gravità rischia di "legittimare" tutto ciò che non è grave e, quindi, per rendere lecite le condotte che possano cagionare un danno "semplicemente normale" (i.e. "non grave") alla vittima. Il che ha in sé qualcosa di tragicomico.

La lett. d) richiede che vengano sanzionate le condotte di rendere accessibile al pubblico, tramite TIC, materiale contenente i dati personali di una persona, senza il consenso di quest'ultima, al fine di istigare altre persone ad arrecare un danno fisico o psicologico grave alla persona in questione.

Il legislatore con la lett. d) dell'art. 7 mira a sanzionare il c.d. *doxing* che si verifica allorché vengano diffuse informazioni personali – senza il consenso della vittima e tramite TIC – al fine di istigare altre persone ad arrecare un danno fisico o un grave danno psicologico. Alcune brevi considerazioni sul punto:

1) in ordine alla "gravità" del danno psicologico valgono le riflessioni svolte in precedenza;

2) il fine di istigare[59] richiama una specifica volontà e l'eventuale

[57] Si pensi alla c.d. violenza impropria che comprende ogni mezzo che produca il medesimo risultato, esclusa la minaccia; costituiscono – è stato affermato – violenza impropria tutte le attività insidiose con le quali il soggetto viene posto, totalmente o parzialmente, nell'impossibilità di volere o di agire, cfr. A. PECCIOLI, *Reati contro la persona*, in F. ANTOLISEI, A. ROSSI (a cura di) *Manuale di diritto penale. Parte speciale*, 17ed., Milano, 2022, I, pp. 5 -339.

[58] In proposito cfr. E. MEZZETTI, *Violenza privata e minaccia*, in *Digesto delle Discipline Penalistiche*, Torino, 1999, n. XV, pp. 264-286.

[59] Sull'istigazione v. *infra* par. 8.

fattispecie incriminatrice andrebbe incontro ad un duplice rischio: quello di vanificare ogni diffusione non finalizzata all'istigazione (si pensi all'esempio di scuola dello scherzo) e la difficoltà di accertamento dello scopo specifico. Anche se ci rendiamo conto che è proprio la finalità di istigare a giustificare, per il legislatore comunitario, una fattispecie incriminatrice in considerazione del fatto che, altrimenti, la semplice diffusione di informazioni personali è già coperta dal Codice in materia di protezione dei dati personali dopo le innovazioni di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 e dai documenti correlati (ad esempio, direttiva (UE) 2016/680; Regolamento (UE) 2018/1725, ecc.).

7. *L'istigazione alla violenza o all'odio online (art. 8)*

L'art. 8 della direttiva fa carico agli Stati membri di sanzionare la condotta (posta in essere intenzionalmente) di istigazione alla violenza e all'odio di genere; istigazione che deve avvenire pubblicamente attraverso l'uso di TIC.

Le ragioni di tale disposizione si colgono richiamando il considerando n. 25 secondo cui: "Negli ultimi anni l'aumento dell'uso di internet e dei social media ha portato a un'impennata dei casi di istigazione pubblica alla violenza e all'odio, anche basati sul genere. L'effetto disinibente di internet moltiplica la condivisione facile, rapida e vasta dei discorsi d'odio nel mondo digitale, in quanto il presunto anonimato sul web e il senso di impunità che ne deriva riducono il senso di inibizione che normalmente frenerebbe le persone. Le donne sono spesso il bersaglio dell'odio sessista e misogino online, che può degenerare in reati generati dall'odio nel mondo reale. È un fenomeno che va prevenuto e intercettato fin dalle prime fasi".

Il sistema penale interno già contiene diverse fattispecie contro l'ordine pubblico che in qualche modo potrebbero essere utilizzate: vari tipi di istigazione e una di apologia; anche se a venire in rilievo nel caso di specie, oltre all'art. 414, è l'art.604-*bis* c. p.; occorre, allora, verificare se le figure presenti nel codice penale possano essere adoperate per suffragare quanto sollecitato in sede sovranazionale oppure necessitano di integrazioni o, addirittura, sussista la necessi-

tà di nuove incriminazioni; ipotesi quest'ultima che ci pare da escludere.

In via di pura schematizzazione la fattispecie di cui all'art. 414 c.p. copre le esigenze avanzate in sede comunitaria e, per molti aspetti, offre una tutela maggiore di quella richiesta dalla direttiva, soddisfacendo anche le esigenze di prevenzione evidenziate dal legislatore comunitario e ciò per le susseguenti motivazioni:

a) per la struttura della fattispecie:

1) trattandosi di reato comune la cui condotta incriminata consiste nell'istigare pubblicamente (circostanza questa che assolve anche il riferimento "al pubblico" di cui alla direttiva) a commettere delitti o contravvenzioni; di pericolo concreto[60];

2) sorretta, secondo la tesi maggioritaria, da dolo generico consistente nella volontà di incitare alla commissione di determinati fatti delittuosi, unitamente alla consapevolezza del loro carattere illecito e di agire in pubblico;

3) che si consuma non appena viene realizzata pubblicamente la condotta istigatrice[61].

b) per la previsione della figura dell'apologia (art. 414 co. 3):

1) trattandosi di reato comune;

2) caratterizzato da dolo c.d. istigatorio, che si consuma non diversamente dall'istigazione;

3) che, dopo l'intervento della Corte costituzionale, risulta trasformata in una sorta di istigazione "indiretta". Infatti, relativamente a quest'ultimo punto, la Corte con una sentenza interpretativa di rigetto ha affermato che per apologia punibile non è sufficiente una mera e semplice manifestazione di pensiero ma solo quella che, per le sue

[60]Cfr. Corte di Cassazione sentenza del 3 luglio 2001 n. 26907, secondo cui il delitto di istigazione a delinquere, previsto dall'art. 414 c.p., è reato di pericolo concreto e non presunto; pertanto, l'esaltazione di un fatto di reato o del suo autore finalizzata a spronare altri all'imitazione o almeno ad eliminare la ripugnanza verso il suo autore non è, di per sé, punibile, a meno che, per le sue modalità, non integri un comportamento concretamente idoneo a provocare la commissione di delitti.

[61] Cfr. G. FIANDACA, E. MUSCO, *Diritto penale. Parte speciale*, 6ed., Bologna 2021, p. 499, che auspicano la completa eliminazione della figura dell'apologia trattandosi – dopo l'intervento della Corte costituzionale – di un "doppione" della fattispecie di istigazione.

modalità, integri un comportamento idoneo a provocare la commissione di delitti e, dunque, le espressioni usate generino il serio pericolo di compimento, nell'immediato circostante contesto spazio-temporale, di fatti criminosi da parte di terzi. La Corte, in tal modo, ha trasformato l'apologia da fattispecie di pericolo astratto/presunto a pericolo concreto e "salvato" la stessa dai rischi di incostituzionalità per contrasto con il principio di libertà di manifestazione del pensiero;

c) per la previsione, nella forma aggravata, dell'uso degli strumenti telematici e informatici come richiesto dalla direttiva[62].

Senza entrare nel merito dei rapporti tra istigazione e, soprattutto, apologia con i principi costituzionali, va segnalato che ai fini della determinazione del momento consumativo – sia per quanto concerne l'istigazione che l'apologia – "se è corretto ritenere che sia irrilevante la realizzazione della condotta istigata, è ben più dubbio che basti la condotta istigatoria o apologetica a prescindere dall'effettiva percezione da parte dei destinatari; questo punto di vista, benché diffuso presso la giurisprudenza sembra però accoglibile solo accettando la configurazione come reati di pericolo presunto delle fattispecie dell'art. 414, superata dopo l'intervento della Corte costituzionale del 1970"[63].

L'art. 414 c.p. richiede, è noto, che vi sia una fattispecie a monte e, dunque, che i fatti a cui fa riferimento la direttiva siano già previsti come reato[64].

[62] Corte costituzioale, 4 maggio 1970, n. 65, disponibile su *https://giurcost.org*, secondo cui "L'apologia punibile ai sensi dell'art. 414, ultimo comma, del codice penale non è, dunque, la manifestazione di pensiero pura e semplice, ma quella che per le sue modalità integri comportamento concretamente idoneo a provocare la commissione di delitti".

[63] Così G. FORNASARI, *Istigazione a delinquere*, in G. FORNASARI, S. RIONDATO, (a cura di), *Reati contro l'ordine pubblico*, 2ed., Torino, 2017, pp. 3-12.

[64] La Corte di Cassazione, sentenza dell'8 giugno 2018. n. 26315, ha affermato che la condotta di chi esalta un fatto di reato al fine di spronare altri all'imitazione integra il delitto di istigazione a delinquere quando, per il suo contenuto intrinseco, per la condizione personale dell'autore e per le circostanze di fatto in cui si esplica, sia effettivamente idonea a determinare il rischio concreto della commissione di altri reati lesivi di interessi omologhi a quelli offesi dal crimine esaltato; non diversamente per le ipotesi di cui all'art. 414 co. 3 c.p. secondo cui ai fini dell'integrazione di tale delitto non basta l'esternazione di un giudizio positivo su un episodio criminoso, ma occorre che il comportamento dell'agente sia tale per il suo contenuto intrinseco, per la condi-

Altra possibile fattispecie utilizzabile, come si anticipava, è quella delineata dall'art. 604-*bis*, (reato comune, plurioffensivo venendo in rilievo l'ordine pubblico e la dignità umana[65], a forma libera, a dolo generico[66], che si consuma nel momento e nel luogo dell'istigazione) che punisce chiunque fa propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa. Si tratta di una disposizione alquanto prossima all'istigazione alla violenza e all'odio online richiesta dalla direttiva. In particolare, a venire in evidenza sono: da un lato, la seconda parte della norma (co. 1 lett. a) che sanziona l'istigazione a commettere atti di discriminazione (dopo la riformulazione ad opera della Legge n. 85/2006 che ha sostituito l'istigazione all'incitamento e, considerata la sostanziale equivalenza dei due termini, nulla cambia ai fini dell'incriminazione[67]); dall'altro la seconda parte (co. 1 lett. b) che prevede un reato di istigazione ovvero di commissione di atti violenti e/o provocatori determinata da motivi razziali e/o discriminatori[68].

Il legislatore interno potrebbe:

1) inserire nel corpo dell'art. 604-*bis* c.p. un riferimento alla violenza di genere e all'odio ricorrendo all'uso di tecnologie dell'informazione e della comunicazione; in quest'ultimo caso la sede più appropriata potrebbe essere quella della lett. b), co. 1 art. 604-*bis* c.p., che utilizza la formula "istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi";

2) emanare una nuova fattispecie strutturata secondo lo schema

zione personale dell'autore e per le circostanze di fatto in cui si esplica, da determinare il rischio effettivo della consumazione di altri reati lesivi di interessi omologhi a quelli offesi dal crimine esaltato (Corte di Cassazione, sentenza del 17 luglio 20199. n. 31562).

[65] Corte di Cassazione, sentenza del 23 giugno 2015, n. 36906.

[66] Corte di Cassazione, sentenza del 7 maggio 2008, n. 37581.

[67] Cfr. F. BACCO, *Norme antidiscriminazione*, in D. PULITANÒ (a cura di), *Diritto penale. Parte speciale*, I, *Tutela della persona*, 3ed., Torino, 2019, pp. 408-416 e bibliografia e giurisprudenza ivi richiamata.

[68] M.E. SALERNO, sub *art. 604*-bis, in A. CADOPPI, S. CANESTRARI, P. VENEZIANI (a cura di), *Codice penale commentato con dottrina e giurisprudenza*, Torino, 2021, pp. 2501-2506.

dell'art. 414-*bis* c.p. ed inserendo gli elementi elencati nel co. 1 dell'art. 8.

Le norme appena richiamate abbracciano anche le disposizioni di cui al n. 2 dell'art. 7 della direttiva che stabilisce: "Ai fini del paragrafo 1, gli Stati membri possono decidere di configurare come reato soltanto le condotte atte a turbare l'ordine pubblico o che sono minacciose, offensive o ingiuriose".

8. *Istigazione, favoreggiamento, concorso e tentativo (art. 9)*

L'art. 9 co. 1 della direttiva prevede che gli Stati membri puniscano l'istigazione a commettere i reati di: mutilazioni genitali femminili, matrimonio forzato, condivisione non consensuale di materiale intimo o manipolato*, stalking* online, molestie online di cui alla lett. b), vale a dire quando la condotta – adottata pubblicamente tramite TIC – consiste in comportamenti minacciosi o ingiuriosi nei confronti di una persona, qualora tale comportamento possa arrecare un grave danno psicologico alla persona in questione.

Il co. 2 dello stesso articolo stabilisce che siano previsti i reati di favoreggiamento e di concorso di persone nel reato quando i fatti abbiano ad oggetto: l'escissione, l'infibulazione o altra mutilazione della totalità o di parte delle grandi labbra o delle piccole labbra vaginali o del clitoride nei reati; le mutilazioni genitali femminili, il matrimonio forzato, la condivisione non consensuale di materiale intimo o manipolato, lo *stalking* online, le molestie online, l'istigazione alla violenza o all'odio online.

Il co. 3, a sua volta, statuisce che le mutilazioni genitali femminili e il matrimonio forzato siano puniti a titolo di tentativo.

Non pare che tali indicazioni possano sollevare particolari problemi atteso che il sistema penale interno prevede, come si anticipava, la fattispecie dell'istigazione a delinquere, di cui all'art. 414 c.p.; e, dunque, non sussistono problemi nel sanzionare, ai sensi dell'art. 414 c.p., l'istigazione alle mutilazioni genitali femminili oppure al matrimonio forzato.

Spetta al legislatore valutare possibili ipotesi di previsione di particolari forme di istigazione – ancorate a particolari esigenze politico-

criminali – per i fatti menzionati dalla direttiva, non diversamente da come è stato fatto con la previsione dell'istigazione a pratiche di pedofilia e di pedopornografia di cui all'art. 414-*bis* c.p. Seguendo l'impostazione della direttiva – che venga sanzionata, ad esempio, l'istigazione a commettere fatti di mutilazioni genitali – il legislatore dovrebbe prevedere nella stessa fattispecie una specifica forma di istigazione supportata da una specifica sanzione; la presenza dell'art. 414 c.p. rende tale sollecitazione del tutto superflua.

Lo stesso può dirsi per la punibilità dei fatti di favoreggiamento di cui all'art. 9 co. 2 della direttiva in quanto gli artt. 378 e 379 c.p. riescono a fronteggiare quanto richiesto in sede comunitaria, sul presupposto della commissione di un reato. Nel caso di specie alcuna questione sussiste, ad esempio, per le mutilazioni genitali femminili, il matrimonio forzato, la condivisione non consensuale di materiale intimo o manipolato essendo fatti già coperti da fattispecie incriminatrici. Il favoreggiamento personale[69], consistendo in un aiuto dato all'autore del reato e, dunque, prevedendo una condotta descritta in termini molto generici, consente un'applicazione alquanto ampia in grado di coprire le esigenze avanzate dalla direttiva. Lo stesso può dirsi per il favoreggiamento reale consistente in qualsiasi aiuto prestato per stabilizzare l'acquisizione dei proventi (prodotto, prezzo, profitto) del reato.

Ugualmente si verifica per la compartecipazione criminosa atteso che gli artt. 110-119 forniscono piena copertura ai fatti previsti dalla direttiva.

L'art. 56 c.p., infine, consente di anticipare l'intervento sanzionatorio a tutte le possibili figure delittuose previste dalla direttiva, qualora la struttura della specifica figura delittuosa consenta l'ammissibilità

[69] Fattispecie funzionale a tutelare l'interesse al corretto ed efficiente svolgimento delle attività di investigazione e di ricerca svolte dall'autorità giudiziaria e dalla polizia giudiziaria; reato a forma libera; ove il dolo richiede la consapevolezza del reato presupposto e dell'aiuto prestato ad eludere le investigazioni o a sottrarsi alle ricerca dell'autorità giudiziaria; che ammette la configurabilità del tentativo pur avendo uno spazio limitato, in tal senso cfr. M. PELISSERO, *I delitti contro l'amministrazione della giustizia*, in R. BARTOLI, M. PELISSERO, S. SEMINARA (a cura di), *Diritto penale parte speciale*, Torino, 2021, pp. 613-722.

del tentativo e ciò dipende dalla redazione delle singole fattispecie ancorate al danno oppure al pericolo.

Le fattispecie incriminatrici dell'istigazione a delinquere, del favoreggiamento (personale o reale) da un lato, gli istituti della compartecipazione criminosa (morale e/o materiale) e del delitto tentato, dall'altro, consentono forme di tutela ben oltre i limiti segnati dall'art. 9 dalla direttiva applicandosi a tutte le diverse tipologie delittuose.

La maggiore tutela accordata dal sistema penale interno ai fatti di reato elencati nella direttiva si allinea al considerando n. 91 della stessa che stabilisce "norme minime", lasciando liberi gli Stati "di adottare o mantenere in vigore norme di diritto penale più rigorose per quanto riguarda la definizione dei reati e delle sanzioni in materia di violenza contro le donne. Per quanto riguarda le disposizioni sui diritti delle vittime contenute nella presente direttiva, gli Stati membri possono introdurre o mantenere in vigore norme più rigorose, comprese norme che assicurino un maggiore grado di tutela e assistenza alle vittime".

9. *Regime sanzionatorio e circostanze*

L'art. 10 della direttiva (dedicato alle "sanzioni") stabilisce una doppia indicazione in ordine alla pena: la prima (co. 1) attiene all'aspetto "qualitativo" della punizione stabilendo – con una formula ormai consuetudinaria – per tutti i reati previsti (artt. da 3 a 9 della direttiva stessa) che le sanzioni penali siano "effettive, proporzionate e dissuasive".

A tal fine – si legge nel considerando n. 28 – "è opportuno stabilire livelli minimi per la pena massima della reclusione delle persone fisiche. La reclusione massima prevista dalla presente direttiva per i reati commessi da persone fisiche dovrebbe applicarsi almeno alle forme più gravi di tali reati".

I co. 2, 3 e 4 stabiliscono un limite "non inferiore nel massimo" diversificato in base al disvalore del fatto di reato, di modo che: a) per le mutilazioni genitali femminili è prevista una soglia di cinque anni (co. 2); per il matrimonio forzato tre anni (co. 3); per la condivisione non consensuale di materiale intimo o manipolato, *stalking* online e

molestie online (ad eccezione della lett. d) dell'art. 7) limite massimo non inferiore ad un anno.

L'art. 11 della direttiva prevede una serie di inasprimenti sanzionatori, rimettendo agli Stati la scelta se considerarle o meno circostanze aggravanti; l'inciso "possano essere considerate (…) circostanze aggravanti in relazione ai pertinenti reati" lascia intendere che la previsione di aggravamenti di pena sia rimessa alla discrezionalità dei singoli legislatori.

Va detto che molte delle circostanze elencate nell'art. 11 della direttiva sono già previste dall'ordinamento interno e dunque già sono "attivate", come ad esempio nei casi di recidiva; di minore difesa; di violenza assistita; di violenza commessa nei confronti di soggetti minorenni; del numero di persone; di uso di armi; di abuso di una posizione di fiducia; di abuso di autorità o influenza; di fatto commesso ai danni di un coniuge o partner o di un ex coniuge o ex partner; ecc.

Si tratta di "scegliere" – dall'ampio elenco di cui all'art. 11 – quelle che sono ritenute maggiormente idonee ad individuare la "giusta" sanzione da applicare al caso in concreto verificatosi.

Del resto, il lungo elenco delle circostanze aggravanti di cui all'art. 61 c.p. e l'eventuale istituto del concorso di circostanze consente estesi margini di manovra al legislatore nell'individuazione della pena da applicare al fatto storico.

Abstract

Nell'ambito di una serie di misure protese a contrastare il grave fenomeno della violenza di genere e la violenza domestica la recente direttiva (UE) 2024/1385 coinvolge anche il diritto penale sostanziale con la previsione di nuove fattispecie di reato. In verità si tratta di fatti, in larga parte, già coperti dall'attuale sistema penale; si pensi ad esempio alle mutilazioni genitali femminili, al matrimonio forzato, alla condivisione non consensuale di materiale intimo. Si pensi, ancora, alle varie disposizioni in tema di istigazione che pure è oggetto delle sollecitazioni del legislatore comunitario. Altri fatti, all'opposto, risultano sussumibili nelle vigenti norme solo parzialmente. Il contributo attraverso un'analisi comparata (tra quanto previsto dalla direttiva e quanto già disciplinato dal codice penale) pone in evidenza le norme appli-

cabili alle varie ipotesi di reato delineate nella direttiva e quelle, invece, che appaiono meritevoli della formulazione di nuove figure di reato.

KEYWORDS: violenza – genere – nuove norme incriminatrici – direttiva (UE) 2024/1385 – diritto penale sostanziale

LA "RESPUESTA PENAL" A LA VIOLENCIA CONTRA LAS MUJERES Y A LA VIOLENCIA DOMÉSTICA EN LA DIRECTIVA 2024/1385: ¿HACIA NUEVAS FIGURAS PENALES?

Como parte de una serie de medidas destinadas a combatir el grave fenómeno de la violencia de género y la violencia doméstica, la reciente directiva (UE) 2024/1385 también afecta al derecho penal sustantivo con la tipificación de nuevos delitos penales. En realidad, se trata de hechos que, en gran medida, ya están contemplados en el sistema penal vigente; piénsese, por ejemplo, en la mutilación genital femenina, el matrimonio forzado, el intercambio no consentido de material íntimo. Pensemos también en las diversas disposiciones sobre incitación, que también es objeto de las solicitudes del legislador de la UE. Otros hechos, en cambio, sólo están parcialmente subsumidos en las normas actuales. La contribución, mediante un análisis comparativo (entre lo previsto en la directiva y lo ya regulado por el código penal), pone de relieve las normas aplicables a las distintas hipótesis delictivas esbozadas en la directiva y las que, por el contrario, parecen merecer la formulación de nuevas figuras delictivas.

PALABRAS CLAVE: violencia – género – nuevas normas incriminatorias – directiva (UE) 2024/1385 – derecho penal sustantivo

IL QUADRO GIURIDICO GENERALE AUSPICATO NELLA FONTE SOVRANAZIONALE: DALLA PROTEZIONE DELLE VITTIME ALL'ACCESSO ALLA GIUSTIZIA

*Luigi Kalb**

SOMMARIO: 1. Le finalità programmate dalla fonte sovranazionale nell'ottica del processualpenalista. – 2. Le iniziative di denuncia del fatto. – 3. Formazione e specializzazione degli attori del procedimento. – 4. Attività investigativa e pericoli di dispersione probatoria. – 5. La protezione della vittima mediante ricorso agli ordini dell'autorità procedente. – 6. Durata del procedimento penale e prescrizione del reato. – 7. I limiti dell'intervento della giurisdizione penale nazionale.

1. *Le finalità programmate dalla fonte sovranazionale nell'ottica del processualpenalista*

In via preliminare, occorre rilevare che la nuova direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio sulla lotta alla violenza contro le donne e alla violenza domestica si pone in linea con la finalità perseguita a livello euro unitario di contenere fenomeni criminali che, superando l'ambito ristretto dei singoli Stati membri, assumono una rilevanza comune, fondando la necessità di predisporre un apparato minimo di tutela nello spazio europeo. Il testo normativo, entrato in vigore il 13 giugno 2024, impone ai destinatari l'attuazione delle disposizioni recate entro il 14 giugno 2027, termine previsto dall'art. 49[1].

*Professore ordinario di Procedura penale. Università degli Studi di Salerno. Email: lkalb@unisa.it.

[1] Per le prime analisi sulla direttiva cfr. E. BERGAMINI, *La proposta di una direttiva dell'Unione europea sulla lotta alla violenza contro le donne e alla violenza domestica*, in A. DI STASI, R. CADIN, A. IERMANO, V. ZAMBRANO (a cura di), *Donne migranti e violenza di genere nel contesto giuridico internazionale ed europeo*, Napoli, 2023, p. 487 ss.; M. BIANCHI, *L'abuso dell'immagine intima nella direttiva (UE) 2024/1385*, in *Sistema penale*, 2024; S. BRASCHI, *La nuova direttiva sulla lotta alla violenza contro le*

Quest'ultimo prevede che gli Stati membri mettano in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 14 giugno 2027, informandone immediatamente la Commissione.

Entro il 14 giugno 2032 gli Stati membri devono comunicare alla Commissione tutte le informazioni pertinenti riguardanti il funzionamento della presente direttiva necessarie a consentire alla Commissione di redigere una relazione sulla valutazione della nuova direttiva (art. 45).

In ogni caso, l'attuazione di questa direttiva non deve pregiudicare i regimi speciali di responsabilità relativi ai principi fondamentali della libertà di stampa e della libertà di espressione nei media protetti esistenti negli Stati membri al 13 giugno 2024, a condizione che tali regimi possano essere applicati nel pieno rispetto della Carta.

L'obiettivo perseguito dall'Unione si evince, innanzitutto, dai molteplici considerando posti in apertura della direttiva.

Con la nuova fonte sovranazionale si intende fornire un quadro giuridico generale in grado di prevenire e far fronte efficacemente alla violenza contro le donne e alla violenza domestica in tutta l'Unione. Per il conseguimento di questa finalità si auspica l'introduzione e il rafforzamento di misure in relazione alla definizione dei reati e delle pene irrogabili, alla protezione delle vittime e all'accesso alla giustizia, all'assistenza alle vittime, al miglioramento della raccolta di dati, alla prevenzione, al coordinamento e alla cooperazione[2]. Alla luce delle

donne e alla violenza domestica e le sue ricadute nell'ordinamento nazionale, in *Diritto* penale e processuale, n. 10, 2024, p. 1367 ss.; I. CONTI, *La Direttiva U.E. 2024/1385 sulla lotta alla violenza sulla donna e alla violenza domestica*, in *IUS Penale*, 2024; M. FERRARI, *Violenza contro le donne: l'Unione europea adotta finalmente la direttiva (UE) 2024/1385*, in *Eurojus*, 17 giugno 2024; A. GRUEV-VINTILA, A. RURKA, *Transforming the understandings of domestic violence through coercive control in France*, in *Discover Global Society*, n. 2, 2024; L. KALB, *Novità normative*, in *Diritto penale e processuale,* 2024, p. 851; M. LOMBARDO, *In vigore la Direttiva sulla lotta alla violenza contro le donne e alla violenza domestica*, in *Altalex*, 13 giugno 2024; B. PEZZINI, *Una Direttiva in materia di lotta alla violenza contro le donne e alla violenza domestica*, in *Quaderni costituzionali*, n. 3, 2024, pp. 730-734; G. PIZZOLANTE, *Alcune riflessioni in tema di violenza domestica correlata alla libera circolazione e al diritto di soggiorno dei coniugi o dei partner extra UE*, in *Freedom Security & Justice Review*, n. 2, 2024, 322 ss.

[2] Considerando 1 della direttiva (UE) 2024/1385 del Parlamento europeo e

specificità connesse ai reati di violenza contro le donne e di violenza domestica, è apparso necessario stabilire un complesso di norme che affrontino in modo mirato il problema persistente di tale violenza, al fine di offrire una risposta concreta alle esigenze specifiche riconducibili alle singole vittime dei reati in esame. L'iniziativa muove dalla constatazione della insufficiente capacità delle disposizioni vigenti – tanto a livello dell'Unione, quanto di quello nazionale – di combattere e prevenire efficacemente la violenza contro le donne e la violenza domestica. In particolare, si evidenziano le lacune presenti nell'attuale panorama normativo, in quanto sebbene con le direttive 2011/36/UE e 2011/93/UE – riguardanti essenzialmente forme specifiche di tale violenza – e con la direttiva 2012/29/UE – con la quale si offre il quadro generale per le vittime di reato – si introducono alcune garanzie per le vittime, restano purtroppo senza risposte pertinenti le esigenze specifiche connesse a tali manifestazioni di reato[3].

Le disposizioni contenute in questa direttiva sono dirette a salvaguardare i diritti di tutte le vittime di condotte criminose consistenti in atti di violenza contro le donne o di violenza domestica, penalmente rilevanti ai sensi del diritto dell'Unione o nazionale.

Il riferimento a tali condotte criminose include anche i reati espressamente definiti nella presente direttiva, vale a dire le mutilazioni genitali femminili, i matrimoni forzati, la condivisione non consensuale di materiale intimo o manipolato, lo *stalking* online, le molestie online, il *cyberflashing*, l'istigazione alla violenza o all'odio online, e le condotte criminose contemplate da altri atti giuridici dell'Unione, in particolare le direttive 2011/36/UE e 2011/93/UE.

Nella definizione di violenza contro le donne rientrano pure i reati previsti dagli ordinamenti nazionali, come nel caso del femminicidio, dello stupro, delle molestie sessuali, dell'abuso sessuale, dello *stalking*, dei matrimoni precoci, dell'aborto forzato, della sterilizzazione forzata e delle diverse forme di violenza online, come le molestie sessuali online e il cyberbullismo.

del Consiglio, *sulla lotta alla violenza contro le donne e alla violenza domestica*, del 14 maggio 2024, in GUUE L, del 25 maggio 2024, pp. 1-36.

[3] *Ivi*, considerando 5.

In merito alla individuazione delle fattispecie di reato la direttiva formula alcune precisazioni.

Innanzitutto, quella domestica è una forma di violenza che potrebbe configurare un reato specifico ai sensi del diritto nazionale o rientrare tra i reati commessi all'interno della famiglia o del nucleo familiare, o tra coniugi o ex coniugi o partner, a prescindere che convivano o meno. Ciò non toglie che i singoli Stati membri possono ampliare la definizione di ciò che costituisce violenza contro le donne ai sensi del diritto penale nazionale. Si precisa pure che la presente direttiva non affronta l'intero spettro di condotte criminose consistenti in atti di violenza contro le donne[4].

In merito ai soggetti meritevoli di protezione, la fonte sovranazionale in esame premette che le misure ivi previste sono concepite per rispondere alle esigenze specifiche delle donne, delle ragazze e delle bambine, in quanto, come confermano dati e studi, sono vittime per antonomasia delle forme di violenza ivi contemplate, segnatamente la violenza contro le donne e la violenza domestica.

Ciò non significa che le misure in questione siano precluse ad altre persone, eventualmente destinatarie di queste forme di violenza.

Non a caso la direttiva in esame precisa che il termine "vittima" si riferisce a chiunque, indipendentemente dal genere, e, salvo diversa indicazione contenuta nella direttiva del 2024, con la conseguenza che tali persone dovrebbero beneficiare dei diritti connessi alla protezione delle vittime nonché all'accesso alla giustizia, alle particolari misure di assistenza e a quelle preventive[5].

In ragione di queste premesse sembra auspicarsi, sul punto, l'introduzione di una nozione ampia di vittima, al fine di agevolare l'estensione della disciplina di tutela anche a soggetti che, pur non appartenendo al genere femminile, subiscano la medesima fenomenologia criminosa.

Una particolare attenzione è destinata alla figura dei minori.

I minori che assistono ad atti di violenza domestica commessi all'interno della famiglia o del nucleo familiare subiscono generalmente un danno psicologico ed emotivo diretto, che incide sul loro svilup-

[4] *Ivi*, considerando 9.

[5] *Ivi*, considerando 12.

po e li espone ad un maggior rischio di soffrire malattie fisiche e mentali, sia a breve che a lungo termine.

Questa presa d'atto nei confronti dei minori testimoni di atti di violenza domestica è ritenuto un rilevante passo importante per assicurare loro una tutela efficace avverso quanto sofferto a causa della violenza domestica[6].

A questo proposito, merita di essere evidenziato come in materia di maltrattamenti contro familiari o conviventi, pur trattandosi di un reato abituale (richiedendo la reiterazione di un certo numero di condotte ai fini della tipicità del fatto), la giurisprudenza nazionale riconosca la sussistenza dell'aggravante, consistente nell'aver posto in essere il fatto in presenza del minore, anche qualora solo uno degli atti abituali si sia consumato dinanzi a quest'ultimo (con un evidente innalzamento della tutela del minore stesso)[7].

Sulla delimitazione dei fatti penalmente rilevanti ai fini dell'operatività della stessa fonte sovranazionale si riscontra una scelta che merita di essere evidenziata.

Il bilanciamento tra valori contrapposti induce ad affermare che la diffusione al pubblico – tramite il ricorso alle Tecnologie dell'Informazione e della Comunicazione (TIC) – di immagini, video o altro materiale ritraente atti sessualmente espliciti o le parti intime di una persona senza il consenso della persona non configura necessariamente un reato laddove risulti indispensabile per salvaguardare i diritti fondamentali tutelati dalla Carta dei diritti fondamentali dell'Unione europea, in particolare la libertà di espressione, compresa quella di ricevere e comunicare informazioni e idee in una società aperta e democratica, nonché la libertà delle arti e delle scienze, compresa quella accademica.

Inoltre, si ribadisce quanto previsto in altre fonti sovranazionali ovvero che il reato non dovrebbe riguardare il trattamento del materiale da parte delle autorità pubbliche, in particolare al fine di condurre procedimenti penali o di prevenire reati, individuarli e indagare su di essi, e gli Stati membri dovrebbero poter esentare una persona dalla

[6] *Ivi,* considerando 13.

[7] Cfr. Corte di Cassazione, Sezione 6, n. 40045, 21 ottobre 2022; ID., Sezione 6, n. 8323, 9 febbraio 2021.

responsabilità in determinate circostanze, come nel caso ad esempio di linee di assistenza telefonica o su Internet che trattano materiale per segnalare un reato alle autorità[8].

La disposizione sembrerebbe porre limiti all'applicazione dell'art. 612-*ter* c.p., paradigma punitivo dei fatti di *revenge porn*, in tutti i casi in cui la finalità perseguita dall'agente consista nella salvaguardia dei diritti fondamentali. In tal caso, si pone ovviamente il problema di stabilire quando e come questo obiettivo vada accertato, e, soprattutto, quali siano i limiti oltre i quali possa ritenersi sussistente una seppur celata finalità lesiva della vittima ritratta in video o immagini sessualmente espliciti.

Una particolare attenzione viene destinata alle vittime dei reati di violenza online con la conseguente formulazione di alcune proposte.

Innanzitutto, al fine di favorire l'esercizio del diritto di rimozione del materiale illegale relativo a tali reati, si sollecitano gli Stati membri ad incoraggiare la cooperazione in materia di autoregolamentazione tra i pertinenti prestatori di servizi intermediari.

In secondo luogo, per garantire che tale materiale sia tempestivamente individuato ed efficacemente contrastato e che le vittime siano adeguatamente assistite e sostenute, si chiede agli Stati membri di agevolare l'introduzione di misure di autoregolamentazione di tipo volontario, o di sensibilizzare in merito a quelle esistenti, come i codici di condotta.

In particolare, si prospetta la necessità di includere misure di autoregolamentazione per l'individuazione dei rischi sistematici, in particolare per rafforzare i meccanismi volti a contrastare la violenza online e migliorare la formazione del personale di tali prestatori intermediari di servizi, in modo da impegnarli nella prevenzione della violenza e nell'assistenza e sostegno alle vittime. Tali misure di autoregolamentazione potrebbero integrare l'azione a livello dell'Unione, in particolare nell'ambito del regolamento (UE) 2022/2065[9].

La sintesi di quanto fin qui programmato è rintracciabile nell'art. 1 della direttiva del 2024.

Le norme minime per "prevenire e combattere la violenza contro

[8] *Ivi*, considerando 20.

[9] *Ivi*, considerando 86.

le donne e la violenza domestica" sono espressamente individuate nella definizione dei reati e delle sanzioni in materia di sfruttamento sessuale femminile e minorile e di criminalità informatica; nei diritti delle vittime di tutte le forme di violenza contro le donne o di violenza domestica prima, durante e per un congruo periodo dopo il procedimento penale; nella protezione e nell'assistenza delle vittime e nella prevenzione previa assicurazione di un intervento precoce.

Le disposizioni destinate a conseguire tali finalità riguardano tutte le vittime di reati di violenza contro le donne e di violenza domestica a prescindere dal genere. A tal fine, rilevano le indicazioni presenti in questa direttiva nonché in altri atti giuridici dell'Unione o del diritto nazionale configuranti tale tipo di reato.

Sul piano della concreta assistenza delle vittime merita attenzione la previsione di cui all'art. 30, volta a garantire con la creazione delle case rifugio e delle altre sistemazioni temporanee di cui all'art. 9, par. 3, lett. a) della direttiva 2012/29/UE le esigenze delle vittime, tra cui quelle delle vittime ad alto rischio, assistendole nel percorso di recupero, fornendo loro condizioni di vita sicure, facilmente accessibili e adeguate ai fini del ritorno a una vita indipendente, e fornendo informazioni sui servizi di assistenza e di indirizzamento, anche per un'ulteriore assistenza medica.

2. *Le iniziative di denuncia del fatto*

L'accertamento dei fatti oggetto di attenzione in questa direttiva e le correlate iniziative a tutela della vittima sono tanto più facilitate quanto più tempestiva e completa sia l'informazione resa all'autorità competente ad intervenire.

A tal fine, la direttiva del 2024 pone una serie di indicazioni agli Stati, riguardanti modalità e tempi per la trasmissione della notizia relativa ad un reato di violenza contro le donne o di violenza domestica e, eventualmente, per la informazione di elementi di carattere probatorio anche in ragione della rilevante esigenza di evitare che a causa di tale iniziativa la vittima possa subire una vittimizzazione secondaria o ripetuta.

A questo proposito si rileva la particolare importanza attribuita

dalla direttiva alla circostanza che, al momento della denuncia del reato, la vittima sia indirizzata verso un punto di contatto specializzato, ove possibile, indipendentemente dalla presentazione di una formale denuncia per l'attivazione di una indagine penale. Infatti, si prevede che il punto di contatto destinatario della informazione sul fatto sia tanto un funzionario di polizia dotato di specifica formazione sul tema, quanto qualsiasi professionista purché formato per assistere le vittime.

In merito ai meccanismi idonei a comunicare l'informazione sulla violenza subita, la direttiva prevede la opportunità di utilizzare gli strumenti offerti dalla moderna tecnologia ovvero la possibilità di sporgere denuncia online o tramite altre tecnologie di comunicazione accessibili, a maggior ragione in occasione di reati informatici di condivisione non consensuale di materiale intimo o manipolato, di *stalking* online, delle molestie online, dell'istigazione alla violenza o all'odio online, definiti nella presente direttiva.

Il ricorso a tali modalità, tra l'atro, consentirebbe di allegare alla denuncia documenti o altro materiale utile a dimostrare i fatti, come ad esempio screenshot che attestino la presunta condotta violenta[10].

Quanto programmato in questo considerando suscita particolare attenzione, dal momento che potrebbe costituire il presupposto per la introduzione nel codice di procedura penale del nostro ordinamento di nuove modalità tecnologiche di allertamento delle autorità competenti.

Segnatamente, la predisposizione di un portale nazionale, dal quale possa risalirsi all'ufficio competente di prossimità, consentirebbe alle vittime di denunciare i fatti di reati in sicurezza, evitando, soprattutto nei piccoli centri, che l'aggressore si accorga dell'intervento degli organi di polizia. La previsione potrebbe costituire anche l'occasione per incentivare su base nazionale una campagna informativa sull'utilizzo di simili tecnologie, in parte già esistenti, come confermato dall'applicazione *YouPol* gestita dalla polizia di Stato. L'applicazione informatica permette all'operatore di polizia di aprire una chat sulla quale è possibile scambiarsi, in tempo reale, messaggi e file multimediali, come normalmente accade in un'applicazione di messaggistica istantanea. Inoltre, la nuova funzionalità di geolocalizzazione permette

[10] Ivi, considerando 30.

di fornire con immediatezza la posizione del segnalante, con evidente facilitazione di intervento.

La necessità di perfezionare tutti i meccanismi di informazione sul fatto inerente alla violazione subita non esclude che l'attivazione di indagini e il conseguente esercizio dell'azione penale – come nell'ipotesi di atti di stupro – prescindano dalla proposizione della querela o della denuncia da parte della vittima o del suo rappresentante.

Analogamente, il procedimento penale dovrebbe proseguire anche nel caso in cui la vittima ritiri la denuncia. Ciò non pregiudica la facoltà delle autorità responsabili dell'azione penale di interrompere il procedimento penale per altri motivi, ad esempio qualora concludano che non esiste materiale di carattere probatorio sufficiente per sostenere l'accusa[11].

A tal proposito, è opportuno ricordare che nel nostro ordinamento l'art. 609-*septies* c.p. prevede espressamente i casi nei quali i fatti di violenza sessuale divengono procedibili d'ufficio. In ogni caso, anche quando il reato è procedibile su istanza punitiva di parte, la disposizione appena richiamata sancisce il carattere irrevocabile della querela che, in via eccezionale, è suscettibile di proposizione entro 12 mesi e non entro il termine di 3 mesi previsto dall'art. 124 c.p.

L'onere da parte degli Stati membri di provvedere affinché la vittima possa denunciare – nonché allegare elementi conoscitivi, fatte salve le norme procedurali nazionali relative alla formalizzazione della presentazione delle prove – alle autorità competenti atti di violenza contro le donne o di violenza domestica attraverso canali accessibili – ricorrendo pure a modalità online o tramite altre tecnologie accessibili e sicure – di facile utilizzo e prontamente disponibili è disciplinato nell'art. 14 della direttiva in esame.

A tal fine, vengono formulate altre importanti indicazioni destinate a favorire l'attività di denuncia da parte delle vittime di tali violenze.

Innanzitutto si prescrive la possibilità di accedere al patrocinio a spese dello Stato, previa attuazione dell'art. 13 della direttiva 2012/29/UE nei singoli ordinamenti nazionali, nonché di adottare le misure necessarie a incoraggiare chiunque sia a conoscenza di atti di violenza contro le donne o di violenza domestica, o in buona fede so-

[11] *Ivi*, considerando 37.

spetti che atti di violenza siano avvenuti o che possano prodursi nuovi atti di violenza, a segnalarlo alle autorità competenti senza temere conseguenze negative.

Particolare attenzione viene dedicata alla necessaria professionalità dell'operatore destinatario della denuncia, in ragione della situazione in cui si trova la vittima di violenze, soprattutto se minore.

Per quanto concerne i professionisti della sanità soggetti a obblighi di riservatezza, la direttiva invita gli Stati membri ad adottare quanto necessario affinché possano segnalare alle autorità competenti i casi in cui abbiano fondati motivi per ritenere che sussista il rischio imminente che una persona subisca un danno fisico grave risultante da violenza contro le donne o da violenza domestica.

Se la vittima è un minore, fatte salve le norme sul segreto professionale oppure, se previsto dal diritto nazionale, il sigillo sacramentale o principi equivalenti, i professionisti soggetti agli obblighi di riservatezza a norma del diritto nazionale possano segnalare alle autorità competenti i casi in cui abbiano fondati motivi per ritenere che un minore abbia subito un danno fisico grave a causa di violenza contro le donne o di violenza domestica.

Se il minore è l'autore della segnalazione, gli Stati membri devono provvedere affinché le procedure di denuncia siano sicure, riservate, a misura di minore e accessibili con un linguaggio consono, in funzione della loro età e maturità.

Il coinvolgimento del minore impone una idonea professionalità da parte di tutti gli operatori in modo tale che i minori ricevano adeguata assistenza nelle procedure di denuncia, al fine di garantire che esse rispettino l'interesse superiore del minore.

Ciò comporta che, nell'ipotesi di coinvolgimento del titolare della responsabilità genitoriale negli atti di violenza, la capacità del minore di denunciare l'atto non sia subordinata al consenso della persona titolare della responsabilità genitoriale e che le autorità competenti adottino le misure necessarie per tutelare la sicurezza del minore prima che tale persona sia informata della segnalazione.

3. *Formazione e specializzazione degli attori del procedimento*

Si è già sottolineato come una tempestiva ed efficace tutela della vittima della violenza presupponga spesso l'intervento di un qualificato professionista[12].

Per evitare qualsiasi condizione ostativa alla denuncia del fatto da parte della vittima, soprattutto se la violenza è ascrivibile a parenti stretti o partner o comunque se la coercizione dall'autore del reato sia tale da impedire un qualsiasi contatto con le autorità competenti, la direttiva in esame indica agli Stati membri la necessità di garantire che le loro norme in materia di riservatezza non impediscano ai professionisti della sanità di segnalare alle autorità competenti i casi in cui abbiano fondati motivi per ritenere che vi sia un rischio imminente di danno fisico grave.

Il *favor* a segnalare i fatti di violenza non riguarda solo tali operatori. È il caso in cui a riconoscere casi di violenza domestica o di violenza contro le donne che riguardano i minori siano soltanto terzi che notano comportamenti irregolari o danni fisici nel minore stesso.

Per garantire forme efficaci di protezione dei minori da queste forme di violenza con la tempestiva adozione di misure adeguate, la direttiva ritiene che debba escludersi l'operatività del vincolo di riservatezza da parte del professionista – tanto in ambito sanitario, quanto in quello sociale o educativo – che entri in contatto con il minore vittima ove abbia fondati motivi per ritenere che il minore abbia subito un danno fisico grave.

Ciò significa che, ove il professionista proceda alla segnalazione della violenza, l'ordinamento nazionale deve escludere ipotesi di responsabilità per violazione della riservatezza.

È altresì indispensabile trovare sul punto una soluzione equilibrata in ragione delle contrastanti esigenze in gioco. Pertanto, andrebbe comunque tutelato il segreto professionale da parte degli avvocati coinvolti per l'esercizio delle loro funzioni professionali; così come, ove previsto dal diritto nazionale, dovrebbe essere tutelato anche il sigillo sacramentale o principi equivalenti applicabili al fine di salvaguardare la libertà di religione. La possibilità per i professionisti di se-

[12] *Ivi*, considerando 33.

gnalare tali casi di violenza lascia inoltre impregiudicate le norme nazionali in materia di segretezza delle fonti di informazione nel contesto dei media.

L'esigenza di specializzazione coinvolge soprattutto gli operatori giudiziari[13].

Sono proprio le peculiari circostanze connotanti i reati di violenza contro le donne e di violenza domestica a giustificare l'adozione di specifici orientamenti tanto per le forze dell'ordine, quanto per le autorità responsabili dell'esercizio dell'azione penale.

La tutela a favore di queste persone particolarmente vulnerabili può essere assicurata a condizione che vengano predisposte linee guida da seguire in ogni fase del procedimento penale, in modo da garantire tempestive iniziative finalizzate all'accertamento del fatto ed evitare che il meccanismo procedimentale comporti effetti di vittimizzazione a danno delle persone coinvolte.

Gli orientamenti per le autorità legittimate ad intervenire dovrebbero mirare all'adozione delle migliori pratiche da attuare sia in occasione del contraddittorio da instaurare con le vittime, sia dei successivi rapporti o nelle conseguenti informazioni da offrire, come nell'ipotesi dell'indicazione alle donne dei servizi di assistenza specialistica.

Si tratta di orientamenti che, probabilmente, necessitano di un periodico adeguamento anche in ragione dei segnali che provengono dagli stessi servizi di assistenza specialistica alle donne.

Così come si prospetta la stessa necessità in ordine agli orientamenti per le forze dell'ordine e le autorità responsabili dell'azione penale qualora si verifichino importanti sviluppi nei propri quadri giuridici o nella società in generale.

Ciò potrebbe includere i casi in cui vi sono modifiche sostanziali alle leggi esistenti o alla giurisprudenza consolidata o in cui emergono nuove tendenze o forme di violenza, in particolare quando gli sviluppi tecnologici portano a nuove forme di violenza online.

Nessun dubbio, poi, sull'opportunità che l'assistenza e il sostegno alle vittime siano prestati prima, durante e per un congruo periodo dopo il procedimento penale, come ad esempio verificabile ove necessitano ancora cure mediche per far fronte alle gravi conseguenze fisi-

[13] *Ivi*, considerando 49.

che o psicologiche della violenza oppure sia a rischio l'incolumità della vittima, in particolare a causa di dichiarazioni rese dalla stessa in sede processuale[14].

Nella direttiva si ribadisce che uno degli strumenti più idonei per assicurare costante assistenza alle vittime è rappresentato dalle linee nazionali di assistenza telefonica[15].

A tal fine la direttiva in esame sostiene, previa adeguata informazione, l'utilizzo del numero unico, gratuito, appositamente istituito a livello dell'Unione, ossia il "116 016", oltre ai numeri nazionali esistenti, disponibili 24 ore su 24.

Merita di essere sottolineata una duplice indicazione sul punto.

Da un lato, si ritiene indispensabile che tali linee di assistenza telefonica debbano essere gestite da servizi di assistenza specialistica, compresi i servizi di assistenza specialistica per le donne, conformemente alla prassi nazionale.

Dall'altro, si suggerisce che l'assistenza prestata attraverso tali linee di assistenza telefonica debba includere una consulenza psicologica e la fornitura di informazioni alle vittime in merito ai servizi in presenza, quali le case rifugio, i servizi di assistenza specialistica, altri servizi sociali e sanitari pertinenti o la polizia.

Nell'art. 25 la direttiva disciplina l'assistenza alle vittime prevedendo l'onere degli Stati membri di fornire la protezione e i servizi di assistenza specialistica necessari per rispondere in modo esauriente alle molteplici esigenze delle vittime, prestando tali servizi in una medesima sede e coordinandoli attraverso un punto di contatto.

I servizi in parola devono comprendere almeno l'assistenza medica di prima necessità e l'indirizzamento a ulteriori cure mediche, come previsto dal sistema sanitario nazionale, nonché i servizi sociali, il sostegno psicosociale, i servizi legali e i servizi di polizia, o informazioni su tali servizi e su come raggiungerli.

Nell'ipotesi di violenza sessuale, l'art. 26 richiede un più elevato standard di assistenza, mediante la creazione di centri antistupro o di centri anti-violenza sessuale adeguatamente attrezzati e facilmente accessibili, che possono far parte del sistema sanitario nazionale.

[14] *Ivi*, considerando 63.

[15] *Ivi*, considerando 66.

La finalità è quella di garantire un'assistenza efficace alle vittime e assicurare la gestione clinica dello stupro, anche prestando specifica assistenza in merito alla formazione e alla conservazione di materiali di carattere probatorio.

Con l'art. 29 la direttiva mette a punto la disciplina in materia di linee di assistenza telefonica per le vittime.

Premesso l'impegno da parte degli Stati membri di mettere a disposizione gratuitamente, senza alcuna interruzione temporale, le linee di assistenza telefonica a livello statale, per fornire informazioni e consulenza alle vittime, la direttiva precisa alcune modalità nel loro utilizzo.

Oltre a prevedere il ricorso anche ad altre tecnologie di comunicazione sicure e accessibili, comprese le applicazioni online, si precisa che la relativa gestione possa essere attribuita ai servizi di assistenza specialistica, purché siano sempre fornite in via riservata o tenendo debitamente conto dell'anonimato della vittima. Gli Stati membri sono incoraggiati a garantire che tali servizi telefonici per le vittime di violenza contro le donne siano raggiungibili attraverso il numero armonizzato a livello di Unione, il "116 016", oltre a qualsiasi numero o numeri nazionali esistenti, previa attivazione di adeguata informazione dell'esistenza e del numero delle linee di assistenza telefonica, anche mediante periodiche campagne di sensibilizzazione.

Se si tratta di vittime con disabilità, occorre fornire idonea assistenza per favorire l'accesso ai servizi attraverso il ricorso ad un linguaggio di facile comprensione.

Quest'ultima esigenza deve essere sempre conseguita, come dimostra l'espressa richiesta rivolta agli Stati membri di garantire la prestazione dei servizi in una lingua che le vittime comprendono, anche mediante un servizio di interpretazione telefonica.

Particolare attenzione viene dedicata alla formazione e informazione dei professionisti (art. 36).

La direttiva attribuisce agli Stati membri l'impegno di provvedere per assicurare ai funzionari che hanno probabilità di entrare in contatto con le vittime, come gli agenti di polizia e il personale giudiziario, una formazione sia generale che specialistica, offrendo informazioni mirate di livello adeguato ai loro contatti con le vittime, in modo che possano individuare, prevenire e affrontare i casi di violenza contro le

donne o di violenza domestica e interagire con le vittime in termini consoni al trauma, alla dimensione di genere e all'età del minore. La formazione comporta un approfondimento di dettaglio a proposito dei reati informatici, in ragione della specificità della violenza contro le donne e della violenza domestica.

Gli Stati membri provvedono affinché le autorità competenti a ricevere le segnalazioni di reati dalle vittime siano adeguatamente formate per agevolare la denuncia di tali reati e assistere le vittime in questo compito nonché per evitare la vittimizzazione secondaria.

Al fine di conseguire questi obiettivi si prevede la necessità di offrire una formazione specialistica ad una pluralità di professionisti.

Innanzitutto, l'attenzione è rivolta ai professionisti della sanità, ai servizi sociali e al personale educativo che hanno probabilità di entrare in contatto con le vittime, al fine di consentire loro di individuare i casi di violenza contro le donne o di violenza domestica e di indirizzarle verso servizi di assistenza specialistica.

Per tutti i professionisti della sanità interessati, compresi pediatri, ginecologi, ostetrici e personale sanitario che si occupa di assistenza psicologica, è prevista una formazione mirata per consentire di affrontare, in modo attento alle specificità culturali, le conseguenze fisiche, psicologiche e sessuali delle mutilazioni genitali femminili.

Quanto ai soggetti del potere giudiziario, fatte salve l'indipendenza della magistratura e le differenze nell'organizzazione del potere giudiziario in tutta l'Unione, si prevedono misure necessarie per garantire che sia fornita una formazione sia generale che specialistica ai giudici e ai pubblici ministeri coinvolti nei procedimenti penali e nelle indagini in relazione agli obiettivi della presente direttiva e che tale formazione sia adeguata alle funzioni di tali giudici e pubblici ministeri. La formazione è basata sui diritti umani, incentrata sulle vittime e sensibile alle specificità di genere, delle persone con disabilità e dei minori.

Altri destinatari espressamente indicati sono quelli che esercitano la professione forense: senza intaccare la loro indipendenza, agli Stati membri spetta l'obbligo di raccomandare ai responsabili della formazione degli avvocati di offrire una formazione sia generale che specialistica per sensibilizzare maggiormente gli avvocati alle esigenze delle vittime e interagire con le vittime in modo consono al trauma, alla dimensione di genere e all'età dei minori.

Per il personale con funzioni di vigilanza sul luogo di lavoro, nel settore pubblico come in quello privato, è prevista una formazione per imparare a riconoscere, prevenire e affrontare le molestie sessuali sul lavoro, ove queste ultime costituiscano reato ai sensi del diritto nazionale.

L'obiettivo della formazione professionale non dimentica gli operatori dell'informazione: senza interferire sulla libertà e sul pluralismo dei media, gli Stati membri devono incoraggiare e sostenere attività di formazione per i media a cura di organizzazioni professionali, organismi di autoregolamentazione e rappresentanti del settore o altri organismi indipendenti, al fine di combattere le rappresentazioni stereotipate di donne e uomini, le raffigurazioni sessiste delle donne e la colpevolizzazione delle vittime nei media, così da ridurre il rischio di violenza contro le donne e di violenza domestica.

4. *Attività investigativa e pericoli di dispersione probatoria*

Alla luce delle specificità della violenza contro le donne e della violenza domestica, nonché del maggior rischio che la vittima possa ritirare la denuncia pur essendo stata vittima di un reato, è importante che le prove pertinenti vengano raccolte nelle primissime fasi del procedimento penale in maniera esaustiva, conformemente alle norme procedurali nazionali applicabili[16].

A questo proposito, meritano un breve richiamo quelle soluzioni normative destinate ad assicurare priorità in ordine alla conduzione delle indagini, in modo da riservare una corsia preferenziale ai reati in materia di violenza domestica e di genere[17]. Sempre in materia, le misure di prevenzione personali di cui al codice antimafia possono rappresentare un utile strumento di tutela, soprattutto in ragione del loro frequente utilizzo in guisa di misure cautelari.

[16] *Ivi*, considerando 31.

[17] Per le riforme apportate, sul punto, nel codice di procedura penale italiano cfr. in questo Volume R. ALFANO, *Le scelte del legislatore italiano: attività investigativa e procedimento cautelare "speciale"/Las opciones del legislador italiano: actividad de investigación y procedimientos cautelares "especiales"*, in questo Volume, pp. 455-473.

Ai fini dell'accertamento del fatto, si sottolinea l'opportunità di attivare misure idonee per consentire alle autorità competenti di acquisire e conservare i risultati dell'attività investigativa, soprattutto quelli dotati di particolare attitudine probatoria.

Tali misure potrebbero consistere ad esempio nell'imporre ai prestatori di servizi di *hosting* o di altri servizi intermediari interessati di trasmettere il materiale alle autorità o di conservarlo per un periodo di tempo limitato che non si protragga oltre il necessario. Qualunque misura di questo tipo dovrebbe garantire la sicurezza del materiale, limitarsi a quanto ragionevole e proporzionato e rispettare le norme di protezione dei dati personali applicabili[18].

La particolare vulnerabilità delle vittime dei reati di violenza in esame e la stessa natura traumatica della violenza sessuale, compreso lo stupro, esigono una risposta improntata a grande sensibilità da parte di un personale specializzato e appositamente formato.

Appare evidente che le vittime di questo tipo di violenza hanno immediato bisogno di sostegno per il trauma subito, unitamente a perizie medico-legali immediate, idonee a fornire elementi probatori da utilizzare per le determinazioni inerenti all'esercizio dell'azione penale.

Una efficace assistenza psicologica e medica impone l'allestimento di centri antistupro o centri antiviolenza sessuale, disponibili in numero sufficiente e adeguatamente distribuiti sul territorio di ciascuno Stato membro, tenendo conto della geografia e della composizione demografica degli Stati membri interessati. Si ribadisce, insomma, l'importanza che gli Stati membri garantiscano un'assistenza specifica per tali vittime, da realizzare nel rispetto delle norme più rigorose in materia di vita privata e riservatezza[19].

Queste indicazioni costituiscono l'oggetto della previsione contenuta nell'art. 15, riguardante lo svolgimento e le iniziative da attuare nel corso delle indagini sui reati di violenza contro le donne.

L'esigenza evidenziata nella fonte sovranazionale riguarda, da un lato, l'attribuzione di competenze specifiche nei confronti degli operatori legittimati ad intervenire nel corso dell'attività investigativa e, dall'altro, la disponibilità di efficaci strumenti investigativi per indaga-

[18] Direttiva (UE) 2024/1385, cit., considerando 55.

[19] *Ivi*, considerando 64.

re e perseguire efficacemente le condotte penalmente rilevanti, in particolare per raccogliere, analizzare e procurarsi prove elettroniche nei casi di criminalità online.

La celerità costituisce la connotazione principale della previsione ora in esame.

Innanzitutto, si stabilisce che gli atti di violenza contro le donne o di violenza domestica denunciati siano trattati e deferiti "senza indugio" alle autorità competenti per le indagini e per l'esercizio dell'azione penale nonché ai fini dell'adozione delle misure di protezione.

"Senza indebito ritardo" le autorità competenti che sospettano l'avvenuta commessione di un reato devono indagare in modo efficace, a seguito di una denuncia o di propria iniziativa, su atti di violenza contro le donne o di violenza domestica.

Sempre "senza indebito ritardo" le autorità competenti indirizzano la vittima verso i professionisti della sanità o i servizi di assistenza al fine di assicurare quella assistenza specialistica idonea, tra l'altro, a fornire quegli accertamenti probatoriamente rilevanti.

Si precisa, inoltre, che le vittime sono informate dell'importanza della raccolta di tali prove "quanto prima".

Ulteriore indicazione prevede che gli Stati membri si adoperino affinché le indagini o l'azione penale in relazione ad atti di stupro non siano subordinate alla querela o alla denuncia della vittima o del suo rappresentante e che il procedimento penale non sia interrotto per il solo fatto che la querela o la denuncia è stata ritirata.

Per quanto concerne il profilo probatorio, va evidenziata pure la previsione di cui all'art. 20, secondo la quale non è preclusa l'ammissione di prove relative al comportamento sessuale passato della vittima o ad altri aspetti della sua vita privata a quello connessi, ove però ciò sia pertinente e necessario.

Un'ultima riflessione deriva dall'art. 25, riguardante l'assistenza specialistica alle vittime, laddove si evidenzia che gli orientamenti e protocolli espressamente previsti comprendono la conservazione e la documentazione delle prove e la loro ulteriore trasmissione ai centri medico-legali competenti conformemente al diritto nazionale.

5. *La protezione della vittima anche mediante il ricorso agli ordini dell'autorità procedente*

Per garantire alla vittima un'assistenza e una protezione complete, tutte le autorità e gli organismi competenti, non solo le forze dell'ordine e le autorità giudiziarie, dovrebbero partecipare alla valutazione dei rischi per la vittima stessa e di misure di assistenza adeguate sulla base di orientamenti chiari emanati dagli Stati membri. Tali orientamenti dovrebbero indicare i fattori da considerare per valutare il rischio che rappresenta l'autore del reato o l'indagato, anche tenendo conto del fatto che un indagato per reati minori può essere altrettanto pericoloso di un indagato per reati più gravi, soprattutto in caso di violenza domestica e *stalking*. Le autorità competenti dovrebbero riesaminare la valutazione individuale a intervalli regolari per garantire che le nuove esigenze di protezione o di sostegno della vittima non restino senza risposta. Ad esempio, tale riesame potrebbe avvenire in fasi importanti del processo, come l'inizio di un procedimento giudiziario, la pronuncia di una sentenza o di un'ordinanza, o nel contesto di un procedimento di revisione degli accordi per l'affidamento o del diritto di visita[20].

L'auspicio intende sollecitare l'introduzione di nuove disposizioni processuali finalizzate alla disciplina di specifici doveri di valutazione periodica anche a carico degli organi di polizia ovvero dell'autorità giudiziaria (intesa in senso ampio). L'obiettivo sembrerebbe essere quello di evitare che, nonostante l'avanzamento del procedimento penale, la presunta vittima del fatto oggetto di accertamento rimanga "sola", subendo gli effetti negativi della erronea valutazione dei rischi compiuta inizialmente. L'aggiornamento della valutazione dovrebbe realizzarsi attraverso un flusso informativo tra organi procedenti e vittima, al fine di alimentare una interlocuzione costante che consenta un intervento tempestivo (attraverso la richiesta di misure cautelari o preventive) a fronte di mutate esigenze di tutela.

Senza alcun dubbio nella direttiva in esame si ipotizzano diverse tipologie di ordini la cui esecuzione mira a tutelare con efficacia le vit-

[20] *Ivi*, considerando 40.

time delle violenze: ordini urgenti di allontanamento, ordinanze restrittive e ordini di protezione[21].

Senza che tali misure si sostituiscano all'arresto e alla detenzione di indagati e autori di reati, i vari ordini possono trovare attuazione, ad esempio, quando il danno è imminente o si è già concretizzato e può essere nuovamente inflitto. Se le misure, ai sensi del diritto nazionale, sono soggette a una richiesta da parte della vittima, quest'ultima deve essere informate della possibilità di richiederle[22].

Gli ordini di protezione possono comprendere il divieto per l'autore del reato o l'indagato di accedere a determinate località, di avvicinarsi alla vittima o alle persone a carico a una distanza inferiore a quella prescritta o di contattarla anche attraverso interfacce online. Gli ordini di protezione possono comprendere anche il divieto di detenere armi da fuoco o letali, ove necessario.

Gli ordini urgenti di allontanamento, le ordinanze restrittive o gli ordini di protezione dovrebbero essere emessi per un periodo specifico oppure fino alla loro modifica o revoca[23].

Si sottolinea l'utilità di far ricorso al monitoraggio elettronico, in quanto consente, ove possibile, di assicurare il rispetto di ordini urgenti di allontanamento, ordinanze restrittive e ordini di protezione, di registrare prove di violazioni di tali misure e di potenziare la vigilanza sugli autori di reati. Tale monitoraggio opera a condizione che sia disponibile, opportuno e pertinente, tenendo conto delle circostanze del caso e della natura giuridica del procedimento.

In caso di ricorso al monitoraggio elettronico, le vittime dovrebbero essere sempre informate sulle sue capacità e sui suoi limiti[24].

Per preservarne l'efficacia, le violazioni degli ordini urgenti di allontanamento, delle ordinanze restrittive e degli ordini di protezione dovrebbero essere soggette a sanzioni. Tali sanzioni possono avere carattere penale o non penale e possono comprendere pene detentive, ammende o altra sanzione che sia effettiva, proporzionata e dissuasiva. È essenziale che le vittime abbiano la possibilità di essere informate di

[21] *Ivi*, considerando 43.
[22] *Ivi*, considerando 44.
[23] *Ivi*, considerando 45.
[24] *Ivi*, considerando 46.

una violazione degli ordini urgenti di allontanamento, delle ordinanze restrittive o degli ordini di protezione, qualora tale violazione si possa ripercuotere sulla loro sicurezza. Poiché le violazioni degli ordini urgenti di allontanamento, delle ordinanze restrittive o degli ordini di protezione possono aumentare i rischi e richiedere la messa in atto di un'ulteriore protezione, dopo la segnalazione di una violazione dovrebbe essere presa in considerazione, se necessario, una revisione della valutazione individuale[25].

Le informazioni relative ai programmi di intervento disponibili dovrebbero essere fornite a un autore o indagato di reati di violenza di cui alla presente direttiva che sia oggetto di un ordine urgente di allontanamento, di un'ordinanza restrittiva o di un ordine di protezione[26].

Ferma restando l'eventuale adozione di misure adeguate a prevenire la violenza contro le donne e la violenza domestica (art. 34), l'art. 16 della direttiva specifica le tipologie di misure prescrivibili sulla base della valutazione individuale delle esigenze di protezione delle vittime.

In aggiunta agli obblighi della valutazione individuale a norma dell'art. 22 della direttiva 2012/29/UE, gli Stati membri provvedono affinché, almeno nei confronti delle vittime di violenza sessuale e di violenza domestica, siano soddisfatti gli obblighi di tutela delle vittime di violenza.

Si prevede, pertanto, l'onere in capo agli Stati membri di provvedere affinché le autorità competenti, sulla base della valutazione individuale, adottino misure di protezione adeguate.

Tra tali misure possono rientrare: a) le misure di cui agli artt. 23 e 24 della direttiva 2012/29/UE (protezione delle vittime nel corso del procedimento penale e protezione dei minori); b) ordini urgenti di allontanamento, ordinanze restrittive e ordini di protezione a norma dell'art. 19 della presente direttiva; c) ulteriori misure diverse da quelle di cui alle lettere a) e b) del presente paragrafo per gestire il comportamento dell'autore del reato o indagato, in particolare a norma dell'art. 37 della presente direttiva.

[25] *Ivi*, considerando 47.

[26] *Ivi*, considerando 81.

Ove necessario, la valutazione individuale è effettuata in collaborazione con altre autorità competenti a seconda della fase del procedimento e con i pertinenti servizi di assistenza, quali i centri per la protezione delle vittime, i servizi specializzati, i servizi sociali, i professionisti della sanità, le case rifugio per donne, i servizi di assistenza specialistica e altri pertinenti portatori di interessi.

Occorre premettere, sul punto, che è attribuito agli Stati membri il potere di stabilire orientamenti per i casi di violenza contro le donne o di violenza domestica nei confronti delle autorità competenti che agiscono nei procedimenti penali, compresi orientamenti sull'azione penale. Tali orientamenti sono attenti alla prospettiva di genere, hanno natura consultiva e possono includere linee guida anche per l'adozione di ordini (art. 21).

A seguito della valutazione individuale di cui all'art. 16 della direttiva le autorità competenti valutano le esigenze individuali di assistenza della vittima, adottando i provvedimenti più idonei (art. 17).

A questo proposito, la direttiva indica presupposti e conseguenti misure adottabili, incidenti sulle libertà riconducibili alla persona oggetto di investigazione (art. 19).

In ipotesi di pericolo immediato per la salute o l'incolumità della vittima o delle persone a suo carico, le autorità competenti dispongano del potere di emettere, senza indebito ritardo, provvedimenti che ingiungono all'autore o indagato di reati di violenza di cui alla presente direttiva di allontanarsi dalla residenza della vittima o delle persone a suo carico per un periodo di tempo sufficiente, e che vietano a detto autore del reato o indagato di entrare nella residenza o nel luogo di lavoro della vittima, o di avvicinarsi oltre una distanza prestabilita, ovvero di contattare in qualsiasi modo la vittima o le persone a suo carico.

Alle autorità competenti è pure attribuito il potere di adottare ordinanze restrittive o ordini di protezione per assicurare, per il tempo necessario, protezione alle vittime da qualsiasi atto di violenza contemplato dalla presente direttiva, disciplinando tanto l'iniziativa, quanto l'eventuale violazione dell'ordine.

Non si trascura di sottolineare l'esigenza di assicurare una tempestiva informazione a favore della vittima.

Agli Stati membri è imposto di prevedere una disciplina mediante la quale alla vittima sia offerta la possibilità di essere informata, senza

indebito ritardo, in caso di violazione di un ordine urgente di allontanamento, di un'ordinanza restrittiva o di un ordine di protezione, che potrebbe avere un impatto sulla sua incolumità.

In ragione delle soluzioni già vigenti nei vari ordinamenti nazionali, come verificabile anche per quello italiano, merita di essere sottolineata la precisazione secondo la quale questa previsione della direttiva non obbliga gli Stati membri a modificare i sistemi nazionali per quanto riguarda la qualifica penale, civile o amministrativa degli ordini urgenti di allontanamento o degli ordini di protezione.

Infine, l'art. 23 evidenzia i limiti posti all'adozione degli ordini.

Si stabilisce, infatti, che gli ordini e altre misure adottabili siano disposti secondo procedure trasparenti e soggetti ad adeguate garanzie, in modo che la loro esecuzione sia limitata a quanto necessario e proporzionato rispetto alla vicenda oggetto di esame, tenendo sempre conto dei diritti e degli interessi di tutte le parti coinvolte, compresi i loro diritti fondamentali a norma della Carta.

In questo contesto, altre precisazioni riguardano gli ordini di rimozione di materiale online. Si prevede, infatti, che i prestatori di servizi di *hosting*, gli altri pertinenti prestatori di servizi intermediari e i fornitori di contenuti interessati da questo ordine di rimozione abbiano diritto a un ricorso giurisdizionale effettivo. Tale diritto comprende il diritto di impugnare tale ordine dinanzi agli organi giurisdizionali dello Stato membro dell'autorità competente che lo ha emesso.

La rimozione del materiale online o la disabilitazione dell'accesso al medesimo conformemente agli ordini o altre misure adottate non deve impedire, però, alle autorità competenti il potere di procurarsi, senza indebito ritardo, le prove necessarie per indagare e perseguire i reati di violenza oggetto della direttiva in esame.

6. *Durata del procedimento penale e prescrizione del reato*

L'esigenza di trovare una soluzione equilibrata tra l'esigenza di assicurare una durata ragionevole del procedimento penale attivato per l'accertamento dei reati di violenza alle donne e di violenza domestica e quella di fissare termini certi di prescrizione di tali reati trova indicazioni anche in questa direttiva del 2024.

A questo proposito, occorre sottolineare come in via di premessa[27], la fonte sovranazionale sembra circoscrivere l'esigenza di adottare le misure necessarie a prevedere un termine di prescrizione che consenta di condurre le indagini, esercitare l'azione penale, svolgere il processo e adottare la decisione giudiziaria solo all'ipotesi del reato di matrimonio forzato. Si aggiunge, a questo proposito, come in ragione della circostanza che le vittime di matrimoni forzati sono spesso minori, i termini di prescrizione dovrebbero protrarsi per un periodo di tempo sufficiente e proporzionale alla gravità del reato in questione, per consentire alla vittima di vedere perseguito il reato dopo avere raggiunto i 18 anni di età.

In realtà, la disciplina contenuta nella direttiva del 2024 indica una differente operatività di tale esigenza.

Infatti, ai sensi dell'art. 13, è previsto che gli Stati membri devono adottare le misure necessarie a prevedere un termine di prescrizione che consenta di condurre le indagini, esercitare l'azione penale, svolgere il processo e adottare la decisione giudiziaria in merito ai reati di cui agli artt. 3 e 9 entro un congruo lasso di tempo successivamente alla commissione di tali reati, al fine di contrastarli efficacemente. Il termine di prescrizione è commisurato alla gravità del reato in questione.

In ragione del perimetro indicato, i reati coinvolti sono: le mutilazioni di genitali femminili; l'istigazione al matrimonio forzato, la condivisione non consensuale di materiale intimo o manipolato, lo *stalking* online, le molestie online, il concorso tra questi reati, compresa pure l'Istigazione alla violenza o all'odio online.

Se la vittima è un minore, il termine di prescrizione per i reati di cui all'art. 3 inizia a decorrere non prima che la vittima abbia compiuto i 18 anni di età.

7. *I limiti dell'intervento della giurisdizione penale nazionale*

In conclusione, ulteriori preziose indicazioni per quanto concerne il profilo processuale sono offerte dall'art. 12 in merito al perimetro di operatività della giurisdizione penale nei singoli ordinamenti nazionali.

[27] *Ivi*, considerando 16.

Il primo rilievo riguarda l'individuazione del catalogo di reati per il quali può attivarsi la giurisdizione nazionale.

L'art. 12 della direttiva del 2024 rinvia agli artt. da 3 a 9 della stessa ovvero alle seguenti fattispecie: le mutilazioni di genitali femminili, il matrimonio forzato, la condivisione non consensuale di materiale intimo o manipolato, lo *stalking* online, le molestie online, l'istigazione alla violenza o all'odio online, le ipotesi di istigazione, favoreggiamento, concorso e tentativo di cui all'art. 9 della stessa direttiva.

Per tali reati la giurisdizionale nazionale è attivabile ove il reato è stato commesso in tutto o in parte sul proprio territorio oppure l'autore del reato è un suo cittadino.

È previsto, altresì, che uno Stato membro informi la Commissione in merito alla decisione di estendere la propria giurisdizione ai reati di cui agli artt. da 3 a 9 commessi al di fuori del proprio territorio quando il reato è stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio oppure l'autore del reato risiede abitualmente nel suo territorio.

In ragione di interventi mirati sull'elenco di reati indicato, si adottano alcune specifiche regole operative.

Innanzitutto, facendo rinvio al catalogo di reati in precedenza evidenziato – con esclusione dell'ipotesi del matrimonio forzato – è previsto che la giurisdizione nazionale operi nei casi in cui il reato sia stato commesso tramite tecnologie di informazione e di comunicazione cui l'autore ha avuto accesso dal loro territorio, a prescindere dal fatto che il prestatore di servizi intermediari sia basato o meno sul loro territorio.

Per le sole ipotesi di matrimonio forzato e di condivisione non consensuale di materiale intimo o manipolato, ove l'autore del reato sia un suo cittadino, ciascuno Stato membro deve provvedere affinché la sua giurisdizione non sia subordinata alla condizione che la condotta sia punita come reato nello Stato in cui è stata commessa.

Sempre nell'ipotesi in cui l'autore del reato sia un suo cittadino, devono adottarsi le misure necessarie per garantire che l'esercizio della loro giurisdizione non sia subordinato alla condizione che il reato sia perseguibile solo su querela della vittima nel luogo in cui è stato commesso il reato o su denuncia dello Stato sul cui territorio è stato commesso il reato.

La direttiva conferma pure il collegamento tra accertamento della responsabilità penale e la pretesa risarcitoria promossa da parte della vittima. L'art. 24 disciplina l'ipotesi del risarcimento a carico dell'autore del reato, stabilendo che gli ordinamenti nazionali prevedano il diritto della vittima di chiedere all'autore del reato, a norma del diritto nazionale, il risarcimento integrale dei danni derivanti da reati di violenza contro le donne e di violenza domestica.

A questo punto, dal quadro complessivo risultante dalla direttiva 2024/1385/UE risulta chiaro l'intento perseguito dal legislatore sovranazionale e altrettanto evidenti gli ambiti in cui sono destinati ad operare gli interventi programmati.

I risultati attesi, in ordine al livello di assistenza concretamente adottabile nei confronti delle vittime di violenza alle donne e di violenza domestica, nonché di tempestivo intervento dei vari operatori coinvolti al fine di prevenire o accertare tali condotte criminose, saranno condizionati dal perfezionamento dei singoli ordinamenti nazionali in attuazione di questa direttiva, ma è facile prevedere che si concretizzeranno, soprattutto, in misura del livello di professionalità e di specializzazione assicurato e in ragione delle risorse personali, strutturali e finanziarie destinate all'obiettivo contenuto nella direttiva del 2024.

Abstract

In attuazione di quanto previsto dalla direttiva (UE) 2024/1385, destinata fornire un quadro giuridico generale in grado di prevenire e combattere efficacemente la violenza contro le donne e la violenza domestica in tutta l'Unione, con lo specifico obiettivo di rafforzare e di introdurre – ove non già previsto dagli ordinamenti dei singoli Stati – misure efficaci per "la protezione delle vittime e l'accesso alla giustizia, l'assistenza alle vittime, una migliore raccolta di dati, la prevenzione, il coordinamento e la cooperazione" (v. considerando n. 1), il contributo mira ad evidenziare e ad analizzare le disposizioni di carattere processualpenalistico, al fine di offrire una lettura sistematica e coordinata in ragione della tipologia degli istituti coinvolti.

KEYWORDS: direttiva (UE) 2024/1385 – violenza di genere – diritto penale processuale – vittima – Unione europea

EL MARCO JURÍDICO GENERAL PROPUESTO EN LA FUENTE SUPRANACIONAL: DE LA PROTECCIÓN DE LAS VÍCTIMAS AL ACCESO A LA JUSTICIA

En aplicación de lo previsto en la directiva (UE) 2024/1385, destinada a establecer un marco jurídico general para prevenir y combatir eficazmente la violencia contra las mujeres y la violencia doméstica en toda la Unión, con el objetivo específico de fortalecer e introducir – cuando no estén ya previstas en las legislaciones de los distintos Estados – medidas eficaces para "la protección de las víctimas y el acceso a la justicia, la asistencia a las víctimas, la mejor recogida de datos, la prevención, la coordinación y la cooperación" (v. considerando n. 1), la contribución pretende resaltar y analizar las disposiciones procesales-penales, con el fin de ofrecer una lectura sistemática y coordinada teniendo en cuenta el tipo de instituciones implicadas.

PALABRAS CLAVE: directiva (UE) 2024/1385 – violencia de género – derecho procesal penal – víctima – Unión Europea

LE SCELTE DEL LEGISLATORE ITALIANO: ATTIVITÀ INVESTIGATIVA E PROCEDIMENTO CAUTELARE "SPECIALE"

Rocco Alfano[*]

SOMMARIO: 1. L'avvio del percorso legislativo italiano tra Convenzione di Istanbul e sentenza *Talpis*. – 2. La legge n. 69/2019 e il primo ambito applicato del cd. Codice Rosso. – 3. Le principali novità sostanziali e processuali della Legge n. 69/2019. – 4. L'ulteriore passo in avanti effettuato con la Riforma Cartabia e la rinnovata figura del P.M. civile. – 5. Il Codice Rosso rinforzato e la nuova centralità e specialità della fase cautelare. – 6. Conclusione: una specialità fino in fondo?

1. *L'avvio del percorso legislativo italiano tra Convenzione di Istanbul e sentenza* Talpis

Il percorso legislativo italiano, a partire dalla Legge 19 luglio 2019 n. 69, recante "Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere" (cd. legge istitutiva del Codice Rosso), si è mosso lungo le direttrici già a suo tempo segnate dalla Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica di Istanbul dell'11 maggio 2011, ratificata in Italia con la Legge 27 giugno 2013, n. 77.

Ci riferiamo ai quattro pilastri di quella Convenzione, indicati con l'ormai nota locuzione delle "4 P": prevenire, proteggere, perseguire e pratiche integrate.

In particolare, la Convenzione di Istanbul dedica il capitolo VI (articoli da 49 a 58) agli aspetti processuali connessi ai reati di violenza di genere e individua le misure, di vario tipo, che gli Stati aderenti devono adottare per garantire il pieno rispetto dell'accordo internazionale.

[*] Procuratore della Repubblica Aggiunto presso il Tribunale di Salerno. E-mail: rocco.alfano@giustizia.it.

Nel caso italiano il legislatore del 2019 si è mostrato maggiormente attento a due di quei quattro pilastri ovvero alle azioni di prevenzione dei reati e di protezione delle vittime.

La scelta di un percorso legislativo che ha voluto fare del contrasto alla violenza di genere una priorità o meglio una vera e propria emergenza giudiziaria, oltre ad essere stata una opzione politica verso un tema sempre più attenzionato dall'opinione pubblica, è stata anche la conseguenza della sentenza in data 2/03/2017 della Corte europea dei diritti dell'uomo di condanna dell'Italia per il noto caso *Talpis*.

Con questa pronuncia, la Corte di Strasburgo ha affermato che il ritardo, con il quale le autorità competenti, alle quali era stato denunciato un caso di violenza domestica, avevano adottato le misure necessarie a tutelare la vittima, integrava la violazione dell'art. 2 della Convenzione europea dei diritti dell'uomo, relativo al diritto alla vita, in quanto di fatto aveva privato di qualsiasi effetto la denuncia della violenza subita.

Secondo la stessa decisione, quella vicenda costituiva anche violazione dell'art. 3 della medesima Convenzione, sotto un profilo procedurale per il mancato adempimento degli obblighi positivi di protezione della vittima, atteso il lungo periodo di inattività da parte delle autorità prima di avviare il procedimento penale per lesioni aggravate definito poi con la successiva archiviazione del caso.

La medesima sentenza, infine, ha ritenuto che il venir meno di uno Stato all'obbligo di protezione delle donne contro le violenze domestiche, si traduceva in una violazione del loro diritto a una uguale protezione di fronte alla legge e, pertanto, era pure discriminatoria. In particolare, si è evidenziato in motivazione come occorresse prevenire situazioni di stallo nell'avvio delle indagini dopo la denuncia, considerato che, proprio in ragione di tali ritardi e della connessa sottovalutazione del rischio, il nostro paese era stato condannato da parte della Corte per mancata adozione di adeguate ed efficaci misure di protezione.

Per tutti questi motivi quella sentenza è stata considerata, a ragione, come una vera e propria "*sentenza monito*" per il legislatore italiano.

2. *La Legge n. 69/2019 e il primo ambito applicativo del cd. Codice Rosso*

In data 9 agosto 2019 è entrata in vigore la Legge n. 69, istitutiva del Codice Rosso, e finalmente è stato dato seguito ai moniti della Corte di Strasburgo.

Deve evidenziarsi che quella legge si occupa di un fenomeno – definito violenza domestica e di genere – ove il metronomo della sensibilità sociale oscilla non solo tra prevenzione e protezione penale (in termini processuali si tratta delle esigenze cautelari della fase delle indagini preliminari), ma anche tra prevenzione e assistenza sociale fuori del procedimento penale (prima, durante e dopo lo stesso).

Una prima scelta del legislatore del 2019 è già nell'utilizzo del termine violenza domestica e non violenza intrafamiliare, che sta a significare una scelta verso il concetto di *domus* di stampo quasi romano, ovvero di luogo di relazione affettive stabili, e non verso il concetto tradizionale di famiglia, che avrebbe escluso le unioni civili e le convivenze stabili.

Scelta non altrettanto di modernità e di lungimiranza è stata il riportare ancora la definizione di "violenza di genere" e non quella di "violenza contro le donne", cioè replicando meramente i termini della Convenzione di Istanbul, nonostante che già la prima direttiva UE in materia[1] parlasse espressamente di violenza contro le donne, atteso che già risultava dai dati statistici che il genere prevalentemente, se non quasi esclusivamente, offeso da quella violenza era il genere femminile[2].

In via preliminare, deve circoscriversi l'ambito di operatività della nuova normativa: in quella prima occasione sono stati considerati, da una norma processuale (il comma 1 *ter* aggiunto all'art 362 c.p.p.) reati da Codice Rosso le seguenti fattispecie delittuose: tentato omicidio

[1] La Direttiva (UE) 2012/29 del Parlamento europeo e del Consiglio, *che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI*, del 25 ottobre 2012, in GUUE L 315, del 14 novembre 2012, pp. 57-73, dettava le prime norme europee in materia di diritti, assistenza e protezione delle vittime dei reati di violenza di genere.

[2] A. ORIOLO, A. CASTALDO, A. DI STASI, M. NINO (a cura di) *Criminalità transnazionale e Unione Europea*, Napoli, 2024, pp. 215 – 255, sulla importanza della tutela dei valori comuni dell'Unione europea, fra i quali anche la tutela delle donne.

(art. 56-575 c.p.), maltrattamenti contro familiari e conviventi (art. 572 c.p.), violenza sessuale, aggravata e di gruppo (artt. 609-*bis*, 609-*ter* e 609-*octies* c.p.), atti sessuali con minorenne (art. 609-*quater* c.p.), corruzione di minorenne (art. 609-*quinquies* c.p.), atti persecutori (art. 612-*bis* c.p.); diffusione illecita di immagini o video sessualmente espliciti (art. 612-*ter* c.p.); deformazione dell'aspetto della persona mediante lesioni permanenti al viso (art. 583-quinquies, c.p.); lesioni personali (art. 582 c.p.) aggravate ai sensi e degli artt. 576 e 577 c.p., ovvero agevolati da rapporti familiari, da relazioni affettive o da connessione con maltrattamenti o atti persecutori (cd. reati-spia).

Si tratta, a ben vedere, di una serie di ipotesi non tutte omogenee, che potremmo individuare qui, quale nucleo fondamentale, in ipotesi di violenze verificatesi all'interno di quel concetto di *domus* ovvero di luogo di relazione affettive stabili sopra già indicato (tra coniugi, conviventi, legati in unione civile, prossimi familiari, parenti e affini), ovvero in quelle che la Cassazione definisce le "relazioni strette", che per un principio di affidamento inducono la vittima ad abbassare la soglia della cautela[3].

Appare così, con tutta evidenza, eccentrico rispetto a quell'ambito applicativo l'inserimento dell'ipotesi di tutti i casi di atti persecutori, ivi compresi quindi quelli di c.d. *stalking* condominiale e di *mobbing* lavorativo, atteso il richiamo *tout court* al dato normativo all'art. 612 *bis* c.p.; in tal modo si costringe il Pubblico Ministero (P.M.) a trattare allo stesso modo e con analoga urgenza situazioni che invece dovrebbero consentire scelte e valutazioni investigative differenziate.

3. *Le principali novità sostanziali e processuali della Legge n. 69/2019*

Il ruolo degli operatori di prima linea – ci riferiamo alla Polizia giudiziaria (P.G.) e al P.M. – è stato, con la legge istitutiva del cd. Codice Rosso, completamente ridisegnato in quella materia.

[3] Da ultimo v. Corte di Cassazione, Sezione 6, sentenza n. 11910 del 9/2/2023 in tema di esigenze cautelari allorché si procede per reati consumati all'interno di "relazioni strette" (nella specie, maltrattamenti in famiglia e lesioni personali aggravate). Conformi anche Corte di Cassazione Sezione 6, n. 15658 del 2021, n. 11031 del 2018 e n. 47619 del 2016.

Infatti, quella Legge ha comportato, per il P.M., significative novità di diritto penale sostanziale e soprattutto processuale e, per la P.G., una forte specializzazione, che ha richiesto, e richiede tuttora, una formazione specifica e costante.

Iniziamo dalle novità di diritto sostanziale, quelle che invero si sono rilevate meno innovative e meno incisive rispetto alle novità processuali.

La novella legislativa, sul piano del diritto sostanziale, si è mossa lungo due direttrici: introduzione di nuove figure delittuose e aumento di limiti edittali per alcuni delitti già esistenti.

Con l'art. 4 della Legge n. 69/2019 è stato introdotto il delitto di cui all'art. 387 *bis* c.p., ovvero la violazione dei provvedimenti di allontanamento dalla casa familiare e del divieto di avvicinamento ai luoghi frequentati dalla persona offesa. La norma va a colmare un pericoloso vuoto di tutela penale, atteso che la Cassazione era stata sempre costante nell'escludere, in questi casi e in casi simili, la configurabilità della mera ipotesi contravvenzionale di cui all'art. 650 c.p., generando, quella violazione, solo la possibilità di aggravare la misura cautelare in esecuzione[4].

Resta ancora il vuoto normativo della violazione di un obbligo di dimora o di un divieto di dimora, applicato in materia di Codice Rosso: esso sfugge alla sussumibilità del fatto nell'art. 387 *bis* c.p., per il noto principio della tipicità del fatto-reato; residuano qui solo spazi per una richiesta di aggravamento della misura violata.

Un breve cenno anche ad un'altra occasione persa ovvero quella per risolvere l'annoso problema dalla procedibilità[5] per il delitto di atti persecutori.

Il legislatore ha ancora una volta confermato – salvo i casi di *stalking* in danno di minorenne e di persona in condizione di disabilità, ovvero della connessione con un reato per cui si procede di ufficio – la scelta di lasciare la procedibilità nella disponibilità della p.o., facoltà che oggi sembra difficilmente compatibile con l'impostazione del Codice Rosso, che esige immediatamente un intervento penale urgente e

[4] Per tutte vedi, da ultimo, Corte di Cassazione, Sezione 1, sentenza n. 2968 del 08/01/2020.

[5] Vedi il regime disciplinato dall'art. 612 *bis,* ultimo comma, c.p.

significativo da parte dello Stato a tutela di una vittima particolarmente fragile e vulnerabile, condizione che imporrebbe, per coerenza, quell'intervento anche a prescindere da una sua espressa richiesta.

Il termine di sei mesi per presentare la querela è un termine troppo lungo che poco si concilia con i tempi urgente della prevenzione. Inoltre, la possibilità di remissione dovrebbe essere limitata per evitare che la p.o. sia sottoposta allo stillicidio della pressione del suo abusante finalizzata al "ritiro della querela": da un lato, dunque, è auspicabile una interpretazione estensiva dell'ipotesi di minacce reiterate con le modalità di cui all'art. 612, co 2°, c.p., che rende la querela irrevocabile; dall'altro, una interpretazione restrittiva del concetto di remissione processuale ovvero dell'unica tipologia di remissione possibile in materia, proprio a garanzia e tutela della persona offesa, particolarmente esposta e vulnerabile.

L'art. 7 della Legge n. 69/2019 ha introdotto il delitto di cui all'articolo 558 *bis* c.p. ovvero la costrizione o induzione al matrimonio, ipotesi di scarso impatto pratico.

L'art. 10 ha previsto la nuova fattispecie di cui all'art. 612 *ter* c.p. (*revenge pornography* o vendetta sessuale), che invece ha avuto un maggiore impatto nella realtà giudiziaria, se non in termini quantitativi, quantomeno in termini di pericolosità sociale, specialmente negli ambienti giovanili.

L'art. 12 ha tipizzato la deformazione dell'aspetto della persona mediante lesioni permanenti al viso ovvero il cd. sfregio permanente (ora art. 583 *quinquies* c.p.). Apprezzabile, in questo caso, la scelta del legislatore di portare nell'alveo della struttura incriminatoria e non più della mera circostanza aggravante, sia pure ad effetto speciale (art. 583, n. 4 c.p.), gli episodi gravissimi di lesioni che conducono alla perdita della identità personale – si pensi al noto fenomeno dello sfregio al volto con acido – per sottrarla alla possibilità di una sua sostanziale elisione in un eventuale giudizio di bilanciamento delle circostanze ex art. 69 c.p.p., come a volte è purtroppo successo.

Quanto all'elevazione di pene per figure delittuose già esistenti, gli artt. 9 e 13 della Legge n. 69/2019 hanno previsto aumenti dei limiti edittali dei delitti di maltrattamenti, di atti persecutori, di violenza sessuale aggravata, di atti sessuali con minorenni e di violenza sessuale di gruppo; infine, si è prevista un'aggravante ad effetto

speciale (fino alla metà) se il maltrattamento è effettuato in presenza o in danno di minore o di donna in stato di gravidanza o di persona disabile.

Sicuramente più rilevante l'impatto delle novità processuali, che hanno dato la stura ad un percorso legislativo profondamente innovativo in materia.

L'art. 1 della Legge n. 69/2019 ha integrato l'art. 347, comma 3° c.p.p., prevedendo che la P.G., acquisita la notizia di reato relativa ai reati sopra meglio indicati, la comunichi immediatamente, anche in forma orale, al P.M.

L'art. 2 ha introdotto all'art. 362 c.p.p. il co.1-*ter*, in virtù del quale, sempre in relazione ai medesimi delitti, il P.M. deve assumere informazioni dalla persona offesa e da chi ha presentato denuncia, querela o istanza entro il termine di tre giorni dalla iscrizione nel registro di reato, salvo che sussistano imprescindibili esigenze di tutela di minorenni ovvero di riservatezza delle indagini, anche nell'interesse della persona offesa.

L'art. 3 ha integrato l'art. 370 c.p.p., prevedendo, ai nuovi commi 2-*bis* e 2-*ter*, che, in relazione ai nostri delitti, la P.G. senza ritardo proceda al compimento degli atti delegati dal P.M. e ponga a disposizione di quest'ultimo – in altri termini depositi – la documentazione dell'attività posta in essere.

L'art. 362, comma 1-*ter*, c.p.p. è sicuramente la norma manifesto della Legge n. 69/2019: con lo stabilire l'obbligo di assumere informazioni dalla persona offesa entro tre giorni dall'iscrizione, da un lato, si assegna fin dall'origine una corsia preferenziale a quelle indagini e, dall'altro, si opta per una immediata loro direzione ad opera del P.M., unico soggetto in grado di dare, con disposizioni di urgenza, i primi indirizzi investigativi, anche al fine di evitare il rischio di vittimizzazione secondaria.

Ma quale è la conseguenza della violazione di una scansione temporale così stringente?

Sul piano processuale nessuna, in quanto i termini indicati al P.M. (tre giorni dalla iscrizione del fascicolo) e alla P.G. (immediatamente e senza ritardo) sono sprovvisti di sanzione procedurale e, quindi, sono qualificabili solo come ordinatori; al più, potrebbero, in caso di reiterate e ingiustificate violazioni, generare ipotesi di responsabilità disci-

plinare, sia per il Sostituto, che per il Procuratore che non vigila, sia per l'Ufficiale di P.G., che per il Dirigente che non vigila.

Sul piano delle conseguenze, però, la norma è stata rinforzata dall'art. 1 della Legge 8 settembre 2023, n. 122, concernente i poteri del Procuratore della Repubblica nei casi di violazione dell'art. 362, comma 1 *ter* c.p.p., con la possibilità ora per il Procuratore, in caso di violazioni del termine o di omissioni del Sostituto, non giustificate né giustificabili, di revocare l'assegnazione del procedimento penale per riassegnarlo ad altro Sostituto, con tutte le conseguenze in termini di eventuale responsabilità disciplinare e di valutazione di professionalità per il Sostituto revocato.

Il nuovo complesso normativo ha così determinato la necessità – a livello di direttive emanate dai vari uffici di Procura – di procedimentalizzare in maniera snella ed efficace quella scansione procedurale, che altrimenti sarebbe potuta restare lettera morta, con il rischio di condurre ad un pericoloso ingolfamento dell'attività di P.G. e, cosa più grave, avrebbe potuto generare un perverso meccanismo di vittimizzazione secondaria della persona offesa, la cui ravvicinata e reiterata escussione avrebbe potuto rilevarsi pregiudizievole, con inutili sofferenze per la vittima.

Allo stesso tempo si è imposta anche la necessità di adeguare le modalità di trattazione dei fascicoli di Codice Rosso al fine di prevedere un sistema di monitoraggio efficace del rispetto degli adempimenti previsti dall'art. 362, comma 1-*ter* c.p.p., in modo tale da consentire al Procuratore della Repubblica un tempestivo ed effettivo controllo delle modalità esecutive delle prime indagini.

Una prima riflessione qui si impone.

Quella che abbiamo definito la norma manifesto dell'intero provvedimento – ovvero l'obbligo di assumere informazioni dalla persona offesa entro tre giorni dall'iscrizione nel registro delle notizie di reato – è con tutta evidenza anche la reazione del legislatore italiano alla sentenza monito *Talpis*, da cui siamo partiti in questo ragionamento sulle scelte fatte dal legislatore italiano nel tempo.

La dichiarata *ratio* della Legge n. 69/2019 è, infatti, quella di non far neppure percepire alla persona offesa un senso di solitudine e di abbandono da parte delle istituzioni, obiettivo che può ritenersi in buon parte raggiunto ormai a più di cinque anni dall'entrata in vigore di quella norma.

4. *L'ulteriore passo in avanti effettuato con la Riforma Cartabia e la rinnovata figura del P.M. civile*

Le novità analizzate al paragrafo precedente, sia sul piano sostanziale, che su quello procedurale introdotte dalla Legge n. 69/2019, hanno segnato un significativo passo in avanti nell'ottica del raggiungimento dell'obiettivo che la Corte di Strasburgo aveva individuato.

La stessa Corte EDU riconosce i progressi compiuti dall'Italia nella lotta alla violenza domestica negli anni; tuttavia, ha continuato a imputare all'Italia condotte non del tutto osservanti degli obblighi convenzionali. Ciò trova conferma anche nel fatto che lo stato di esecuzione della sentenza *Talpis*, pronunciata ormai anni fa, non è stato ancora dichiarato concluso. In particolare, nel corso di questo costante monitoraggio, il Comitato dei Ministri del Consiglio d'Europa aveva rilevato l'opportunità di proseguire la supervisione dell'esecuzione di quella sentenza*,* in ragione della necessità di garantire che l'Italia dia effettiva attuazione a tutto il quadro giuridico predisposto a tutela delle vittime di violenza domestica.

Del resto, le principali criticità che destavano ancora preoccupazione nel Comitato dei Ministri erano le stesse ravvisate dal Comitato GREVIO nel primo rapporto sullo stato di applicazione della Convenzione di Istanbul in Italia [6].

Nello specifico, tali criticità sono state concentrate sulla mancata considerazione degli episodi di violenza domestica nelle decisioni civili concernenti l'affidamento dei figli minorenni e i diritti di visita; in particolare, è stato evidenziato, in più parti del rapporto, il mancato coordinamento tra giustizia civile e penale in Italia.

Proprio per porre rimedio a queste criticità il legislatore italiano ha colto l'occasione, più generale, della Riforma Cartabia (D. Lgs. 10 ottobre 2022, n. 150) per ridisegnare – con la nuova formulazione degli artt. 473 *bis*, 40 e ss, c.p.c. – il nevralgico rapporto tra P.M. e giudice civile nelle cause in materia di persone minorenni e famiglia, specialmente nei casi critici in cui siano emersi abusi familiari o condotte di violenza domestica (non solo vere e proprie ipotesi di reato, ma an-

[6] Gruppo di esperti indipendenti *"Group of experts on action against violence against women and domestic violence"* nel rapporto Italia del 2020.

che meri fatti allegati), fornendo al P.M. in sede civile una centralità e una specializzazione che non aveva mai avute prima.

Infatti, quando una delle parti allega in una causa civile condotte di violenza o di abusi nei confronti di familiari o di minori, il giudice civile deve ora attivare una procedura rinforzata, per la quale si abbreviano i termini processuali, e deve compiere tutte le attività necessarie, anche d'ufficio, per accertare nel rispetto del contraddittorio le condotte allegate dalle parti, chiedendo al P.M., ove nulla osti, la trasmissione di atti non coperti da segreto o comunque ad avviso di quest'ultimo discoverabili.

Il nuovo quadro normativo, di fatto, ha inciso su un duplice fronte: da un lato, ha consentito l'istaurazione di un canale privilegiato negli affari civili del P.M. che consente di filtrare le richieste urgente del giudice civile che possano incidere sugli esiti delle controversie negli ambienti familiari abusati o anche solo critici; dall'altro, il maggiore ruolo assegnato al P.M. nella materia civile impone, anche nella scelta e nella gestione dei modelli organizzativi, un P.M. altamente competente e specializzato.

Per questo i provvedimenti organizzativi adottati dalle Procure in Italia hanno optato per una precisa scelta di campo: ovvero che il P.M. civile, cioè il Sostituto assegnatario dei pareri e delle informazioni richieste dal giudice civile, deve tendenzialmente coincidere con quello penale, ovvero con il medesimo Sostituto che sta coordinando o ha coordinato le indagini.

A questa specializzazione del P.M. fa il paio anche la specializzazione delle forze di P.G., già prevista dalla Legge n. 69/2019 che si preoccupava espressamente anche della formazione degli operatori (art. 5); in questa materia, infatti, la sfida investigativa più impegnativa è quella di garantire un approccio adeguato anche da parte della P.G. sia in sede centrale, che periferica: costituendo essa il primo baluardo di tutela, i suoi rappresentanti devono necessariamente essere capaci di orientarsi non solo nelle decisive scelte investigative, ma anche e soprattutto nel primo approccio alla vittima di violenza.

La Riforma Cartabia, infine, ha ridisciplinato le modalità di documentazione delle dichiarazioni della vittima vulnerabile ed ampliato gli oneri di comunicazione verso la persona offesa dei provvedimenti a sua tutela (come anche dei successivi provvedimenti di revoca), stru-

menti entrambi utili, le prime, per prevenire successive ritrattazioni e ridimensionamenti dei fatti, i secondi, per una corretta individuazione dei fattori di rischio, sulla cui inadeguatezza delle procedure di valutazione pure si erano appuntate alcune critiche emerse nel corso del monitoraggio operato dal Comitato dei Ministri del Consiglio d'Europa e dal GREVIO.

5. *Il Codice Rosso rinforzato e la nuova centralità e specialità della fase cautelare*

La Legge 24 novembre 2023, n. 168 "Disposizioni per il contrasto della violenza sulle donne e della violenza domestica" (cd. Codice Rosso rinforzato) ha ulteriormente caratterizzato la strada scelta del legislatore italiano in materia, soprattutto nel procedimento cautelare, che oggi segna decisamente il passaggio da una generale prevenzione dei reati ad una protezione specifica della vittima.

La vasta gamma, oggi esistente, di misure a tutela della vittima di violenza di genere, oltre ad avere una indiscutibile potenzialità dissuasoria, garantisce un ventaglio particolarmente ampio delle scelte, che vanno dalla possibilità, oggi ampliata, di arresto in flagranza di reato, alle misure cautelari di carattere generale (custodia in carcere e arresti domiciliari), a quelle di carattere specifico (obbligo e divieto di dimora, divieto di avvicinamento alla persona offesa e allontanamento dall'abitazione familiare) alle misure di prevenzione, fino alla possibilità di applicare l'ammonimento del Questore e l'ordine di protezione in sede civile.

Per l'allontanamento dalla casa familiare e il divieto di avvicinamento ai luoghi frequentati dalla persona offesa., ora si prevede non solo la prescrizione al cautelato del divieto di avvicinarsi ad una distanza inferiore ai 500 metri, ma anche che l'eventuale diniego all'applicazione delle modalità di controllo previste dall'art. 275 *bis* c.p.p. (c.d. braccialetto elettronico) possa comportare anche l'applicazione congiunta di misure più gravi, quali l'obbligo e il divieto di dimora. Tanto che ormai è invalsa la prassi di presentare un doppio *petitum*, come sopra indicato, al giudice per le indagini preliminari (GIP) in occasione già della prima richiesta cautelare.

Particolarmente incentivato è il ricorso al c.d. braccialetto elettronico**,** che prevede la dotazione in favore della parte offesa, previo consenso, di un apparecchio che nel caso di violazione faccia partire l'immediato allarme sul suo dispositivo e contemporaneamente presso la centrale operativa della P.G. preposta al controllo. Tale sistema, oltre a dare sicurezza alla persona offesa, riduce le violazioni per la certezza della loro scoperta e consente di verificare anche i tentativi di incontro da parte del denunciato, risultando monitorato continuamente lo spostamento dell'indagato.

Si è finalmente posto rimedio ad una pericolosa falla del sistema complessivo di tutela delle vittime. La fattispecie di cui all'art. 387-*bis* c.p. (violazione dei provvedimenti di allentamento dalla casa familiare ex art. 282 *bis* c.p.p. e del divieto di avvicinamento dai luoghi frequentati dalla persona offesa ex art. 282 *ter* c.p.p.), pur imponendo l'arresto obbligatorio in flagranza, non consentiva l'emissione di misura cautelare prima della Legge n. 168/2023; il che determinava una fase temporale di scopertura di tutela della persona offesa che poteva, prima della modifica del 2023, essere assicurata solo dall'accoglimento di una eventuale richiesta di aggravamento della misura violata e già emessa nell'ambito del procedimento originario.

Sul punto, il legislatore del 2023 è intervenuto prevedendo innanzitutto l'estensione dell'oggettività della fattispecie di violazione dei provvedimenti di allontanamento dalla casa familiare e del divieto di avvicinamento ai luoghi frequentati dalla persona offesa, adesso integrata, con il nuovo co. 2° dell'art. 387 *bis* c.p., anche dalla violazione dell'ordine di protezione previsto dall'art. 342 *ter* del codice civile.

Ma il legislatore del Codice Rosso rinforzato è intervenuto anche sulla pena della fattispecie, aumentando nel massimo la cornice edittale, che passa da 3 anni a 3 anni e 6 mesi, così da consentire l'adozione di misure cautelari, prima non consentite, nonostante si vertesse in ipotesi di arresto obbligatorio in flagranza di reato cui, pertanto, seguiva sempre l'immediata liberazione dall'arrestato.

Inoltre, con l'art. 13 della Legge n. 168/2023 sono stati modificati gli artt. 275, 280 e 391 c.p.p. ed ora le disposizioni relative ai limiti edittali per l'applicazione della custodia cautelare in carcere (art. 275 c.p.p.: condanna superiore a tre anni), quelle relative ai limiti edittali generali per l'applicazione delle misure coercitive personali (art. 280

c.p.p: pena superiore a tre anni) e quelle per la valutazione delle esigenze cautelari in caso di pericolo di recidivanza per l'applicazione di misura all'esito della convalida di arresto (combinato disposto degli artt. 391, co. 5°, c.p.p e art. 274, lett. c), c.p.p.) non si applicano all'ipotesi di cui all'art. 387-*bis* c.p., come opportunamente anche alle lesioni aggravate dai rapporti intrafamiliari e dalla connessione con maltrattamenti, abusi sessuali e atti persecutori.

Ancora, nella medesima ottica, è stato introdotto il co. 3.*bis* all'art. 280 c.p.p., che, escludendo l'applicazione dei co. 1, 2 e 3 in relazione al medesimo elenco di reati, consente oggi di applicare anche la custodia carceraria per fattispecie di violenza di genere, *rectius* sulle donne, che in passato erano prive di copertura cautelare, anche non custodiale.

Tutte queste norme, unitariamente lette, hanno come chiaro intento quello di inasprire il trattamento cautelare e di creare una sorta di regime derogatorio, che sembra costituire la regola, anziché l'eccezione ai noti principi di residualità e di sussidiarietà delle misure cautelari[7].

Con la Legge n. 168/2023 si rinforza anche la fase precautelare, con la possibilità ora sia dell'arresto in flagranza differita, strumento che consente alla P.G. di procedere all'arresto dell'indagato per i reati di cui agli artt. 387-*bis,* 572 e 612-*bis* c.p. entro le 48 ore successive dalla commissione del fatto, qualora emerga l'inequivoca attribuibilità del fatto alla persona offesa sulla base di documentazione video fotografica o altra documentazione legittimamente acquisita da dispositivi informatici e telematici.

Accadeva, infatti, con una certa frequenza che la P.G., intervenuta per fatti avvenuti poco tempo prima, non potesse adottare provvedimenti d'urgenza non essendovi lo stato di flagranza e non sussistendo in casi del genere i presupposti per il fermo di iniziativa, difettando sia i limiti edittali, sia di norma il pericolo di fuga.

Si è fatto, dunque, ricorso ad un istituto, quello della flagranza differita, già conosciuto dall'ordinamento[8] ed oggetto di ampio dibatti-

[7] L. KALB (a cura di), *Le novità del procedimento cautelare*, Milano 2024, pp. 8-15, in cui si parla di "modello differenziato".

[8] Vedasi la normativa di contrasto alla violenza commessa in occasione o a causa

to, per le criticità che pone sul rispetto delle garanzie connesse alla riserva di giurisdizione di cui all'art. 13 della Costituzione.

Sempre nell'ottica del potenziamento della fase precautelare si inserisce, con l'introduzione del co. 2 *bis* dell'art. 384-*bis* c.p.p., anche l'ampliamento dell'ambito applicativo dell'allontanamento d'urgenza dalla casa familiare, ora esteso anche al decreto urgente del P.M.

Ma la novità più rilevante è stata l'introduzione di una norma che, per la prima volta nell'ordinamento italiano, prevede una cronoscansione dell'*iter* di adozione di una misura cautelare: con l'introduzione dell'art. 362-*bis* c.p.p., infatti, è previsto che il P.M., entro trenta giorni dall'iscrizione della notizia di reato a carico dell'indagato, valuti la sussistenza dei presupposti per l'applicazione di misure cautelari e che, nei venti giorni successivi al deposito della richiesta, il GIP provveda sulla suddetta richiesta.

Con il nuovo art. 362-*bis* c.p.p. (Misure urgenti di protezione della persona offesa", deve innanzitutto osservarsi che l'ambito applicativo dell'art. 362-*bis* c.p.p. non coincide perfettamente con quello di cui all'art. 362, co. 1 *ter* c.p.p., essendo, da un lato, più esteso quanto alla tipologia dei reati inclusi nell'elenco, comprendendo anche delitti comuni, quali la violenza privata e la violenza grave, ma, dall'altro lato, restringendone l'ambito, quanto al contesto in cui i predetti reati si vengano a manifestare per far scattare quella corsia preferenziale cautelare, e cioè deve trattarsi di delitti consumati o tentati in danno del coniuge, anche separato o divorziato, della parte dell'unione civile o del convivente o di persona che è legata o è stata legata da relazione affettiva ovvero di prossimi congiunti (sfera intrafamiliare, formale e di fatto, e comunque di affettività).

Dunque, possono ritenersi esclusi dal meccanismo valutativo dell'art. 362 *bis* c.p.p. i casi – in realtà da sempre critici e non occasionali, rispetto all'applicazione del regime giuridico del Codice Rosso – di atti persecutori tra vicini di casa (*stalking* condominiale) e di maltrattamenti dei dipendenti (*mobbing* aziendale o lavorativo).

Deve poi osservarsi che, in assenza di un dato testuale chiaro nel nuovo art. 362 *bis* c.p.p., in seno agli uffici di Procura è stata posta la seguente questione: qualora il P.M. entro trenta giorni dall'iscrizione

di manifestazioni sportive.

del nominativo dell'indagato non abbia depositato una richiesta di misura cautelare, deve esplicitare espressamente in un provvedimento, anche sommario, da depositare agli atti del fascicolo delle indagini preliminari, la valutazione effettuata, evidentemente di carattere negativo, della mancanza dei presupposti indiziari e/o cautelari, almeno in quella fase, ovvero quella valutazione può ritenersi implicita nel mancato deposito di una richiesta di misura, fungendo così, la norma in questione, solo come mera indicazione di priorità cautelare.

Sul punto, una recente nota della Procura Generale presso la Corte di Cassazione[9] ha fatto chiarezza evidenziando espressamente che la scelta del P.M. di non richiedere una misura cautelare va formalizzata per iscritto allo scopo di evitare addebiti di inerzia e/o comportamenti omissivi.

Gli autorevoli orientamenti della Procura Generale capitolina ritengono però sufficiente anche solo una annotazione sul fascicolo con contestuale aggiornamento avente data certa dell'avvenuta valutazione, ma al contempo non vietano, pur non ritenendolo previsto dalla norma, altre forme scritte (decreto o altro) con le quali cristallizzare l'avvenuta valutazione di insussistenza, allo stato degli atti, dei presupposti di applicazione delle misure cautelari; anzi, espressamente affidano all'autonomia dei singoli Procuratori della Repubblica l'ampiezza e i limiti contenutistici del provvedimento di annotazione sulla valutazione cautelare effettuata.

La necessità, *rectius* opportunità, di un provvedimento espresso indicativo della valutazione effettuata sui presupposti cautelari è confermata poi dalla modifica dell'art. 127 delle disposizioni di attuazione del c.p.p., che prevede anche l'onere di comunicare al Procuratore Generale presso la Corte d'Appello, con cadenza trimestrale, i dati relativi ai procedimenti iscritti di cui all'art. 362-*bis* c.p.p.

[9] V. la nota della Procura Generale presso la Corte di Cassazione del 28.5.2024, avente ad oggetto *"Orientamenti in materia di applicazione delle leggi n. 122 e 168 del 2023 in materia di violenza di genere"*.

6. *Conclusioni: una specialità fino in fondo?*

Quanto sopra sinteticamente evidenziato porta alla conclusione che la prioritaria necessità di prevenzione dei reati di Codice Rosso e di protezione dalla vittima hanno segnato in materia un percorso legislativo che ha costruito una corsia privilegiata, che ha condotto non solo ad una evidente accelerazione investigativa, ma soprattutto ad un procedimento cautelare agevolato, perché connotato da elementi tali di specialità, che lo hanno differenziato in maniera significativa dal modello ordinario del giudizio cautelare.

Il vero *punctm dolens* dell'intera materia è la mancanza di un ultimo passo coraggioso da parte del legislatore italiano ovvero la mancata previsione di differenti requisiti indiziari generali previsti per l'esercizio dell'azione cautelare, che ne agevolino l'accesso, come pure sarebbe stato se non necessario, quantomeno opportuno.

Infatti, si potrebbero modulare differentemente i presupposti per l'applicazione delle misure cautelari con una sorta di "doppio binario"*:* gravità indiziaria per le misure coercitive personali limitative di libertà personali in maniera significativa quali carcere, arresti domiciliari, obblighi e divieti di dimora; sufficienza indiziaria rispetto a misure coercitive personali impeditive o ostative, quali il divieto di avvicinare la persona offesa, di frequentare i luoghi abitualmente frequentati dalla stessa o l'allontanamento dalla casa coniugale.

Si è, invece, lasciato invariato il regime cautelare per tutte le tipologie di misure, in ogni caso ancorato alla sussistenza dei gravi indizi di colpevolezza.

Questo approccio potrebbe rivelarsi non del tutto adeguato ad un settore, come quello della violenza di genere, che impone inevitabilmente un agire in tempi sempre più ristretti e veloci, obiettivo forse realmente realizzabile con una revisione minima delle garanzie personali, nei termini limitati sopra indicati.

Altra mancata occasione del legislatore italiano sta nella omessa previsione, al di là di mere indicazioni di priorità nella formazione dei ruoli di udienza, di una corsia preferenziale che proseguisse anche per tutta la fase dibattimentale, fino almeno alla sentenza di primo grado, che pure dovrebbe svolgersi dinanzi a un giudice del merito specializzato.

E sicuramente la riforma istitutiva del nuovo Tribunale per la famiglia è stata un'occasione persa.

Vedremo, nei prossimi tempi, se quell'occasione per il legislatore nazionale sarà recuperata in sede di attuazione dell'ultima direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e la violenza domestica, che dovrà essere recepita dagli Stati membri entro il 14 giugno 2027.

In verità, la direttiva mira soprattutto alla formulazione di nuove fattispecie di reato. Sul punto, il legislatore europeo ha spinto sulla necessità – rilevata dalla Corte EDU, con la decisione n. 56867/2020 – di formulare appropriate norme incriminatrice sulla *cyberviolence* [10], avendo il GREVIO già più volte evidenziato la gravità della violenza digitale sulle donne, realizzata attraverso quegli strumenti informatici oggi estremante diffusi (e-mail, messaggeria istantanea, blog, telefoni cellulari, siti web, …) che ne fanno un fenomeno estremamente pericoloso, soprattutto negli ambienti adolescenziali.

Ma, a ben vedere, oltre all'obiettivo principale sopra indicato, l'ultima direttiva UE evidenzia, più in generale, anche la necessità di potenziare l'accesso alla giustizia delle vittime di reato di genere, la necessità di assicurare loro protezione adeguata e di offrire in tutti i campi un'adeguata assistenza.

Questi ultimi aspetti offrono la possibilità al legislatore italiano *de iure condendo* di inserire una normativa specifica anche sulla tutela della vittima durante la fase dibattimentale, attraverso strumento di priorità che sanciscano una rigorosa scansione temporale pure per la fase di cognizione, al fine di evitare il paradosso di una corsia emergenziale, segnata dal Codice Rosso fin dalla prima fase delle indagini, equiparabili, per restare nel campo medico, al primo acceso al pronto soccorso, senza però consentire poi una definitiva diagnosi e una risolutiva terapia nel reparto di specializzazione, vale a dire il nostro giudice del dibattimento.

[10] L'ultimo intervento legislativo in materia in Italia risale ormai al lontano Decreto Legge 14 agosto 2013, n. 93, con cui sono state inasprite le pene per lo *stalking*, introducendo sanzioni più severe per chi commette il reato attraverso strumenti informatici e telematici; l'aggravante prevista prevede solo un aggravamento ordinario (di 1/3) della pena stabilita per il reato di atti persecutori nel caso in cui il fatto sia commesso "attraverso strumenti informatici o telematici".

Abstract

Il contributo mira ad evidenziare come tutto il percorso legislativo italiano, a partire dalla Legge n. 69/2019 istitutiva del Codice Rosso, si sia mosso lungo le direttrici segnate dalla Convenzione di Istanbul del 2011, ratificata in Italia nel 2013. Il percorso legislativo italiano ha fatto del contrasto alla violenza di genere una emergenza giudiziaria, in conseguenza anche della sentenza della CEDU di condanna dell'Italia per il caso *Talpis* del 2017. Quella legge ha previsto significative novità di diritto penale sostanziale e soprattutto processuale. Lungo quella strada si sono inserite la "*Riforma Cartabia*" (D. Lgs. 10 ottobre 2022, n. 150) e la Legge 24 novembre 2023, n. 168 (cd. "Codice Rosso rinforzato") che hanno rafforzato il procedimento cautelare. La prevenzione dei reati di "Codice Rosso" e la protezione dalla vittima hanno condotto ad un procedimento cautelare connotato da elementi tali di specialità, che lo hanno differenziato significativamente dal modello ordinario.

KEYWORDS: percorso legislativo – Codice Rosso – tutela della vittima – procedimento cautelare – regime speciale

LAS OPCIONES DEL LEGISLADOR ITALIANO: ACTIVIDAD DE INVESTIGACIÓN Y PROCEDIMIENTOS CAUTELARES "ESPECIALES"

La contribución tiene como objetivo resaltar cómo el proceso legislativo italiano, a partir de la Ley núm. 69/2019, que establece el Código Rojo, ha seguido la línea marcada por el Convenio de Estambul de 2011, ratificado en Italia en 2013. El camino legislativo italiano ha hecho de la lucha contra la violencia de género una emergencia judicial, también como consecuencia de la sentencia de TEDH que condena a Italia por el caso *Talpis* de 2017. Esta ley introdujo importantes innovaciones en el Derecho penal material y, sobre todo, procesal. En ese camino, se han incorporado la "Reforma Cartabia" (Decreto Legislativo de 10 de octubre de 2022, n. 150) y la Ley de 24 de noviembre de 2023, n. 168 (denominado "Código Rojo Reforzado") que fortaleció el procedimiento cautelar. La prevención de los delitos de "Código Rojo" y la protección de la víctima, han dado lugar a un procedimiento cautelar caracterizado por elementos tan especializados, que lo han diferenciado significativamente del modelo ordinario.

PALABRAS CLAVE: vía legislativa – Código Rojo – protección de la víctima – procedimientos cautelares – régimen especial

ORDINAMENTO SPAGNOLO
ORDENAMIENTO ESPAÑOL

LA CIBERVIOLENCIA DE GÉNERO EN ESPAÑA: LÍMITES Y OPORTUNIDADES DE LA RESPUESTA LEGAL A UN FENÓMENO GLOBAL

Noelia Igareda González[*]

SUMARIO: 1. La ciberviolencia de género como un fenómeno creciente y global. – 2. Las conexiones de la ciberviolencia de género con el movimiento global anti-género. – 3. Los instrumentos legales para abordar la ciberviolencia de género. – 4. Los límites del abordaje legal.

1. *La ciberviolencia de género como un fenómeno creciente y global*

La ciberviolencia de género abarca todas las formas de violencia digital que se dirigen contra las mujeres o contra las personas por razón de su sexo, género u orientación sexual. Hay una variedad de denominaciones para refeirse a un mismo fenómeno, entre las que encontramos la ciberviolencia de género[1]; la violencia de género digital/en línea/en internet[2]; las ciberviolencias machistas[3] o las violencias machistas digitales[4]. Esta diversidad terminológica complica su identificación y su abordaje legal, y aún más cuando la ley española más importantes sobre violencia de género, la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la violencia de

[*] Profesora titular de Filosofía del Derecho, Universidad Autónoma de Barcelona. Email: noelia.igareda@uab.cat.

[1] Instituto Europeo de Igualdad, *Cyber violence against women and girl,. European Institute for Gender Equality,* 2017. https://eige.europa.eu/publications/cyber-violence-against-women-and-girls; A. A. GARCÍA COLLANTES, M.J. GARRIDO ANTÓN, *Violencia y ciberviolencia de género*, Valencia, 2021.

[2] T. DONOSO-VÁZQUEZ Y A. REBOLLO-CATALÁN, *Violencia de género en entornos virtuales*, Octaedro, 2018.

[3] N. IGAREDA, A.PASCALE, M. CRUELLS, P. PAZ, *Les ciberviolències masclistes*. Institut Català de les Dones, Generalitat de Catalunya, 2019.

[4] FEMBLOC*, Marc conceptual per a un abordadge de les Violències Masclistes digitals*, FemBloc, 2022, disponible en: https://fembloc.cat/archivos/recursos/5/legal-conceptual-and-methodological-frameworkdefce.pdf

género, no hace mención alguna a esta violencia digital. Además, aunque en su preámbulo se refiere a todas las violencias que se ejercen contra las mujeres por el hecho de ser mujeres, en coherencia con la definición de la violencia de género del Convenio de Estambul[5], despues en su articulado sólo se ocupa de la violencia que se ejerce en el ámbito de la pareja o ex pareja.

Esta diversidad de denominaciones también está influida por los intereses de quienes están detrás de cada nombre. El sector tecnológico ha estado más interesado en poner de relieve el contexto o el medio en el que tenían lugar estos comportamientos violentos, sin tener en cuenta la dimensión de género, ni el carácter estructural de dichas violencias. El feminismo en cambio no ha prestado suficiente atención al componente tecnológico que exige un tratamiento diferente a las demás violencias de género. Las instituciones dedicadas a la lucha contra los delitos cibernéticos han prestado tradicionalmente más atención a la pornografía infantil y otros abusos a menores a través de internet, y apenas a las otras formas de ciberviolencia de género[6].

Pero todas estas denominaciones aluden a la diversidad de violencias que se ejercen en el contexto digital contra estas personas, ya que la razón que hay detrás de esta violencia es una sociedad patriarcal que defiende la dicotomía sexual tradicional, la complementariedad de los sexos, y los roles y estereotipos de género como características naturales y permanentes de hombres y mujeres.

Existe además una gran diversidad de ciberviolencias de género, que pueden agruparse en tres categorías principales[7]. En primer lugar, están las violencias digitales generales hacen referencia a aquellas conductas que buscan aislar, silenciar, controlar, humillar, disciplinar en función de los roles de género socialmente impuestos y dañar a las mujeres, como por ejemplo los insultos y las injurias por razón de sexo, género y/o orientación sexual; los discursos de odio anti-género, el ciberacoso las amenazas, o el seguimiento o control de movimientos.

En segundo lugar, podemos identificar las violencias machistas

[5] Convenio del Consejo de Europa *sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica*, 2011 (que entró en vigor en 2014).

[6] FEMBLOC, *op.cit*.

[7] *Ibidem.*

digitales de alto componente tecnológico que son aquellas que buscan ampliar y profundizar en los efectos de las anteriores, incrementando las posibilidades virales y grupales, convirtiéndose en masivas y requiriendo generalmente de importantes conocimientos técnicos para su ejecución. Entre estas conductas podemos destacar la suplantación y robo de identidad, el *doxing* (utilizar información privada de una mujer y difundirla públicamente), el silenciar, tumbar servidores, páginas web o perfiles de mujeres, jaquear cuentas y controlar de forma remota. En este grupo también se pueden incluir la utilización del Internet de las cosas que se refiere a la red de dispositivos inteligentes conectados a Internet que pueden compartir datos entre sí, que incluye televisión, reloj, frigorífico, sistema de calefacción, cámara o cerradura inteligente.

En tercer lugar, encontramos las violencias machistas digitales de carácter sexual que forman parte de aquellas que afectan desproporcionalmente a las mujeres y a las niñas y buscan agredir sexualmente a las mujeres. Aquí se incluyen las amenazas de violación, el acoso sexual, el *grooming* (la captación de menores para abusarlos sexualmente o convertirlos en víctimas de explotación sexual), los comentarios de contenido sexual, el envío de contenido digital de carácter sexual a una mujer sin que esta lo haya pedido, la grabación y distribución de una violación, la sextorsión (uso de fotografías o vídeos íntimos para extorsionar económicamente o a cambio de otros favores); la violencia sexual digitalizada (grabar y divulgar agresiones y abusos sexuales) o la distribución, creación, difusión, distribución e intercambio de imágenes o vídeos íntimos sin consentimiento. Esta última forma de ciberviolencia de género se ha denominado comúnmente como "pornovenganza", un término no exento de polémica, porque esconde la dimensión de violencia de género que tiene esas conductas y parece centrarse más en la intención del agresor, y no en el impacto en la víctima.

También en esta tercera categoría pueden incluirse los ataques de carácter sexual utilizando la Inteligencia Artificial (como por ejemplo los deepfakes) o los ataques sexuales a los avatares femeninos en el metaverso[8].

Estas diferentes formas de ciberviolencia de género a veces reci-

[8] N. IGAREDA, A.PASCALE, M. CRUELLS, O. PAZ, *op. cit.*

ben denominaciones generalmente en inglés, ya que que contribuyen a una cierta confusión, porque, por un lado, se llega a la conclusión de que la ciberviolencia de género es únicamente esa forma de agresión, y por otro lado, también se pierde la dimensión de género. Ocurre por ejemplo cuando se habla de *hacking* (acceder ilegalmente a sistemas informáticos externos con el propósito de adquirir o modificar información personal, así como difundir material que pueda denigrar o humillar a la víctima/s potencial/es)*;* el ciberacoso (también ciberacecho o *cyberstalking* o *ciberbullying*) o *spamming* (contactar, molestar, amenazar, intimidar o aterrorizar de manera repetitiva y continuada a través de llamadas de teléfono, mensajes de texto, comentarios, etcétera); el *flaming* hace referencia a la acción de mandar mensajes provocadores e insultantes; el *outing* describe la acción de compartir información y material multimedia embarazoso sobre otras personas sin haber obtenido previamente su consentimiento. O el cyberflashing: imágenes sexuales recibidas sin haberlas solicitado previamente, generalmente de los genitales masculinos ("fotopollas")[9].

Aunque el presente capítulo aborda la ciberviolencia de género desde el prisma español, se trata de un fenómeno global, en el que un número creciente sobre todo de mujeres y niñas, son víctimas de diferentes formas de violencia en el contexto virtual, por parte generalmente de hombres, de manera individual o grupal, y muchas veces dificilmente identificables.

La variedad de términos con el que se denomina este fenómeno también dificulta encontrar con unas estadísticas claras sobre su prevalencia. Además, muchas veces las estadísticas disponibles sólo han estudiado alguna forma de ciberviolencia de género, y no siempre reconociendo que su dimensión de género, o no incluyendo datos desagregados por sexo[10].

Sin embargo, las evidencias muestran que más del 80 por ciento de las personas que han sufrido algún tipo de violencia digital sexual

[9] I.Crosas, P. Medina-Bravo, *Ciberviolencia en la red. Nuevas formas de retórica disciplinaria en contra del feminismo*, en *Paper,s,* 2019, n. 104/1, pp. 47-73.

[10] A. Van Der Wilk, *Cyber violence and hate speech online against women*. En *Women's Rights & Gender Equality Department. European Institute for Gender Equality,* 2018. Disponible en: https://policycommons.net/artifacts/2002468/cyber-violence-and-hate-speech-online-against-women/2754233/

son mujeres y/o niñas[11]. También datos recogidos por el Instituto Europeo de Igualdad de Género señalan que 1 de cada 10 niñas y/o mujeres mayores de 15 años ha sufrido alguna forma de ciberviolencia por razón de género[12].

También en este sentido, Amnistía Internacional (2018) identificó que el 21% de las mujeres en diversos países habían sido víctimas de alguna forma de abuso online, y este porcentaje subía hasta el 37% en mujeres entre 18 y 24 años[13].

En general, los estudios disponibles sobre la prevalencia de las diferentes formas de ciberviolencia de género destacan la mayor incidencia entre las mujeres jóvenes, las mujeres racializadas, también entre las personas con diversidad funcional y las personas[14]. También es coincidente en las diferentes investigaciones llevadas a cabo sobre ciberviolencia de género que las mujeres empoderadas con una proyección pública son especialmente vulnerables a esta ciberviolencia de género, políticas, académicas, artistas o *gamers*[15].

La violencia de género en el mundo analógico se traslada de esta manera al mundo virtual, pero con características como el anonimato, la viralidad o la permanencia, que lo convierten en un fenómeno en ocasiones más victimizador. Internet y las redes sociales permiten ataques de manera anónima, donde es muy dificil o imposible identificar al agresor/es. Igualmente las redes sociales están diseñadas para promocionar los contenidos más violentos, y por lo tanto, estas diferentes formas de violencia son generalmente repetidas, potenciadas y transmitidas de manera exponencial. Además, los contenidos violentos

[11] ONU MUJERES , *Informe Ciberviolencia y Ciberacoso contra las muejres y las niñas en el marco de la Convención Belém Do Pará*. ONU Mujeres. América Latina y el Caribe, 2020. Disponible en https://lac.unwomen.org/es/digital-library/publications/2022/04/ciberviolencia-y-ciberacoso-contra-las-mujeres-y-ninas-en-el-marco-de-la-convencion-belem-do-para

[12] Instituto Europeo de Igualdad, *op.cit.*

[13] Amnistía Internacional, *Violencia contra las mujeres en Internet en 2018,* 2018.

[14] FEMBLOC, *op.cit.*

[15] Consejo de Derechos Humanos, Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos, A/HRC/38/47, 18 de junio de 2018.

permanecen en el espacio virtual, no desaparecen, y por lo tanto, el daño a las víctimas se perpetúa en el tiempo y en el espacio.

Todas estas formas de ciberviolencia de género tienen diversas consecuencias en las vidas de las víctimas. Consecuencias individuales, como secuelas psíquicas y físicas, destacando el miedo, la ansiedad o la depresión. Además de estas secuelas, hay que añadir los comportamientos antisociales, las consecuencias físicas, educativas y económicas entre otras[16].

Además de los daños psicológicos asociados a este fenómeno, las víctimas de formas de ciberviolencia de género de contenido sexual sufren diversos daños irreparables que afectan a su vida personal y, sobre todo, profesional.

A través de la ciberviolencia de género se crea para las mujeres un ambiente demasiado tóxico y hostil para soportarlo y que al mismo tiempo persigue unos determinados efectos en el contexto analógico. La consecuencia principal y más grave es muchas veces un estado de hipervigilancia, en el que las víctimas de ciberviolencia de género sienten que los perpetradores están en todas partes, tanto en el mundo virtual como en el mundo analógico[17].

Pero también las diferentes formas de ciberviolencia de género tiene consecuencias colectivas. Muchas víctimas son expulsadas del contexto virtual, ya que apagarse digitalmente se presenta como la única alternativa para poner fin a estas violencias, con el previo personal, social, profesional y político que esto representa. Asimismo estas ciberviolencias no sólo afectan a las víctimas individualmente, sino que constituyen un instrumento de disciplina a todas las mujeres que se atreven a transgredir las normas de género dominantes. La ciberviolencia de género, sobre todo aquella que sexualiza a las víctimas o las

[16] CALALA FONDO DE MUJERES, *Las violencias machistas en línea gacia activistas. Datos para entener el fenómeno*, 2020, Disponible en: https://bit.ly/3eQC1j; L. SERRA PERELLÓ, *Las violencias de género en línea. Pikara Magazine*, 2018. Disponible en: https://bit.ly/2QGo3bP.

[17] N. IGAREDA GONZÁLEZ, *El discurso de odio anti-género en las redes sociales como violencia contra las mujeres y como discurso de odio, en Revista Derechos y Libertades*, 2022, n. 47, pp. 97-122.

agrede sexualmente, contribuye a la socialización en el terror sexual, la amenaza última y más grave de todas las mujeres[18].

2. *Las conexiones de la ciberviolencia de género con el movimiento global anti-género*

Las diferentes formas de ciberviolencia de género están conectadas a un movimiento político global anti-género, que busca cuestionar las teorías de género que han denunciado el patriarcado, y los roles y estereotipos de género como cuestiones normales y naturales. Este movimiento político anti-género está presente en las sociedades occidentales, con características particulares en cada país, pero con rasgos comunes como son sus alianzas con partidos políticos de extrema derecha, con grupos religiosos conservadores y con entidades neoliberales o libertarias[19].

En España, los actores principales de este movimiento anti-género han sido partidos políticos como Vox, que rechaza las leyes relacionadas con la violencia de género, los derechos LGTBIQ+, la educación en diversidad y los avances feministas.

También hay algunas instituciones católicas y asociaciones vinculadas a la Iglesia que promueven un modelo de familia tradicional y se oponen al matrimonio igualitario, las leyes trans o la educación en diversidad sexual.

Igualmente existen asociaciones como Hazte Oír que han tenido un papel destacado en la difusión de la ideología anti-género, organizando campañas mediáticas como el polémico autobús que negaba la identidad de género trans con mensajes como: "Los niños tienen pene, las niñas tienen vulva".

Todos estos actores del movimiento anti-género tienen algunos elementos en común: niegan por ejemplo la existencia de la violencia de género como un fenómeno estructural, reemplazando el término

[18] N. BARJOLA, *Microfísica sexista del poder. El caso Alcàsser y la construcción del terror sexual*, Barcelona, 2018.

[19] D. PATERNOTTE, R. KUHAR, *Disentangling and Locating the 'Global Right': Anti-Gender Campaigns in Europe*, *Politics and Governance*, 2018, vol. 6, n. 3, pp. 6–19.

por "violencia intrafamiliar" para diluir el enfoque en las desigualdades de género. En consecuencia, cuestionan la Ley Orgánica de Medidas de Protección Integral contra la Violencia de Género, alegando que discrimina a los hombres.

Igualmente rechazan la inclusión de temas relacionados con la identidad de género y la orientación sexual en los currículos escolares, argumentando que supone un "adoctrinamiento" de los menores. En este sentido, se oponen a la educación afectivo-sexual que fomente la diversidad y el respeto por las personas LGTBIQ+.

También se muestras críticos con los derechos LGTBIQ+, criticando leyes como la Ley Trans o las iniciativas que buscan proteger a las personas no heteronormativas, calificándolas como una amenaza para los valores tradicionales. Alegan que estas leyes privilegian a ciertos colectivos y limitan la "libertad de expresión" de quienes disienten. Promueven una visión esencialista del género basada en la biología, rechazando los conceptos de género como constructo social y oponiéndose al feminismo interseccional[20].

Las diferentes formas de violencias digitales se convierten la mayoría de las veces en herramientas de control y disciplina para las mujeres o las personas que transgreden la herenormatividad y binarismo sexual en el contexto digital cuando representan una amenaza para una sociedad patriarcal organizada alrededor de la división sexual del trabajo, la complementareidad de los sexos, la dicotomía sexual y los privilegios de los varones. La ciberviolencia de género puede llegar a constituir un instrumento para facilitar la expulsión o la invisibilización de todas aquellas personas que desobedecen los mandatos de género[21].

Todos estos integrantes del movimiento anti-género se han caracterizado por ser especialmente activos en las redes sociales e Internet,

[20] A. FEJOS, V. ZENTAI (eds.), *Anti-gender hate speech in populist Right-wing Social media Communication*, GENHA project, 2021, Disponible en: http://genha.eu/sites/default/files/pdf/Anti-Gender%20Hate%20Speech%20in%20Populist%20Right-Wing%20Social%20Media%20Communication_0.pdf .

[21] C. PEDRAZA, *Cibermisoginia en las redes sociodigitales: claves para el análisis desde la masculinidad*, en *Cuestiones de género: de la igualdad a la diferencia*, 2019, n. 14, pp. 51-66.

y por conectar especialmente bien con las generaciones jóvenes a través de los nuevos canales de comunicación digitales. Esto en parte facilita, que las generaciones digitales sean en las que más abundan tanto entre los agresores como entre las víctimas de las diferentes formas de ciberviolencia de género.

Unidos a este movimiento global anti-género está la machosfera, que como se ha señalado es una variedad de comunidades misóginas online, asi como influencers, youtubers o comunicadores de todo tipo que utilizan masivamente el contexto digital para crear, compartir y difundir contenidos contra las mujeres, las feministas o la comunidad LGTBI. En ocasiones los individuos que integran esta machoesfera actúan individualmente, y otras veces de manera colectiva, pero organizados estratégicamente para atacar en el espacio virtual[22].

Algunas de estas comunidades misóginas virtuales tienen una presencia global, entre los que destacan los "activistas por los derechos de los hombres" (MRA, por sus siglas en inglés), que defienden a los hombres maltratados, y denuncian el trato que reciben los varones en los procesos de separación y divorcio, en especial, en las disputas sobre las custodias de los hijos/as y las decisiones sobre las pensiones de alimentos. Un segundo grupo son "los gurús del ligue" (PUA, por sus siglas en inglés, *pick up artists*), que utilizan sus comunidades virtuales para compartir estrategias para ligar, además de una variedad de recomendaciones sobre entrenamientos físicos, de éxito personal, o sobre las criptomonedas.

Pero una de las comunidades más representativas de esta machosfera son los *incels*, "célibes involuntarios"" Son hombres, que se identifican como incapaces de encontrar una pareja sexo-afectiva a pesar de desearlo, y que culpan a las propias mujeres de ello. Argumentan que las mujeres deberían estar sexualmente disponibles para los hombres y las acusan de egoístas, manipuladoras y dañinas para los hombres, y para la sociedad en su conjunto. Han creado incluso sus propios personajes en forma de memes, como *Chad*, una caricatura de hombre guapo, exitoso y con dinero, y *Stacy*, una imagen que ridiculi-

[22] N. IGAREDA, *El derecho a la libertad versus la libertad de expresión en la machosfera,* en *Derecho y Género,* 2024, n. 1, pp. 56-79; D. GING, *Alphas, Betas, and Incels: Theorizing the Masculinities of the Manosphere*, en *Men and Masculinities*, 2017.

za a las mujeres guapas, que sólo buscan dinero y promiscuas, entre otros memes ofensivos.

En el contexto español existen además algunas comunidades similares, pero más propias del contexto nacional, como Forocoches o Hispachan. También destaca la presencia de youtubers o influencers que de manera individual crean contenidos abiertamente misóginos y que comparten la ideología y la motivación de las comunidades misóginas virtuales (por ejemplo, Unblancohetero).

Las acciones de todas estas comunidades misóginas, y también de los influencers, youtubers o indivudos activos en el contexto virtual con contenidos y discursos abiertamente misóginos podría considerarse un indicador de este movimiento anti-género global, y también una consecuencia. En ocasiones sus acciones en el contexto digital se entienden amparados por el derecho a la libertad de expresión, ya que ser sexista, xenófobo u homófobo no es en sí mismo una cuestión ilegal, por muy despreciable que nos pueda parecer. Pero otras veces, las acciones de los integrantes de la machosfera pueden encajar en verdaderas formas de ciberviolencia de género[23].

Para los integrantes de la machosfera, el feminismo, las teorías de género y la presencia de las mujeres en el espacio virtual representan una amenaza a la masculinidad y se perciben como hombres las verdaderas víctimas. Consideran que el feminismo, y las feministas suponen una amenaza a los privilegios de los hombres, que, por otra parte, consideran naturales y normales[24].

Por consiguiente, las actuaciones de los diferentes la machosfera constituyen así una defensa del espacio masculino de Internet. Sus acciones están dirigidas a defender esta hegemonía masculina que se percibe en peligro. Dado que la agresividad se entiende como una característica inherente de la masculinidad hegemónica, las respuestas a estas pérdidas de poder se convierten en legítimamente agresivas y violentas. Estas acciones violentas de la machosfera también cuentan con

[23] L. RICHARDON-SELF, *Woman-Hating: On Mysogyny, Sexism, and Hate Speech*, en *Hypathia,* 2019, n. 33 (2), pp. 256-271.

[24] M. HANASH*, Disciplinamiento sexual: cazando brujas y ciberfeministas*, en *Investigación y Género. Reflexiones desde la investigación para avanzar en igualdad: VII Congreso Universitario Internacional Investigación y Género*, 2018, pp. 339-350.

la complicidad de otros usuarios de internet que aceptan y reproducen esa masculinidad hegemónica sin cuestionarla, compartiendo y difundiendo estos contenidos violentos[25].

La machosfera se convierte de esta manera en un como espacio de reforzamiento de la masculinidad hegemónica. En sus discursos se glorifica la masculinidad tradicional que asocia a los hombres con el dominio, el poder, la agresividad y el rechazo a mostrar vulnerabilidad. Igualmente, sus acciones contribuyen a perpetuar los roles de género rígidos donde las mujeres son vistas como subordinadas, y los hombres son incentivados a mantener una posición de control en las relaciones. Constituyen en su conjunto una reacción estratégica y organizada contra el feminismo donde se construyen narrativas que presentan al feminismo como una amenaza al "orden natural" y al bienestar de los hombres, lo que fomenta la hostilidad hacia las mujeres.

Cada vez hay más evidencia de que esta machosfera tiene un fuerte impacto en la socialización de los hombres jóvenes, y especialmente, en su educación sexual. Prueba de su impacto son estadísticas como las que muestra el barómetro de juventud de la FAD (2021), donde uno de cada cinco varones entre 15 y 29 años en España considera la violencia de género un "invento ideológico". Algunos autores/as han acuñado el término del "potencial polinizador" de la machosfera, para referirse al fenómeno en el que estos discursos elaborados por las distintas comunidades misóginas virtuales penetran en la esfera pública e influyen en la manera que tienen los hombres jóvenes de percibir la violencia de género, y la violencia sexual contra las mujeres en particular.

Desde edades tempranas, los hombres suelen ser socializados bajo la premisa de que deben cumplir con ciertos estereotipos de género, como, por ejemplo, que la agresividad representa como virtud y los hombres son enseñados a resolver conflictos mediante la imposición y la fuerza, lo que contribuye a la normalización de la violencia en sus interacciones. Otro estereotipo de género es el que desvaloriza siste-

[25] C. PEDRAZA, *op. cit.;* E. GARCÍA-MINGO, S. DÍAZ FERNÁNDEZ, *Jóvenes en la manosfera. Influencia de la misoginia digital en la percepción que tienen los hombres jóvenes de la violencia sexual. Centro Reina Sofía sobre Adolescencia y Juventud*, Fundación Fad Juventud, 2022.

máticamente lo femenino y se asocia lo femenino con debilidad, lo que refuerza el desprecio hacia las mujeres o hacia hombres que no cumplen con las expectativas de la masculinidad tradicional. Igualmente, otro estereotipo esencial es el que relaciona el control con el poder. En las relaciones, los hombres son incentivados a tener control sobre las decisiones, lo que puede derivar en dinámicas de poder abusivas[26].

La machosfera no solo refuerza estos valores tradicionales, sino que los radicaliza. Los foros y comunidades online funcionan como cámaras de eco (las llamadas *eco-chambers*) donde se validan actitudes misóginas y se refuerzan ideas que justifican la violencia hacia las mujeres. En muchos de estos espacios, la violencia se presenta como una respuesta "natural" o "justificada" al desafío a la autoridad masculina, lo que podría llegar a considerarse una verdadera apología de la violencia. Asmismo, la machoesfera contribuye a la elaboración de unas narrativas de victimización masculina en la que predomina una visión en la que los hombres son las verdaderas víctimas de un sistema que supuestamente privilegia a las mujeres, lo que alimenta el resentimiento y puede derivar en actos de violencia.

De la misma manera que las acciones de la machosfera contribuyen a crear un "caldo de cultivo" y una cultura misógina que influye en la socialización de género de los hombres, también favorecerá que indivudos no necesariamente integrantes de estas comunidades perpetren a su vez diferentes formas de ciberviolencia de género[27].

Esta interacción entre la socialización masculina y la machosfera contribuye a la violencia de género legitimando actitudes violentas cuando los discursos de la machosfera justifican o minimizan la violencia de género, lo que puede hacer que los hombres no vean sus acciones como problemáticas. También provoca procesos de deshumanización de las mujeres al reducirlas a estereotipos, lo que facilita la percepción de la violencia como una herramienta de control o castigo[28]. Y

[26] N. BONETA, E. GARCIA MINGO, S. TOMÁS, *Entendiendo el negacionismo de la violencia de género: Discursos sobre violencia de género entre adolescentes españoles/as*, en *Prisma Social: revista de investigación social,* 2024, n. 44, pp. 359-370

[27] E. GARCÍA MINGO Y S. DÍAZ FRENÁNDEZ, *op. cit.*

[28] J. GUTIERRAZ LORCA, E. GARCÍA MINGO, *"Busca, busca, perrita": comunidades digitales misóginas de difusión de imágenes sexuales sin consentimiento*, en *Ex aequo*, 2023, n. 48, pp. 15-32.

en último término también facilita procesos de reclutamiento y radicalización, ya que los hombres que han sido socializados en ambientes machistas encuentran en la machosfera un espacio que valida y profundiza su resentimiento hacia las mujeres[29].

3. *Los instrumentos legales para abordar la ciberviolencia de género*

Uno de los grandes retos del abordaje legal de la ciberviolencia de género es que, al ser un fenómeno muchas veces transnacional, y al tener lugar en un espacio virtual, los instrumentos legales que tradicionalmente se utilizan para prevenir y hacer frente a estas violencias devienen insuficientes[30].

En primer lugar, porque al tener lugar en un contexto virtual, resulta especialmente dificil aplicar la lógica del derecho de un territorio físico, una jurisdicción nacional y un ordenamiento jurídico estatal. Las víctimas de ciberviolencia de género tienen grandes dificultades para entender a qué poderes públicos y bajo qué legislación pueden acudir en búsqueda de amparo legal.

En segundo lugar, muchas veces estas formas de cibervioencia de género tienen lugar de manera transnacional, en redes sociales que son propiedad de empresas privadas, presentes a nivel global, y sin un domicilio legal claramente identificable. También es frecuente que las agresiones se hayan realizado por parte de individuos o grupos de individuos, difícilmente identificables, y aun menos, localizables geográficamente.

En tercer lugar, las diferentes formas de ciberviolencia de género cuesta que sean reconocidas legalmente como verdaderas "violencias", ya que tienen lugar en un espacio intangible. Además, nuestra tradición legal exige generalmente para poder calificar en un acto como violento, el ejercicio de la fuerza física, y por ejemplo, es aún muy costoso la admisión de la violencia psicológica en el ámbito de la violencia de género. De ahí, que ciertas actuaciones en el contexto virtual que

[29] L. RICHARDON-SELF, *Woman-Hating: On Mysogyny, Sexism, and Hate Speech*, en *Hypathia,* 2019, n. 33 (2), pp. 256-271.

[30] FEMBLOC*, op.cit.*

consideramos formas de violencia machista, se encontrarán con reticencias por parte de los operadores jurídicos.

El primer recurso en el ordenamiento jurídico español es el derecho penal. Algunas de las formas más graves de la ciberviolencia de género pueden encajar en algunos comportamientos tipificados como delitos en el código penal (CP). No siempre son reconocidos ni como violencia de género, ni como violencia sexual, ya que la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género sólo se ocupa de la violencia en el ámbito de la pareja o ex pareja, y muchas de estas formas de ciberviolencia de género son perpetradas por personas que no tienen, o no han tenido ninguna relación con la víctima.

Aun así, los diferentes actos violentos en el contexto digital contra las mujeres o contra las personas por su sexo, género, identidad de género u orientación sexual pueden encajar en delitos como el *sexting,* que implica enviar a otras personas vídeos y fotografías de contenidos sexual sin consentimiento de la persona afectada, con la intención de menoscabar gravemente su intimidad, y aunque hayan sido obtenidas con su consentimiento (art. 197.7 CP).

También pueden ser calificados como usurpación de personalidad, el hacerse pasar por otra persona para acceder a recursos o beneficios, usurpando el estado civil (art. 401 CP).

Otro posible delito es el *flaming trolling*, cuando la incitación o generación de discusiones online con un contenido sexista y ofensivo reúne las características para poder ser considerado un discurso de odio bajo el art. 510 del CP.

También esas acciones pueden ser constitutivas del delito de descubrimiento y revelación de secretos contenidos en el art. 197 del código penal, cuando castiga el acceso no consentido a datos alojados en dispositivos o ficheros, así como la escucha y grabación no consentida (art. 197.1 CP); el uso y modificación perjudicial de datos que se encuentren en un fichero público o privado para causar daños al titular o a un tercero (art. 197.2. CP); la divulgación de datos, ya sean contenidos o imágenes (art. 197.3 CP); el *sexpreading* o la divulgación no consentida de imágenes o grabaciones íntimas, castigando en este caso la primera persona que ha divulgado esos contenidos sin consentimiento (art. 197.7 CP).

En ocasiones podían ser calificadas como un delito de amenazas graves contenido en el artículo 169 del Código Penal, donde se castiga la amenaza a una persona, a su familia o a su entorno más íntimo de cometer contra ella o contra su entorno un delito de homicidio, lesiones, delito contra la libertad, de tortura, delitos contra al patrimonio o contra el honor. El delito de amenazas leves contenido en el art. 171 del código penal que castiga aquellas amenazas de un mal que no suponen un delito según su gravedad o las circunstancias de los hechos, incluyendo la exigencia de dinero o recompensa (art. 171.2. CP); las amenazas en el marco de la violencia de género (art. 171.4 del CP); como el delito leve de amenazas fuera del ámbito de la pareja o expareja (art. 171.7 CP).

Ciertas formas de ciberviolencia de género cumplen los elementos del delito de daños o sabotaje informático contenido en el art. 264 del código penal, que incluye la conducta de borrar, dañar, deteriorar, alterar, eliminar o hacer inaccesibles datos o programas informáticos o documentos electrónicos ajenos.

También es frecuente que la ciberviolencia de género encaje en el delito de coacciones contenido en el art. 172.1 del código penal que castiga el hecho de impedir a una persona con violencia, algo que la ley no prohíbe; las coacciones leves (art. 172.3 CP); las coacciones en el ámbito de la pareja o ex pareja (art. 172.3 CP).

Aunque quizás uno de los delitos que más se invocan en la ciberviolencia de género es el delito de acoso *stalking* contemplado en el art. 172 *ter* del código penal. El delito de *stalking* castiga el acoso a otra persona de manera reiterada, alterando el normal desarrollo de su vida cotidiana mediante la vigilancia, la persecución o la cercanía física; intentando establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas; mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella; atentando contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Una tipificación penal no tan común, pero igualmente aplicable a algunas formas de ciberviolencia de género es el delito contra la integridad moral contenido en el art. 173.1 del código penal que castiga el delito genérico de maltrato, denigración o vejación. Se utiliza para cas-

tigar las violencias de género que no pueden encajar en otros tipos penales más específicos y además tiene un párrafo dedicado al ámbito laboral: "… serán castigados los que, en el ámbito de cualquier relación laboral o funcionarial y prevaliéndose de su relación de superioridad, realicen contra otro de forma reiterada actos hostiles o humillantes que, sin llegar a constituir trato degradante, supongan grave acoso contra la víctima". También permite castigar a los divulgadores posteriores al primer divulgador del delito de *sexpreading* del art. 197.3 del CP: "… 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores".

Obviamente también serían de aplicación el delito de lesiones contenido en el art. 147.1. del código penal que castiga a quienes mediante cualquier medio o procedimiento causen en otra persona una lesión que perjudique su integridad corporal o su salud física o mental. El delito de inducción al suicidio contenido en el art. 143 del código penal, que puede llegar a realizarse parcialmente o en su totalidad a través de medios digitales. El art. 143 *bis* del CP castiga la inducción al suicidio a través de medios digitales a menores de edad o personas discapacitadas necesitadas de especial protección. O el delito de calumnias contenido en el art. 205 del código penal que castiga imputar un delito a otra persona sabiendo que es una acusación falsa. Y finalmente el delito de injurias contenidos en el art. 208 del código penal donde se castigan acciones o expresiones que lesionan la dignidad de la víctima, dañando su fama o atentando a su autoestima.

Quizás uno de los delitos más invocados es el delito de odio contenido en el art. 510 del código penal que castiga a quienes públicamente fomenten, promuevan o inciten directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su sexo, orientación o identidad sexual, por razones de género[31]. También castiga a quienes produzcan, elaboren, posean con la finalidad de distribuir, faciliten a terceras personas el acceso, distribuyan, difundan o

[31] F. MIRÓ, *Taxonomía de la comunicación violenta y el discurso del odio en Internet*, en *Revista de Internet, Derecho y Política*, 2016, n. 22, pp. 93-118.

vendan escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos para fomentar, promover, o incitar directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo por las razones anteriores. Igualmente castiga a quienes públicamente nieguen, trivialicen gravemente o enaltezcan los delitos cometidos contra un grupo o una parte del mismo, o contra una persona determinada por razón de su sexo, orientación o identidad sexual, por razones de género cuando de este modo se promueva o favorezca un clima de violencia, hostilidad, odio o discriminación contra los mismos[32].

En segundo lugar, en el ordenamiento jurídico español encontramos la legislación que protege el derecho al honor bajo la jurisdicción civil. Muchas de estas formas de ciberviolencia de género suponen un ataque al derecho al honor, a la intimidad de la persona y a su propia imagen. En el ordenamiento jurídico español nos encontramos con una normativa en el ámbito civil que protege este derecho fundamental contenido en el artículo 18 de la Constitución española, la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. La finalidad principal de esta ley es reparar los daños que un individuo puede sufrir tras las violaciones de este derecho fundamental, y esta reparación se traduce esencialmente en una indemnización económica.

Pero una de las características de este recurso legal es que, al ser una normativa del ámbito civil, la jurisdicción competente es la jurisdicción civil que es competente para resolver conflictos entre individuos, y, por lo tanto, no hay ningún interés público en ello. Esto significa que, a diferencia de la denuncia penal, si se interpone una demanda, y el Juzgado la desestima finalmente, será la persona demandante quien tenga que hacerse cargo de las costas judiciales, incluyendo los honorarios de la representación letrada y procesal de la parte contraria. Esto explica por qué muy pocas víctimas opten por esta vía frente a los ataques sufridos en su derecho al honor, a la intimidad personal y familiar o a su propia imagen.

Además de esta particularidad de la jurisdicción civil, también hay

[32] N. IGAREDA, *El derecho a la libertad versus la libertad de expresión en la machosfera,* en *Derecho y Género,* 2024, n.1, pp. 56-79.

que tener en cuenta que los tribunales a la hora de proteger los derechos fundamentales mencionados deben tener en consideración los usos y costumbre sociales, así como la conducta previa del titular de los derechos afectados, tal y como establece el art. 2.1. de dicha ley "La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservada para sí misma o su familia".

La aplicación e interpretación de esta provisión legal podría llegar a producir que, si la víctima ha tenido una participación activa en redes sociales, por ejemplo, publicando imágenes personales, o compartiendo información personal en abierto, será más difícil que el juez/a considere como intromisiones en este derecho fundamental determinados ataques por parte de la machosfera[33].

En tercer lugar, encontramos el recurso al derecho al olvido. El derecho al olvido consiste en la posibilidad de eliminar la información personal almacenada en el entorno digital, y también la posibilidad de eliminar los vínculos de una persona con datos revictimizadores existentes en Internet[34]. Esta segunda posibilidad ocurre cuando una persona encuentra que los motores de búsqueda en Internet continúan asociando su nombre a hechos y/o datos en el entorno digital que provocan una revictimización (por ejemplo, cuando esa persona ya ha sido previamente víctima de un ataque que de nuevo aparece vinculada) o una vulneración de sus datos personales. El ejercicio de este derecho al olvido será independiente de las posibles denuncias por los ataques sufridos en el contexto virtual que la víctima interponga y de sus procesos judiciales.

En ocasiones, el ejercicio de este derecho al olvido, y la protección de los datos personales relacionados, resulta controvertido cuando la persona titular de los derechos es alguien famoso o con una proyección pública, así como cuando los ataques a sus datos personales han

[33] FEMBLOC, *op.cit.*

[34] M. MARTÍNEZ LÓPEZ-SAÉZ, *Propuestas de regulación frente a una nueva brecha digital por razón de género: ciberviolencia contra la mujer a la luz del marco europeo de protección de datos*, en *Revista de Estudios Jurídicos y Criminológicos*, 2021, n. 4, pp. 211-233.

sido objeto de una amplia cobertura mediática. Este supuesto es especialmente importante en los ataques de las comunidades misóginas de la machosfera, que como se ha señalado, se ensañan especialmente en las mujeres que debido a su activa presencia en el entorno virtual, ya sea por su actividad política, profesional, informativa o activista.

En cuarto lugar, también podemos identificar el recurso a los nuevos instrumentos legales aprobados en el ámbito del derecho antidiscriminatorio en el ordenamiento jurídico español. Suponen nuevos instrumentos de tutela administrativa incluidos en la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y no discriminación, cuando por ejemplo define el acoso discriminatorio en el artículo 6.4. O si se amplía la aplicación del acoso sexual y acoso por razón de sexo contenido en la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres cuando tienen lugar en el contexto digital.

4. *Los límites del abordaje legal*

Más allá del abanico de posibles instrumentos legales a los que las víctimas de ciberviolencia de género pueden acudir, y de algunas de las particularidades de algunos de estos recursos (como el recurso a legislaciones proyectora de la jurisdicción civil o administrativa), también existen algunos límites o problemas comunes que se enumeran a continuación[35].

Una primera categoría de problemas está en la misma redacción legal. En general, se puede hablar de verdaderas lagunas legislativas ya que aún no se cubren adecuadamente las diferentes formas de ciberviolencia de género. Por ejemplo, aun en materia penal se echa de menos la tipificación específica como formas de violencia de género. Los casos se abordan bajo legislaciones genéricas, como las de acoso o difamación, pero no reconocen las dinámicas de género en el ámbito digital. Además, podemos encontrar limitaciones en las definiciones legales, tanto en el ámbito penal, como civil o administrativo. Los con-

[35] N. VERGÉS, *Redes sociales en perspectiva de género: guía para conocer y contrarrestar las violencias de género on-line*, 2017, Disponible en: https://bit.ly/3b0wdCO

ceptos de "violencia", "intimidad" o "acoso" suelen estar vinculados al ámbito físico, dejando fuera muchos comportamientos que ocurren en entornos digitales. Asimismo, está la dificultad del carácter transnacional de muchas de estas formas de ciberviolencia de género. Internet opera a nivel global, pero las leyes tienen alcance nacional. Esto dificulta perseguir ciberdelitos que involucren a perpetradores ubicados en otros países.

Una segunda categoría de problemas está en la dificultad en la identificación de agresores. El anonimato propio del contexto digital permite que los agresores se escondan detrás de identidades falsas, dificultando su identificación y la atribución de responsabilidad. Igualmente, muchas de las formas de ciberviolencia de género se ejercen de manera colectiva y masiva, la violencia en línea puede ser perpetrada por múltiples agresores (como en los casos de ataques coordinados o *doxing*), lo que complica la persecución legal de todos los involucrados.

Un tercer grupo de problemas son los obstáculos puramente técnicos y burocráticos, por ejemplo, las dificultades de prueba, dado que la recopilación de evidencia digital es compleja. Las posibles capturas de pantalla, los registros de chats o correos pueden ser fácilmente alterados, y garantizar su validez jurídica requiere procesos técnicos costosos y especializados. También nos encontramos con los retrasos en la respuesta de plataformas en las que tienen lugar estas formas de violencia digital. Las grandes plataformas digitales (como redes sociales) suelen ser lentas para colaborar con los poderes públicos y operadores jurídicos, ya sea por procesos internos, falta de regulación clara o resistencia a compartir datos de sus usuarios. En esta categoría de obstáculos técnicos también se identifica muchas veces la falta de recursos en las instituciones responsables de dar una respuesta legal a la ciberviolencia de género. Muchas instituciones no cuentan con personal capacitado ni con herramientas tecnológicas para investigar estos ciberdelitos.

Una cuarta clasificación de factores que incluyen en la respuesta legal frente a la ciberviolencia de género es la invisibilización social de la ciberviolencia de género. Muchas formas de violencia de género digital, como los comentarios misóginos o el envío no solicitado de imágenes sexuales, son vistas como "normales" o inofensivas, lo que difi-

culta su reconocimiento como delitos graves, tanto por parte de la sociedad en su conjunto como por parte de las propias víctimas[36].

Es además frecuente la culpabilización a las víctimas, como por ejemplo en casos como la difusión no consentida de imágenes íntimas, las víctimas suelen ser culpabilizadas ("no debiste tomarte esas fotos"), lo que las disuade de denunciar.

También contribuye a esta invisibilización de la ciberviolencia de género la falta de formación por parte de policías, jueces y fiscales que muchas veces no están sensibilizados o capacitados en la perspectiva de género, lo que puede llevar a minimizar o desestimar los casos[37].

En quinto lugar, encontramos las limitaciones en la regulación de plataformas digitales donde tienen lugar muchas de las formas de ciberviolencia de género. Nos encontramos con una ausencia de responsabilidades claras, y aunque tienen políticas para combatir el contenido violento o misógino, estas no siempre se aplican de manera efectiva, y no existe suficiente regulación que las obligue a actuar con rapidez.

Las redes sociales permiten la rápida difusión de contenido dañino, y las medidas para su retirada suelen ser insuficientes o tardías, careciendo de instrumentos para prevenir y/o frenar discurso de odio que se hacen fácilmente virales. En general las regulaciones de estas plataformas digitales tienen enfoques más reactivos que preventivos y solo actúan cuando se presenta una denuncia, en lugar de adoptar medidas preventivas o proactivas para proteger a las usuarias.

Y por último nos encontramos con una falta de armonización global. Al ser la ciberviolencia de género un fenómeno muchas veces transnacional, las diferencias legales entre países generan vacíos legales que los agresores pueden aprovechar. Si un agresor actúa desde otro país, es posible que las leyes locales no puedan aplicarse debido a la falta de acuerdos internacionales efectivos.

[36] A. Del Prete and S. Redón-Pantoja, *The Invisibility of Gender-Based Violence in the Social Network*, en *Multidisciplinary Journal of Gender Studies*, 2022, n. 11(2), pp. 124-143.

[37] L. Serra, *Masclisme 2.0: Una oportunitat per a repensar l'abordatge de les violències Masclistes*, en *Idees: Revista de temes contemp*oranis, 2019, n. 47, pp. 1-7

Finalmente podrías concluir que los instrumentos legales disponibles en el ordenamiento jurídico español son mejorables, ya que deberían partir del diagnóstico de género que caracterizan estas violencias digitales. También las herramientas legales necesitan adaptarse a los retos que supone el contexto virtual que cada vez tiene mayor importancia en la vida de las personas, ya que es a través de internet y las redes sociales donde nos relacionamos, nos comunicamos, nos informamos, y trabajamos.

En último lugar, la lucha del derecho contra las diferentes formas de ciberviolencia de género debería avanzar en otros ámbitos del derecho más allá del derecho penal, que se muestra insuficiente para dar respuesta a un fenómeno estructural como es la violencia de género, tanto en el ámbito analógico, como digital[38]. Existe todo un camino por explorar en el ámbito del derecho antidiscriminatorio que podría servir como instrumento de transformación social y de garantía y tutela de los derechos fundamentales afectados en las diferentes ciberviolencias de género, abordando las causas estructurales de estas formas de violencia, y apelando a las responsabilidades de los poderes públicos en la materia[39].

Abstract

La ciberviolencia de género abarca todas las formas de violencia digital que se dirigen contra las personas por razón de su sexo, género u orientación sexual. Es un fenómeno global, con características como el anonimato, la viralidad o la permanencia, que lo convierten en un fenómeno en ocasiones más victimizador. Las diferentes formas de ciberviolencia de género están conectadas a un movimiento político global anti-género, que busca cuestionar las teorías de género que han denunciado el patriarcado. Es por ello que estas violencias digitales se convierten la mayoría de las veces en herramientas de control y disciplina para las mujeres en el contexto digital, y en su caso, para facilitar su expulsión. El abordaje legal desde el ordenamiento jurídico español ha sido

[38] P. LLORIA, *Algunas reflexiones sobre la perspectiva de género y el poder de castigar del Estado*, en *Estudios Penales y Criminológicos*, 2020, n. 40,

[39] N. IGAREDA, *op. cit.*

tradicionalmente punitivo, pero insuficiente para dar respuesta a un fenómeno estructural, que requiere una actuación garantista de los derechos fundamentales de las víctimas.

PALABRAS CLAVE: Ciberviolencia de género – anti-género – machosfera – derecho – derecho antidiscriminatorio

LA CYBERVIOLENZA DI GENERE IN SPAGNA: LIMITI E OPPORTUNITÀ DELLA RISPOSTA LEGALE A UN FENOMENO GLOBALE

La violenza informatica basata sul genere comprende tutte le forme di violenza digitale dirette contro le persone in base al loro sesso, genere o orientamento sessuale. È un fenomeno globale, con caratteristiche come l'anonimato, la viralità o la permanenza, che lo rendono un fenomeno talvolta più vittimizzatore. Le diverse forme di cyberviolenza di genere sono collegate a un movimento politico globale anti-genere, che cerca di mettere in discussione le teorie di genere che hanno contrastato il patriarcato. Ecco perché queste violenze digitali diventano nella maggior parte dei casi strumenti di controllo e disciplina per le donne nel contesto digitale e, se del caso, per facilitarne l'espulsione. L'approccio giuridico dell'ordinamento spagnolo è stato tradizionalmente punitivo, ma insufficiente a rispondere a un fenomeno strutturale e che richiede un'attuazione garantista dei i diritti fondamentali delle vittime.

KEYWORDS: violenza informatica di genere – anti-genere – machosfera – diritto – diritto antidiscriminatorio

LA PROTECCIÓN PENAL DEL DERECHO A LA IMAGEN ÍNTIMA. ESPECIAL REFERENCIA A LOS CASOS DE *DEEPFAKE* SEXUAL

Ángeles Jareño Leal[*]

SUMARIO: 1. Introducción. – 2. La difusión sin consentimiento de la imagen íntima en el entorno digital: el artículo 197, párrafos 1 y 7 del código penal. – 2.1. La difusión de la imagen íntima cuando ha sido captada "sin" consentimiento. – 2.2. La difusión de la imagen íntima cuando ha sido captada "con" consentimiento. – 3. El acoso digital utilizando la imagen de una persona: art. 172 ter 5 del código penal (ciberacoso). – 4. La calificación típica de la elaboración y difusión del *deepfake* sexual.

1. *Introducción*

La protección del derecho a la imagen íntima se ubica en el código penal español en varios preceptos, y proviene de la declaración del artículo 18.1 de la Constitución española, al señalar que: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". Además, este derecho también encuentra protección de carácter civil en la ley orgánica 1/1982, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, de 5 de mayo de 1982. Por su parte, la jurisprudencia constitucional española ha configurado el derecho a la imagen siguiendo la doctrina del Tribunal Europeo de Derechos Humanos, que engloba su protección dentro del concepto de vida privado recogida en el artículo 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales de Roma[1]. Cuando analizamos la realidad jurisprudenc-

* Catedrática de Derecho penal. Universidad de Valencia (España). angeles.jareno@uv.es

[1] Art. 8 del Convenio: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". Hay que recordar que el Convenio fue redactado en un momento histórico ajeno al desarrollo de la tecnología audiovisual actual.

cial comprobamos que las conductas recogidas en el código penal a las que aquí voy a hacer referencia suelen tener como sujeto pasivo a la mujer, así que puede decirse que estamos ante delitos con un sesgo de género, aunque la configuración de los tipos penales no recoge ninguna restricción en este sentido.

Las posibilidades de lesionar el derecho a la imagen íntima en el ámbito digital son muy variadas, si bien me centraré aquí en el análisis específico de alguna de ellas por razones de espacio: 1)la captación y difusión sin consentimiento de la imagen íntima; 2)la difusión sin consentimiento de la imagen previamente captada con tal consentimiento; 3)el delito de "acoso digital"; y 4)la calificación penal del *deepfake* sexual/pornográfico. Esta última forma de agresión ha irrumpido de forma más o menos reciente en el terreno del derecho penal, para plantear el problema de averiguar cuál debe ser la calificación correcta de los casos en los que, con el uso de un sistema de Inteligencia Artificial (en adelante IA), se genera o manipula un contenido de imagen o vídeo para lograr imágenes con un contenido sexual o pornográfico que resultan casi reales. En el apartado correspondiente realizaré una propuesta de tipificación, y analizaré las dificultades para encajar esta conducta en otros preceptos existentes en el código penal.

2. La difusión sin consentimiento de la imagen íntima en el entorno digital: el artículo 197, párrafos 1 y 7 del código Penal

El art. 197 del código penal se encuentra dentro del Título XIX, que se refiere a los "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio". Dentro Capítulo I, titulado "Del descubrimiento y revelación de secretos", encontramos diferentes conductas atentatorias contra la intimidad, entre las cual interesan aquí, especialmente, las reguladas en los párrafos primero y séptimo de dicho precepto.

2.1. *La difusión de la imagen íntima cuando ha sido captada "sin" consentimiento*

Art. 197.1 CP: "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses…

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior"[2]

El apartado primero de este artículo castiga (entre otras cosas) la captación de la imagen que se ha llevado a cabo utilizando medios subrepticios, es decir, quebrantando la reserva puesta por el titular. De manera que el propio precepto exige medios comisivos determinados, pues usa términos como "interceptar" o "utilizar artificios técnicos"[3]. Por tanto, el conocimiento de la imagen íntima que tiene lugar de for-

[2] El art. 197 del código penal español recoge desde hace años (1995) un grupo de conductas que encajan con lo señalado en el artículo 5. 1. A) de la reciente directiva 2024/1385/UE del Parlamento europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, de 14 de mayo de 2024, en DOUE 1385 de 24 de mayo de 2024, cuando señala que los estados miembros deben garantizar la punibilidad de las conductas que hacen "accesible al público mediante tecnologías de la información y de las comunicaciones (TIC), imágenes, videos o materiales similares que representen actividades sexualmente explícitas o las partes íntimas de una persona sin su consentimiento, cuando sea probable que tal conducta cause graves daños a esa persona".

[3] A. JAREÑO LEAL, *Intimidad e imagen: los límites de la protección penal*, Madrid, 2008, p. 23.

ma natural (por ejemplo, observando a través de una ventana) no constituye un delito.

Según la letra del artículo 197.1 el mero hecho de captar la imagen de una persona en un contexto íntimo, de forma subrepticia, viene a constituir el delito recogido en el precepto. Pero, además, en el párrafo tercero se establece una agravación de la pena cuando dicha imagen se difunde, revela o cede a terceros, por ejemplo, a través de correo electrónico, *whatsapp,* redes sociales, chats, etc. La pena en este caso es más grave porque las posibilidades de difusión son infinitas, de forma que la lesión al bien jurídico se ve multiplicada y es irreversible si ha entrado en internet. De hecho, la gravedad de esta conducta es tal que el código penal llega a castigar también a quien no lleva a cabo la captación de la imagen, pero la recibe, por ejemplo, por *whatsapp* y, a su vez, la transmite a otras personas, en el art. 197.3, apartado segundo.

La cuestión más difícil de resolver al aplicar este precepto es decidir qué debe entenderse por "imagen íntima", ya que se trata de un bien jurídico con unos límites algo difusos, que dependen del valor social del concepto y de la propia voluntad de su titular (recordemos que estamos entre los llamados "delitos contra la intimidad", por lo que la protección penal debe ceñirse a las imágenes captadas en dicho contexto). Así que la primera cuestión que hay que resolver es, precisamente, acotar un concepto sobre el que no hay un estándar social uniforme, a salvo de las imágenes en un contexto sexual, que siempre pueden incardinarse en el objeto de protección del delito[4]; pero, fuera de este ámbito, depende de la propia valoración judicial delimitar lo que constituye la intimidad[5]. Se trata de una cuestión trascendental, ya

[4] De hecho, el propio código penal contiene una agravación penológica específica en el artículo 197.5 para los casos en que la imagen se refiere a "la vida sexual" de una persona.

[5] Puede citarse como ejemplo la sentencia del Tribunal Supremo de 11 de julio de 2022, n. 699/2022. Los hechos probados se refieren a una mujer que envía a su pareja una foto por *whatsapp* en la que aparece con el torso desnudo y, tras la ruptura sentimental, el varón reenvía dicha fotografía a otra persona. Para el Tribunal Supremo existe una vulneración grave de la intimidad, mientras que, en sentido contrario, el Tribunal inferior (cuya sentencia es revisada) había absuelto por estos mismos hechos, considerando que reenviar una foto mostrando el pecho de una mujer no constituye

que para tipificar la conducta en el código penal es necesario delimitar el perfil del bien jurídico, pues, en el caso de que la imagen difundida no tenga carácter íntimo, la respuesta jurídica debe encontrarse en la ley 1/1982.

Además, a la vista del mayor peligro que el uso de medios tecnológicos implica para el derecho a la imagen es necesario revisar dicho concepto recogido como derecho fundamental en el artículo 18.1 de la Constitución española. La utilización de la IA para recrear imágenes idénticas a las veraces obliga a replantearnos esta cuestión, para perfilar con más precisión qué conductas deben incardinarse en los delitos contra la intimidad, cuáles deben acogerse en otros preceptos penales, y en qué casos debe delegarse la protección al ámbito civil de la ley 1/1982. A tales efectos, mi conclusión personal es que el código penal sólo protege en el art. 197.1 la representación de la verdad, es decir, la imagen íntima que reproduce los rasgos auténticos de una persona; por lo que una imagen generada con IA, aunque se refiera a un contexto íntimo (*deepfake* sexual/pornográfico), no es objeto de protección en dicho precepto. Dentro del art. 197.1 sólo puede ser típica la imagen íntima "original", la que es auténtica y reproduce los rasgos reales de una persona, siendo ésta la única conclusión a la que puede llegarse si partimos de que el artículo 197 refleja el valor expresado en el artículo 18.1 de la Constitución, que se refiere a derechos fundamentales de carácter moral cuando garantiza "el derecho al honor, a la intimidad personal y familiar y a la propia imagen"[6]. En este sentido, el Tribunal Constitucional español ha sido siempre claro, sosteniendo que en dicho precepto se protege de forma autónoma el derecho a la imagen como forma de salvaguardar un ámbito propio y reservado (no necesariamente íntimo) frente a la acción y el conocimiento de los demás; declarando que se trata de una concreción del más amplio dere-

una vulneración grave de la intimidad. También es de interés la sentencia de la Audiencia Provincial de Cádiz de 28 de enero de 2020, n. 35/2020, en la que no se considera un atentado grave a la intimidad la difusión de una fotografía en la que una mujer se encuentra posando en ropa interior, sin que se vea su rostro u otro dato que permita su identificación.

[6] *Vid* sobre esta cuestión A. JAREÑO LEAL, *El derecho a la imagen íntima y el Código penal. La calificación de los casos de elaboración y difusión del deepfake sexual*, en *Revista Electrónica de Ciencia Penal y Criminología,* 2024, n. 26, pp. 12 y ss.

cho a la dignidad, y añadiendo que el artículo 18.1 de la Constitución lleva a cabo una protección "de la esfera moral y relacionada con la dignidad humana y con la garantía de un ámbito privado libre de intromisiones ajenas". Y sigue afirmando de forma constante dicho Tribunal Constitucional que el derecho a la imagen abarca para su titular la facultad de decidir qué información gráfica puede tener difusión pública, así como la facultad de impedir su captación, reproducción o publicación por parte de cualquier persona no autorizada, sea cual sea la finalidad perseguida (informativa, comercial, científica o cultural)[7]. En definitiva, el derecho fundamental a la intimidad resulta lesionado sólo cuando la imagen que se capta y difunde es una reproducción de "la verdad", por lo que podemos concluir que las escenas sexuales simuladas con IA no encuentran acogida en el grupo de delitos contra la intimidad.

Además, a la hora de establecer el límite entre la protección penal y la protección civil del derecho a la imagen puede concluirse de la forma siguiente: si la captación audiovisual de la imagen tiene lugar en el *contexto de la vida íntima* de una persona, la protección que debe otorgarse es la recogida en el código penal; por el contrario, si la intromisión en el derecho a la imagen se produce en un *contexto de carácter neutro*, ajeno a la intimidad, debe acudirse al ámbito de la ley civil 1/1982[8].

[7] Se trata de una doctrina que se ha mantenido de forma constante. *Vid* por todas dos sentencias separadas en el tiempo, pero coincidentes en sus fundamentos: sentencia del Tribunal Constitucional de 26 de marzo de 2001, n. 81/2001, y sentencia del Tribunal Constitucional de 24 de febrero de 2020, n. 27/2020.

[8] Un claro ejemplo de conducta penalmente típica es la castigada por la sentencia del Tribunal Supremo de 19 de enero de 2023, n. 15/2023, en el caso del varón que coloca una cámara oculta en el dormitorio de la mujer una vez que han roto su relación sentimental, con la finalidad de controlar su vida íntima.

Entre la doctrina C. JUANATEY DORADO, *Protección penal de la intimidad frente a la utilización ilícita de medios digitales. Un análisis de la reciente doctrina jurisprudencial*, en *Revista General de Derecho Penal*, 2023, n. 39, pp. 7 y ss., apunta que para justificar la intervención penal es necesario realizar "un juicio de ponderación específico que atienda, fundamentalmente, al lugar en el que se desarrolle el hecho, en su caso, y los aspectos de la vida personal que se vean involucrados".

2.2. *La difusión de la imagen íntima cuando ha sido captada "con" consentimiento*

Art. 197.7 CP: "Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada.

En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior cuándo los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa."

La conducta principal castigada en este precepto consiste en captar la imagen audiovisual de una persona con su consentimiento y después difundirla, por ejemplo, en las redes sociales o a través de *whatsapp,* sin contar con su voluntad. Los ejemplos más frecuentes que encontramos en la jurisprudencia sobre el art. 197.7 CP tienen lugar cuando las imágenes han sido captadas en un contexto de intimidad sexual dentro de una pareja, con el acuerdo de ambas partes, y una vez finalizada la relación uno de ellos, generalmente el varón, las difunde en las redes a modo de venganza, o por celos. Para un sector de la doctrina española y de la jurisprudencia aquí también se incluyen los casos en que la propia víctima es quien envía por estos medios a otra persona su propia imagen íntima. De tal forma, se dice, que el tipo acoge ambas modalidades de conducta: captar la imagen, o recibirla y, después, en ambos casos, difundirla sin contar con el consentimiento de quien es su titular[9]. Sin embargo, es muy discutible que la

[9] Pueden encontrarse argumentos a favor de la interpretación que hace la juris-

segunda modalidad, recibir de la propia víctima la imagen de carácter íntimo, pueda incardinarse en este tipo penal. De hecho, el artículo 197.7 señala expresamente que el propio sujeto activo "hubiera obtenido" la imagen audiovisual, lo cual parece incompatible con el hecho de que sea la víctima quien capta su propia imagen y después la remite a otra persona[10]. Aunque es cierto que, cómo también señala la doctrina, este resultado produce efectos restrictivos que carecen de sentido político criminal, y aunque se trata de un defecto de redacción que, seguramente, pasó desapercibido para el legislador, el principio de legalidad obliga a respetar la tipicidad[11].

En definitiva, la conducta recogida en el artículo 197.7 del código

prudencia en: A. COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad: (arts. 197, 197 bis y 197 ter),* en J. L., GONZÁLEZ CUSSAC (a cura di), *Comentarios a la Reforma del Código Penal de 2015*, Valencia, 2015, p. 668; M. A. RUEDA MARTÍN, *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* Barcelona, 2018, p. 166; C. JUANATEY DORADO, *Intimidad y revelación no consentida de imágenes o grabaciones audiovisuales* (art. 197.7 CP), en V. GÓMEZ MARTÍN (a cura di) *Un modelo integral de Derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*, *Vol. II*, Madrid, 2022, p. 1229; F. MORALES PRATS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio,* en G. QUINTERO OLIVARES (dir), *Comentarios al Código Penal español, Vol I*, Navarra, 2016; P. LLORIA GARCÍA, *La difusión de imágenes íntimas sin consentimiento (a propósito de la Sentencia 70/2020 del Tribunal Supremo de 24 de febrero de 2020),* en *LA LEY Privacidad,* 2020, n. 4, p. 4; y la misma autora: *La difusión tecnológica de imágenes íntimas sin consentimiento como manifestación de violencia de género,* en J. G. FERNÁNDEZ TERUELO, P. FERNÁNDEZ-RIVIERA GONZÁLEZ (Dirs.), *Nuevas formas de prevención y respuesta jurídico-social frente a la violencia de género,* Navarra, 2022, p. 199. Sostienen argumentos en contra en: C. TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos,* en M. GÓMEZ TOMILLO (Dir.), *Comentarios prácticos al Código penal, Vol. II*, Navarra, 2015, p. 671; A. JAREÑO LEAL, cit., p. 23.

[10] El tipo del párrafo segundo es ajeno a este problema ("Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada"), pues castiga al que, sin intervenir en la conducta del tipo básico, pero conociéndola, recibe la imagen de quien la ha captado con consentimiento y, a su vez, sigue difundiéndola sin consentimiento del titular.

[11] Pese a ello, el Tribunal Supremo, en su sentencia de 24 de febrero de 2020, n. 70/2020, declara que este precepto es de aplicación al caso en que una mujer envía a su pareja una foto en la que aparece desnuda, por el teléfono móvil, y tras la ruptura el hombre la reenvía a una tercera persona.

Penal protege sólo la difusión sin consentimiento de la imagen íntima de una persona cuando ha sido previamente captada con su consentimiento. Debiendo recordarse de nuevo que el concepto de intimidad no queda reducido al contexto sexual o erótico, como ya se ha señalado, sino que es más amplio. Así que también en este párrafo lo más complejo de resolver es determinar si la imagen difundida es o no una imagen de carácter íntimo. Una vez más, tengamos presente que si se trata de una imagen en un contexto neutro la protección debe quedar extramuros del Derecho penal, dentro del ámbito civil propio de la ley 1/1982.

3. *El acoso digital utilizando la imagen de una persona: art. 172 ter 5 del código penal (ciberacoso)*

"Art. 172 ter 5 CP: El que, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación, será castigado con pena de prisión de tres meses a un año o multa de seis a doce meses. Si la víctima del delito es un menor o una persona con discapacidad, se aplicará la mitad superior de la condena".

Encontramos aquí una figura delictiva que es reciente en el código penal español, castigando una modalidad de "violencia digital", y cuya última modificación se ha realizado con la ley orgánica 1/2023[12]. Se trata de una conducta que anteriormente era tipificada por los tribunales acudiendo a otros delitos como, por ejemplo, el de injurias o, en determinados casos, contra la intimidad; pero este reciente tipo penal se encuentra en un grupo de delitos ajenos al ámbito de la intimidad. Por tanto, no es necesario que la imagen que se utiliza para llevar a cabo el acoso digital sea una imagen íntima, sino que también la imagen en un contexto neutro puede ser

[12] Ley Orgánica 1/2023, *por la que se modifica la Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo*, de 28 de febrero de 2023.

objeto material del delito, ya que no se trata de proteger el derecho fundamental a la intimidad, sino de evitar una situación de acoso, hostigamiento u humillación. Dicho objetivo también puede conseguirse con el uso de una imagen digital creada con IA, por lo que en el caso de utilizarse un *deepfake*, sea o no de carácter sexual, la conducta sí que puede incardinarse en este precepto (a diferencia de lo que ocurre con el artículo 197 del código penal, dónde hemos visto que se protege la imagen íntima que representa la verdad, es decir, la que es auténtica y original). Un ejemplo característico de la conducta que ahora se analiza consiste en utilizar la imagen identificable de una persona, creada con IA, y abrir un perfil falso utilizando el nombre, email, teléfono u otros datos personales suyos, ofreciendo supuestos servicios sexuales. Además, como el precepto se refiere de forma genérica a la imagen, cabe en el tipo penal la utilización del rostro o de la figura completa, ya sea auténtica o falsificada. En definitiva, estamos ante un delito que castiga el uso abusivo de la imagen en el entorno digital, con la finalidad dolosa de crear a la víctima la situación que describe el tipo, y que constituye el resultado material del delito: acoso, hostigamiento o humillación. Aunque el precepto no contiene una referencia al género, de nuevo nos encontramos ante conductas que suelen producirse más sobre las mujeres, normalmente en los casos en que, después de la ruptura sentimental, el varón busca una suerte de venganza sobre su expareja. Lo característico de este delito es que el autor no es el que materializa el acoso u hostigamiento, sino que tales conductas son realizadas por terceras personas que desconocen la falsedad de la situación, lo que tiene como consecuencia que no existe imputación penal para las mismas.

Por otro lado, este delito se encuentra dentro del grupo de las coacciones (Capítulo III del Título VI del código penal: Delitos conta la libertad), donde el bien jurídico protegido genéricamente es la libertad personal. En consecuencia, para que se produzca el tipo penal que ahora se analiza debe constatarse que la víctima se ve obligada a soportar múltiples intentos de acercamiento por parte de terceros, de forma que dicho acoso (por correo electrónico, llamadas de teléfono o *whatsapp*) le produzca una situación de humillación y hostigamiento. Precisamente, teniendo en cuenta este resultado del acoso puede apa-

recer en concurso con el delito de injurias (art. 208 del código penal), si al crear el perfil falso de la víctima se le atribuyen determinados comportamientos que lesionan su dignidad (por ejemplo, creando el perfil con una imagen elaborada con IA que sea lasciva, o simulando la oferta de servicios sexuales por precio). También puede aparecer en concurso con un delito contra la intimidad sí, por ejemplo, para crear el perfil falso en internet se utiliza una imagen auténtica de carácter íntimo (art. 197.1 CP)[13].

4. *La calificación típica de la elaboración y difusión del deepfake sexual*

Los casos de *deepfake* sexual o pornográfico a los que aquí me voy a referir son aquellos en los que la falsificación se elabora a partir del rostro real de una persona (por ejemplo, extraído de las redes sociales, o de imágenes audiovisuales que circulan abiertamente) y se acopla a escenas sexuales o pornográficas, logrando un resultado final de gran verosimilitud[14]. La ley de IA de la Unión Europea[15] en su art. 3.60) traduce este concepto como "ultrasuplantación", y lo define como "un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos".

De entrada, en estos casos existe una injerencia en el derecho a la imagen, porque se manipula el rostro real de una persona sin su con-

[13] El propio artículo 172 ter del código penal establece que "Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso".

[14] La directiva 2024/1385/UE, cit. dispone en su artículo 5. 1. b) que los estados deben garantizar la tipificación como delito de la conducta que consiste en "producir manipular o alterar y, posteriormente, hacer accesible al público, mediante TIC, imágenes, vídeos o materiales similares, haciendo que parezca que una persona está practicando actividades sexualmente explícitas, sin el consentimiento de dicha persona, cuando sea probable que tal conducta cause graves daños a esa persona".

[15] Reglamento (UE) 2024/1689 del Parlamento europeo y del Consejo, *por el que se establecen normas armonizadas en materia de inteligencia artificial*, de 13 de junio de 2024, en DOUE 1689, de 12 de julio de 2024.

sentimiento; lo cual no quiere decir que sea motivo suficiente para llegar a un tipo penal. Pero si la escena es construida artificialmente en su totalidad no cabe plantearse la protección del derecho fundamental recogido en el artículo 18.1 de la Constitución. Las estadísticas actuales sobre el volumen de elaboración de pornografía virtual son abrumadoras, y son numerosas las mujeres con proyección pública que se encuentran involucradas en un *deepfake* pornográfico sin su consentimiento. La elaboración de estas falsificaciones con personas famosas es relativamente fácil de realizar, teniendo en cuenta el numeroso material audiovisual que circula en los medios digitales, sin que sea necesario vencer ninguna barrera protectora para su obtención.

Como se ha argumentado más arriba, la elaboración y difusión del *deepfake* sexual no constituye un delito contra la intimidad, ya que la imagen del cuerpo en el contexto sexual o pornográfico es falsa en relación con el rostro y, por lo tanto, no comporta un atentado al aspecto moral del derecho[16]. La calificación más correcta para esta clase de hechos es el delito de injurias graves del art. 208 del código penal, ya que se produce un atentado contra el honor de la persona[17]; aunque sería necesario añadir una agravación de la pena en los casos de difusión general del *deepfake* en *internet*. Por tanto, lo que más seguridad jurídica puede proporcionar es crear un tipo específico dentro del

[16] Ahora bien, en la medida en que se manipula el rostro auténtico de una persona, sin su consentimiento, se produce una injerencia en la "facultad de disposición" sobre su propia imagen, lo cual queda dentro del ámbito de protección de la ley 1/1982. En este sentido cabe citar la sentencia del Tribunal Constitucional de 24 de febrero de 2020, n. 27/2020, declarando que es ilícita la mera reproducción sin consentimiento de la imagen de una persona (por ejemplo, una fotografía), aunque se trate de un contexto neutro, ya que solo su titular puede decidir quién puede reproducir su imagen y cuándo puede hacerse. Los hechos concretos consistieron en la publicación por parte de un periódico de la fotografía de una persona extraída de *Facebook*, sin contar con su autorización.

[17] Artículo 208 el código Penal: "Es injuria la acción o expresión que lesionan la dignidad de otra persona menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves, sin perjuicio de lo dispuesto en el apartado cuatro del artículo 173"

grupo de delitos de injurias[18]. Normalmente el *deepfake* sexual se elabora y difunde para hacer objeto de burla o escarnio de alguien, aunque en el caso de los vídeos pornográficos falsificados la finalidad también puede ser la de obtener un lucro económico. El delito de injurias exige como elemento subjetivo el *animus iniuriandi*, el cual es inherente a la conducta de quien cuelga en *internet* esta clase de imágenes conociendo que tal difusión producirá el efecto de avergonzar a la persona involucrada. Incluso si el propósito que se persigue con la elaboración de un *deepfake* pornográfico es el de obtener un beneficio comercial, ello no excluye la presencia del elemento subjetivo del delito, puesto que el autor conoce el efecto infamante que tales imágenes elaboradas sin consentimiento tienen cuando se difunden de forma general, y asume dicho resultado cuando sigue adelante con la divulgación. Aunque en el delito de injurias nos encontramos, de nuevo, ante un bien jurídico sometido a los estándares de valoración social, por una parte, y a la discrecionalidad judicial, por otra, no parece cuestionable el daño que puede producir al honor y autoestima de cualquier persona el hecho de ver identificada su imagen en un contexto pornográfico que se difunde en *internet*. En todo caso, en el código penal español el honor es un bien disponible, al requerir querella del ofendido para iniciar el procedimiento (artículo 215.1 del código penal), lo cual quiere decir que el sujeto pasivo del delito es quien debería decidir llevar adelante, o no, dicho procedimiento.

Por otro lado, hay que mencionar aquí que desde la Unión Europea se ha establecido la obligación de transparencia cuando se usa la IA para generar o manipular imágenes, con el fin de que el usuario conozca que el material que está utilizando es una ultrasuplantación. Así, el Reglamento de IA de la UE anteriormente citado establece en su art. 50 las "Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA", señalando en su párrafo 2 que: "Los proveedores de sistemas de IA, entre los que se incluyen los sistemas de IA de uso general, que generen contenido sin-

[18] Existe una proposición de ley orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de IA, presentada el 13 de octubre de 2023 por el grupo parlamentario del partido político SUMAR, proponiendo la creación de un tipo penal específico dentro de los delitos de injurias.

tético de audio, imagen, vídeo o texto, velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial...” Sin embargo, aunque sea obligatorio advertir sobre la utilización de la IA al elaborar una imagen, ello no elimina la lesión al honor que puede producirse con las ultrasuplantaciones. La imagen generada con el uso de esta técnica tiene una similitud casi exacta a la auténtica, lo que puede acabar produciendo efectos similares sobre la autoestima de la víctima si el contenido es humillante, ya que puede convertirse en objeto de burla generalizada. Así que, desde la perspectiva penal, la obligación de transparencia de los contenidos generados con IA tendrá consecuencias limitadas cuando se trata del *deepfake* sexual/pornográfico. Sin embargo, sí que puede ser útil en otro tipo de delitos en los que la suplantación de la imagen o la voz de una persona sea la forma de cometer otro comportamiento ilícito (por ejemplo, una estafa).

Además, no hay que descartar la posible aplicación de otros delitos para los casos de *deepfake* sexual, como el de lesiones psíquicas (art. 147.1 y 2 del código penal), o el de amenazas (art. 169 del código penal). La finalidad que muchas veces persigue el autor de esta clase de falsificación es avergonzar y producir angustia o temor en la víctima, la cual, al ver reconocida su imagen falsificada en un contexto sexual pornográfico, que además puede divulgarse de forma generalizada, puede sentirse humillada y ver afectada su autoestima, de tal forma que altere su comportamiento normal, busque el aislamiento social y desarrolle una alteración emocional que requiera asistencia médica, lo que permite calificar el hecho como lesiones síquicas. Este tipo de consecuencias son frecuentes en el caso de las adolescentes que sufren esta forma de agresión, ya que son más vulnerables emocionalmente. Por lo que se refiere al delito de amenazas básicas, también pueden entrar en juego cuando el autor del *deepfake* intimida a la víctima simplemente anunciándole (por ejemplo, por *mail* o *whatsapp*) que va a divulgar tales imágenes en las redes (art. 169.2 del código penal). De forma similar las amenazas pueden ser condicionales cuando se exige dinero, por ejemplo, a cambio de no divulgar la falsificación (art. 169.1 del código penal).

Actualmente se encuentra en proceso de tramitación en España

una reforma penal que prevé tipificar expresamente estas conductas dentro de los "delitos contra la integridad moral" (artículo 173 y siguientes del código penal), considerando que el *deepfake* sexual/pornográfico vulnera dicho bien jurídico[19]. Esta es la opinión sostenida por algunos autores, con el argumento de que con dicha elaboración se cosifica el cuerpo de la mujer y se la utiliza como un objeto de consumo[20]. Por mi parte, discrepo de esta calificación, ya que la generación con IA de esta clase de imágenes es algo que no encaja con el sentido político criminal de los delitos contra la integridad moral, entre los que se encuentra el delito de torturas, lo cual viene a poner de manifiesto el parámetro valorativo propio del atentado contra la integridad moral que debe protegerse; de tal forma que parece desubicado incluir aquí conductas que consisten en la creación o manipulación digital de imágenes. El injusto que subyace en el tipo básico de los delitos contra la integridad moral exige una actuación directa sobre la víctima, al describirse la conducta en el art. 173.1 del código penal de la siguiente forma: "El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de 6 meses a 2 años". La doctrina que ha estudiado este delito concreto sostiene que debe producirse una intervención sobre la esfera personal del sujeto pasivo, que puede provenir de una agresión física, o de obligar a la víctima a hacer determinadas conductas bajo amenaza de causar un mal mayor[21]. Y se añade que lo característico de este tipo penal es causar padecimientos físicos, síquicos o morales a una persona, que es tratada al margen de toda consideración y respeto, y que es instrumentalizada en manos de un sujeto que abusa

[19] La propuesta del nuevo tipo penal se inserta en el anteproyecto de ley orgánica para la protección de las personas menores de edad en los entornos digitales, y está en fase de tramitación cuando esto se escribe.

[20] A. DEVÍS MATAMOROS, *Algunas claves del castigo penal del deepfake de naturaleza sexual,* en *Revista Pensamiento Penal*, 2023, https://www.ibericonnect.blog/2023/07/algunas-claves-del-castigo-penal-del-deepfake-de-naturaleza-sexual/

[21] J.M. TAMARIT SUMALLA, *De las torturas y otros delitos contra la integridad moral,* en G. QUINTERO OLIVARES (a cura di) *Comentarios al nuevo código penal*, Navarra, 2005, p. 930.

de la superioridad que ostenta[22]. Es decir, se produce el sometimiento de una persona a los dictados de otra, que es colocada en una situación de sumisión, dependencia y envilecimiento, logrando un dominio fáctico sobre ella[23].

Teniendo en cuenta tales parámetros interpretativos del tipo básico de los delitos contra la integridad moral y, teniendo en cuenta, también, que en el mismo Título VII se encuentra el delito de torturas ("De las torturas y otros delitos contra la integridad moral"), además de otros tipos penales que comportan una actuación personal sobre la víctima, la ubicación del *deepfake* sexual en este contexto no es la más adecuada. La única manipulación que se lleva a cabo en estos casos se produce sobre una imagen digital, que ni siquiera se corresponde con la verdadera; no existiendo contacto entre autor y sujeto pasivo. Para evitar los inconvenientes que se acaban de citar al incluir el *deepfake* sexual en las conductas básicas del delito contra la integridad moral, la propuesta de reforma legal contempla introducir un nuevo apartado, el art. 173 bis, con el siguiente tenor: "Se impondrá la pena de prisión de uno a dos años a quienes, sin autorización de la persona afectada *y con ánimo de menoscabar su integridad moral*, difundan, exhiban o cedan su imagen corporal o audio de voz generada, modificada o recreada mediante sistemas automatizados, software, algoritmos, IA o cualquier otra tecnología, de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorias" [24]. Sin embargo, esta redacción tiene el grave inconveniente de exigir el dolo directo de actuar con "ánimo de menoscabar la integridad moral" de la víctima, lo cual impedirá incluir en el precepto modalidades, como el *deepfake* pornográfico, que se elaboran persiguiendo un beneficio comercial, y no con la finalidad concreta de producir un daño a dicha integridad.

[22] N.J. DE LA MATA BARRANCO, A.I. PÉREZ MACHÍO, *El concepto de trato degradante en el delito contra la integridad moral del art. 173.1 del código penal,* en *Revista Penal,* 2005, n. 15, p. 42.

[23] J. BARQUÍN SANZ, *Delitos contra la integridad moral,* Barcelona, 2001, p. 68 y ss.; N. DE LA MATA, A. I. PÉREZ, cit., 2005, p 32.

[24] Y sigue en el párrafo segundo: "Se aplicará la pena en su mitad superior si dicho material ultrafalsificado se difunde a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías, de modo que aquel se hiciera accesible a un elevado número de personas en el espacio virtual."

En el delito de injurias el *animus iniuriandi* es menos exigente, y es fácilmente adherible a este tipo de conductas, al asumirse el descrédito que la venta del material pornográfico tiene en el honor del titular de la imagen. Sin embargo, el dolo específico de "atentar contra la integridad moral" va más allá del *animus iniuriandi*, y tiene una intensidad que debe acompasarse con la entidad del bien jurídico que se protege en ese grupo de delitos contra la integridad moral. Por tanto, con una interpretación escrupulosa deberá excluirse del precepto que se propone el castigo al *deepfake* sexual/pornográfico que se hace por mero divertimento, en desarrollo de la libertad de expresión o sólo con ánimo comercial, al carecer todas estas conductas del mencionado dolo específico de dañar el bien jurídico de la integridad moral. Una vez más, el afán del legislador por *visualizar* la agravación de determinadas conductas puede acabar produciendo el efecto contrario, ya que deberá acudirse al delito de injurias cuando la conducta del autor del *deepfake* sexual no persiga de forma directa dañar la integridad moral de la víctima.

Abstract

La protección de la imagen íntima se encuentra tipificada en varios preceptos del código penal español, siendo objeto de análisis en este trabajo las conductas típicas que tienen mayor incidencia jurisprudencial. Para comprobar que existe una lesión de este bien jurídico previamente debe definirse el concepto de imagen íntima en el contexto actual, ya que la irrupción de la Inteligencia Artificial en este campo abre un panorama que multiplica las posibilidades de lesión. Con el fin de calificar adecuadamente los casos de elaboración y difusión del *deepfake* sexual o pornográfico hay que tener en cuenta que el derecho a la imagen íntima, que deriva del más amplio derecho a la imagen que recoge el artículo 18.1 de la Constitución española, es un derecho personalísimo que solo puede esgrimirse en los casos en los que se representa la verdad, es decir, cuando se capta o se reproduce la figura real y auténtica de una persona en un contexto de intimidad.

PALABRAS CLAVE: Imagen íntima – delitos contra la intimidad – *deepfake* sexual – delito de injurias – acoso digital

LA TUTELA PENALE DEL DIRITTO ALL'IMMAGINE INTIMA. RIFERIMENTO SPECIALE AI CASI DI *DEEPFAKE* SESSUALE

La tutela dell'immagine intima è esemplificata in diversi precetti del codice penale spagnolo, e i comportamenti tipici che hanno il maggiore impatto giurisprudenziale sono oggetto di analisi in questo lavoro. Per verificare che sussista una lesione di questo diritto giuridico, è necessario innanzitutto definire il concetto di immagine intima nel contesto attuale, poiché l'emergere dell'Intelligenza Artificiale in questo campo apre un panorama che moltiplica le possibilità di lesione. Per qualificare adeguatamente i casi di creazione e diffusione di *deepfake* a sfondo sessuale o pornografico, occorre tenere conto che il diritto all'immagine intima, che deriva dal più ampio diritto all'immagine contenuto nell'articolo 18.1 della Costituzione spagnola, è un diritto personalissimo che può essere fatto valere solo nei casi in cui viene rappresentata la verità, quando cioè la figura reale e autentica di una persona viene catturata o riprodotta in un contesto di intimità.

KEYWORDS: Immagine intima – crimini contro l'intimità – *deepfake* sessuale – reato di ingiuria – molestie online

MEDIDAS CAUTELARES NACIONALES Y TRANSNACIONALES DE INTERÉS PARA LA PROTECCIÓN DE VÍCTIMAS DE CIBERVIOLENCIA DE GÉNERO

Juan Carlos Vegas Aguilar[*]

SUMARIO: 1. Estado de la cuestión. – 2. La evolución en la protección de la víctima como finalidad del proceso penal. – 2.1. Ley orgánica 14/1999, *de modificación del Código Penal de 1995, en materia de protección a las víctimas de malos tratos y de la ley de enjuiciamiento criminal*, de 9 de junio de 1999. – 2.2. Ley 27/2003, *reguladora de la orden de protección*, de 31 de julio de 2023. – 2.3. Ley 4/2015, *del estatuto de la víctima del delito*, de 27 de abril de 2015. – 2.4. Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, de 24 de mayo de 2024. – 3. Orden de alejamiento y orden de protección. – 4. La protección de las víctimas en la ley 4/205, *del estatuto de la víctima del delito*, del 27 de abril de 2015. – 5. La orden europea de protección.

1. *Estado de la cuestión*

En el Informe de la Cuarta Conferencia Mundial sobre la Mujer, celebrado en Beijing del 4 al 15 de septiembre de 1995[1] –fechado en la sede de Naciones Unidas en 1996– se establece que "La violencia contra la mujer es una manifestación de las relaciones de poder históricamente desiguales entre mujeres y hombres, que han conducido a la dominación de la mujer por el hombre, la discriminación contra la mujer y a la interposición de obstáculos contra su pleno desarrollo. La violencia contra la mujer a lo largo de su ciclo vital dimana esencialmente de pautas culturales, en particular de los efectos perjudiciales de algunas prácticas tradicionales o consuetudinarias y de todos los ac-

[*] Profesor de Derecho y Criminología - Universidad Católica de Valencia, San Vicente Mártir. Email: jc.vegas@ucv.es.

[1] Beijing Declaration of the Fourth World Conference on Women, *Report of the 4th World Conference on Women*, A/CONF.177/20/Rev.1, 4-15 September 1995.

tos de extremismo relacionados con la raza, el sexo, el idioma o la religión que perpetúan la condición inferior que se asigna a la mujer en la familia, el lugar de trabajo, la comunidad y la sociedad".

Además, continúa el mencionado Informe "La violencia contra la mujer se ve agravada por presiones sociales, como la vergüenza de denunciar ciertos actos; la falta de acceso de la mujer a información, asistencia letrada o protección jurídica; la falta de leyes que prohíban efectivamente la violencia contra la mujer; el hecho de que no se reformen las leyes vigentes; el hecho de que las autoridades públicas no pongan el suficiente empeño en difundir y hacer cumplir las leyes vigentes; y la falta de medios educacionales y de otro tipo para combatir las causas y consecuencias de la violencia. Las imágenes de violencia contra la mujer que aparecen en los medios de difusión, en particular las representaciones de la violación o la esclavitud sexual, así como la utilización de mujeres y niñas como objetos sexuales, y la pornografía, son factores que contribuyen a que se perpetúe esa violencia, que perjudica a la comunidad en general, y en particular a los niños y los jóvenes".

De manera conjunta, el Informe señala que cuando se hace referencia a la "violencia contra la mujer" se hace alusión "a todo acto de violencia basado en el género que tiene como resultado posible o real un daño físico, sexual o psicológico, incluidas las amenazas, la coerción o la privación arbitraria de la libertad, ya sea que ocurra en la vida pública o en la privada".

De este modo, la violencia contra la mujer "puede tener, entre otras, las siguientes formas: a) La violencia física, sexual y psicológica en la familia, incluidos los golpes, el abuso sexual de las niñas en el hogar, la violencia relacionada con la dote, la violación por el marido, la mutilación genital y otras prácticas tradicionales que atentan contra la mujer, la violencia ejercida por personas distintas del marido y la violencia relacionada con la explotación; b) La violencia física, sexual y psicológica al nivel de la comunidad en general, incluidas las violaciones, los abusos sexuales, el hostigamiento y la intimidación sexuales en el trabajo, en instituciones educacionales y en otros ámbitos, la trata de mujeres y la prostitución forzada; c) La violencia física, sexual y psicológica perpetrada o tolerada por el Estado, dondequiera que ocurra".

Por consiguiente, nos encontramos ante una lacra que se fundamenta en la desigualdad entre géneros y en la intención de perpetuar

dicha desigualdad por cualquier medio, llegando, en último extremo, a causar la muerte de la mujer.

La propia directiva sobre violencia contra las mujeres y violencia doméstica[2], prescribe que la violencia contra las mujeres supone "una violación de los derechos fundamentales".

En nuestro ordenamiento jurídico, el concepto normativo sobre violencia de género a nivel del derecho penal[3] es el recogido en la ley orgánica 1/2004 (en adelante, LOVG)[4]. El artículo primero de dicha norma conceptúa esta violencia como aquella "que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia".

De este modo, nos encontramos ante una serie de delitos –los relacionados con la violencia de género– que tienen un gran componente psicológico fruto de la sociedad patriarcal que se ha ido fraguando a lo largo de la historia y que ha intentado subyugar a la mujer de cualquier manera posible. Así, siguiendo a Añón Roig y Mestre i Mestre "La violencia de género tiene causas socioculturales profundas derivadas de la asignación de roles en el proceso de socialización del que surgen desigualdades arraigadas y perdurables que permiten com-

[2] Directiva 2024/1385/UE del Parlamento europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, de 14 de mayo de 2024, en DOUE 1385 de 24 de mayo de 2024, pp. 1-36.

[3] Decimos que este concepto se aplica a efectos penales porque a efectos de protección y asistenciales un gran número de Comunidades Autónomas, en el ejercicio de sus competencias, ha asumido un concepto amplio de Violencia de Género. A título de ejemplo, la ley valenciana preceptúa la violencia sobre la mujer como "todo comportamiento de acción u omisión por el que un hombre inflige a la mujer daños físicos, sexuales, psicológicos y/o económicos basados en la pertenencia de esta al sexo femenino, como resultado de la situación de desigualdad y de las relaciones de poder de los hombres sobre las mujeres; así como las amenazas de tales actos, la coacción o la privación arbitraria de libertad, tanto si se producen en la vida pública como en la privada" (ley 7/2012, *integral contra la violencia sobre la mujer en el ámbito de la Comunitat Valenciana*, de 23 de noviembre de 2012).

[4] Ley orgánica 1/2004, *de Medidas de Protección Integral contra la Violencia de Género*, de 29 de diciembre de 2004.

prender por qué ha sido tolerada la violencia de género y por qué persiste"[5].

Estas raíces socioculturales, hacen que esta violencia se lleve a cabo a través de cualquier medio y, por supuesto, el uso de la tecnología no va a ser ajeno a este género delictivo. Como señala jordán díaz-roncero, en esta misma obra, la "irrupción en nuestras vidas de dichas tecnologías, que forman parte de nuestro quehacer diario y que, sin duda, una gran parte de la población no puede concebir su vida personal y laboral sin ellas, está propiciando la aparición de conductas relacionadas con la violencia de género".

De este modo, la ampliación del abanico de herramientas que propician el ataque sobre la mujer por el hecho de serlo hace más necesario, si cabe, una efectiva protección de la víctima una vez que se inicia el proceso penal. No es ninguna novedad afirmar que la víctima ha sido tradicionalmente la gran olvidad del proceso penal. Si bien esta situación se ha ido modificando paulatinamente, sobre todo a partir del surgimiento de la *victimología*[6], movimiento que ha influido en

[5] M. J. AÑÓN ROIG, R. MESTRE I MESTRE, *Violencia sobre las mujeres: discriminación, subordinación y Derecho*, en J. BOIX REIG, E. MARTÍNEZ GARCÍA (a cura di), *La Nueva Ley Contra la Violencia de Género (LO 1/2004, de 28 de diciembre)*, Madrid, 2005, p. 36. En este sentido C. VILLACAMPA ESTIARTE, afirma que "la violencia contra la mujer se tilda de violencia de género porque constituye un ejemplo de violencia cultural, no sexista" en C. VILLACAMPA ESTIARTE, *La violencia de género: aproximación fenomenológica, conceptual y a los modelos de abordaje normativo*, en C. VILLACAMPA ESTIARTE (a cura di), *Violencia de género y sistema de justicia penal*, Valencia, 2008, p. 31.

[6] TAMARIT SUMALLA la define como una "ciencia multidisciplinar que se ocupa del conocimiento relativo a los procesos de victimización y desvictimización. Concierne pues a la victimología el estudio del modo en que una persona deviene víctima, de las diversas dimensiones de la victimización (primaria, secundaria y terciaria), y de las estrategias de prevención y reducción de la misma, así como del conjunto de respuestas sociales, jurídicas y asistenciales, tendentes a la reparación y reintegración social de la víctima". Esta ciencia surge a mediados del siglo XX como respuesta a los horrores del holocausto judío en la Segunda Guerra Mundial. La doctrina atribuye la paternidad de esta ciencia a HANS VON HENTIG (El criminal y su víctima, 1948) y BENJAMIN MENDELSOHN (La doctrina destaca su conferencia en el hospital Coltzea de Bucarest (1947), en la que estuvieron presentes profesionales de diferentes disciplinas científicas como psiquiatras, psicoanalistas, médicos forenses, juristas, criminólogos, etc., lo que resultó ser una espléndida plataforma de difusión de esta nueva disciplina y un

gran medida en la configuración de la idea sobre la protección a la víctima de una forma general. Asimismo, dicha protección se ha ido incluyendo progresivamente en el proceso penal.

De este modo, comienza a surgir la idea de que las víctimas constituyen uno de los *referentes vertebrales* del sistema jurídico penal[7], llegando a hablarse de un *principio de protección a las víctimas*, entendido como aquel que pretende "garantizar la máxima tutela jurídica de los derechos de las víctimas en el orden penal sin desnaturalizar, con ello, los principios que adecuan el derecho penal a las exigencias de un Estado social y democrático de derecho ni vaciar las notas jurídicas que permiten concebir a un juicio como un proceso justo e idóneo para obtener una tutela efectiva de los derechos e intereses legítimos", el

preludio de su multidisciplinariedad). Entre otros ver E. BACA BALDOMERO, E. ECHEBURÚA ODRIOZOLA, J. M. TAMARIT SUMALLA (a cura di), *Manual de Victimología,* Valencia, 2006; G. LANDROVE DÍAZ, *Victimología*, Valencia, 1990; I. J. SUBIJANA ZUNZUNEGUI, *El Principio de Protección de las Víctimas en el Orden Jurídico Penal: del Olvido al Reconocimiento*, Granada, 2006; S. SEMPERE FAUS, *La participación activa de la víctima en el proceso penal: análisis del art. 11 del Estatuto de la Víctima* en *La ley penal: revista de derecho penal, procesal y penitenciario*, 2019, n. 136.

[7] Que uno de los principios informadores del derecho penal sea el de protección a las víctimas, no ha tenido una acogida uniforme en la doctrina, pudiéndose distinguir tres posicionamientos al respecto. El primero defiende el principio de neutralización de las víctimas, ya que considera el delito como una lesión del bien jurídico protegido por el Estado y el proceso se concibe como una disputa entre el Estado y el acusado, sin que haya un espacio reservado a la víctima, la cual tiene únicamente función de testigo, sin un estatuto jurídico definido. La segunda corriente entiende el delito como una realidad humana que despliega sus efectos entre la víctima, el victimario y las víctimas potenciales, confiriéndole, al comportamiento antijurídico, una dimensión social. Así defienden que el interés del derecho penal se ha de centrar en la lesión a la sociedad. Y una tercera corriente que entiende que ha de ser la víctima "la piedra angular del sistema jurídico penal", debiendo de articularse un estatuto jurídico propio, sacándola de la categoría de testigo y poniéndola en un lugar preferente en el proceso penal, en I. J. SUBIJANA ZUNZUNEGUI, cit., pp. 2-4. En este sentido GÓMEZ COLOMER afirma que "También la protección de la víctima es otro de los fines del proceso penal en su visión más moderna". Así, continúa este autor "el proceso debe prever los mecanismos suficientes para que la víctima de un delito sea restituida, reparada e indemnizada de manera justa y proporcionada al perjuicio personal, físico y moral, sufrido", en J. F. ETXEBARRÍA GURIDI, S. BARONA VILAR, A. PLANCHADELL GARGALLO, E. MARTINEZ GARCIA, I. ESPARZA LEIBAR, J. L. GÓMEZ COLOMER, *Procesal Penal. Derecho Procesal III*, 4ª Edición, Valencia, 2024, pp. 37-38.

cual se encuentra presente en el diseño del *injusto típico*, en la *sanción penal* y en el *proceso debido*[8]. Veamos cómo nuestro ordenamiento jurídico ha ido evolucionando en este sentido.

2. *La evolución en la protección de la víctima como finalidad del proceso penal*

Como se ha dicho anteriormente, una finalidad del proceso penal debe ser la efectiva protección de la víctima durante la sustanciación del mismo. Para ello, tanto el órgano instructor como el órgano encargado del enjuiciamiento pueden adoptar medidas encaminadas a lograr dicho objetivo de protección.

Antes de tratar las medidas de protección que se pueden adoptar a lo largo del proceso penal debemos hacer una puntualización al respecto. El legislador trata estas medidas como medidas cautelares, a pesar de que la finalidad de unas y otras son distintas y, por ende, su naturaleza jurídica es diferente[9]. En este sentido, Cortés Domínguez señala que "las medidas cautelares y las medidas de protección persiguen finalidades diferentes, aunque ambas se adopten en el curso del proceso; las dos suponen limitaciones o prohibiciones al ejercicio de los derechos, de modo que los requisitos para su adopción, entre otros la resolución judicial motivada, deben ser idénticos; ambas se dirigen contra el investigado (cuando se trate de medidas cautelares reales también contra los posibles responsables ci-

[8] I. J. SUBIJANA ZUNZUNEGUI, cit., pp. 23-24.

[9] La equiparación de ambas medidas —cautelares y de protección— conllevan en la práctica algunos problemas que, aunque exceden del objeto de este trabajo, queremos apuntar. El artículo 58 del Código penal prevé el abono de las medidas cautelares a la pena impuesta, con lo que si se aplica una medida de prohibición de aproximarse a la víctima —muy común en los procesos por violencia de género— y posteriormente se impone una pena de prohibición de aproximarse a la víctima —pena cuya aplicación es obligatoria para este tipo de delitos en virtud del artículo 57.2 del CP—, se dará el caso de que deba abonarse y, por consiguiente, no se cumpla dicha pena de prohibición de aproximarse a la víctima. A nuestro parecer, esta situación no se daría si se tuviera en considera la diferente naturaleza jurídica —cautelar y de protección— de ambas medidas, ya que según el CP solo se abonan las medidas cautelares. A título de ejemplo podemos ver la sentencia del juzgado de lo penal de Vitoria-Gasteiz, de 5 de febrero de 2018, n. 50/2018.

viles), y su contenido puede ser el mismo. Sin embargo, por más que incluso vengan reguladas en el mismo precepto, como sucede con la prisión provisional como medida cautelar y la prisión ordenada como protección de la víctima (art. 503 LECrim), se trata de dos realidades distintas no sólo conceptualmente, sino en razón de los presupuestos exigibles en uno y otro caso[10].

En un sentido parecido se pronuncia Barona Vilar al afirmar sobre las medidas preventivas que "La naturaleza no cautelar de éstas se evidencia por la finalidad de prevención a la que se dirigen, ya porque se pretende prevenir la comisión o reiteración de delitos o ya porque se pretende asegurar el control social, la seguridad ciudadana. No son instrumentales del proceso, sino que se sirven del proceso. Han proliferado en los últimos años y se les ha venido vinculando a la tutela cautelar, aunque no sean cautelares"[11].

Dicho esto, y centrándonos en las medidas de protección a las víctimas de violencia de género, en el ordenamiento jurídico español podemos encontrar un gran número de normas encaminadas a la protección de las víctimas en general y de las víctimas de violencia de género en particular.

2.1. *Ley orgánica 14/1999, de modificación del Código Penal de 1995, en materia de protección a las víctimas de malos tratos y de la ley de enjuiciamiento criminal, de 9 de junio de 1999*

Así, en primer lugar, hallamos la ley orgánica 14/1999[12]. Esta norma se dictó con el objetivo de "otorgar una mayor y mejor protec-

[10] V. MORENO CATENA, V. CORTÉS DOMÍNGUEZ, *Derecho Procesal Penal*, 12ª Edición, Valencia, 2024, p. 333.

[11] J. F. ETXEBARRÍA GURIDI, S. BARONA VILAR, A. PLANCHADELL GARGALLO, E. MARTINEZ GARCIA, I. ESPARZA LEIBAR, J. L. GÓMEZ COLOMER, cit., p. 305.

[12] Ley orgánica 14/1999, *de modificación del código penal de 1995, en materia de protección a las víctimas de malos tratos y de la ley de enjuiciamiento criminal*, de 9 de junio de 1999. Para ver la evolución legislativa sobre esta materia ver, entre otros, R. CAMPOS CRISTÓBAL, *Tratamiento penal de la violencia de género*, en J. BOIX REIG, E. MARTÍNEZ GARCÍA (a cura di), *La Nueva Ley Contra la Violencia de Género (LO 1/2004, de 28 de diciembre)*, Madrid, 2005, pp. 256-266; C. ARAGÜEÑA FANEGO, *La reforma de la Ley de Enjuiciamiento Criminal por Ley Orgánica 14/1999, de 9 de junio, en materia de malos tratos; especial referencia a las nuevas medidas cautelares del art. 344 bis* en *Actualidad penal*, 2000, n. 11.

ción a las víctimas" a las víctimas de malos tratos. Para ello se adoptaron una serie de reformas del Código penal, entre las que resaltar la inclusión, como pena accesoria de determinados delitos, de la prohibición de aproximación a la víctima, o la tipificación como delito específico de violencia psíquica ejercida con carácter habitual sobre las personas próximas.

Asimismo, se modificó la ley de enjuiciamiento criminal (LECrim)[13] con el objetivo de facilitar la inmediata protección de la víctima de malos tratos[14]. De este modo, se modificaron las diligencias de prevención que debían realizar las Fuerzas y Cuerpos de Seguridad al llegar al lugar de los hechos en el sentido de que se les permitía adoptar aquellas medidas encaminadas a "proteger a los ofendidos o perjudicados por el mismo, a sus familiares o a otras personas pudiendo acordarse a tal efecto las medidas cautelares a las que se refiere el artículo 544 bis" de la LECrim.

Conjuntamente se modificó el artículo 109 en el sentido de obligar al juez, que conociera de algún proceso por delitos graves[15], a asegurar la comunicación a la víctima de los actos procesales que puedan afectar a su seguridad. Con ello se pretendía avisar a la víctima de estos delitos de posibles situaciones, derivadas de decisiones procesales, que pudieran afectar a su seguridad.

Además, y como reforma de mayor calado, se introdujo en la LECrim el artículo 544 *bis* que otorgaba al juez la posibilidad de adoptar medidas tales como la prohibición de residir en un determinado lugar, barrio, municipio, provincia u otra entidad local, o Comunidad Autónoma; o la prohibición de acudir a determinados lugares, barrios, mu-

[13] Real decreto *por el que se aprueba la Ley de Enjuiciamiento Criminal,* de 14 de septiembre de 1882.

[14] En esta norma no se habla de violencia de género porque este concepto se introdujo en el ordenamiento jurídico español en virtud de la LOVG. Si bien es cierto que la ley 27 /2003, de 31 de julio, *reguladora de la orden de protección* ya hacía mención a la violencia de género en su exposición de motivos.

[15] Estos delitos eran lo establecidos en el artículo 57 del CP, a saber: delitos de homicidio, aborto, lesiones, contra la libertad, de torturas y contra la integridad moral, la libertad e indemnidad sexuales, la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el honor, el patrimonio y el orden socioeconómico.

nicipios, provincias u otras entidades locales, o Comunidades Autónomas, o de aproximarse o comunicarse a determinadas personas.

Ante la insuficiente protección de estas medidas se volvieron a adoptar otras en virtud de la ley 27 /2003[16], la cual añadió el artículo 544 *ter* a la LECrim regulando la denominada orden de protección.

2.2. *Ley 27/2003, reguladora de la orden de protección, de 31 de julio de 2023*

La orden de protección otorga a la víctima un estatuto integral de protección, el cual comprende una serie de medidas penales, civiles, asistenciales, de protección social, etc. La orden se inscribe en el Registro Central para la protección de las Víctimas de la Violencia de Doméstica, suponiendo el deber de mantener informada a la víctima de la situación procesal y, en su caso, penitenciaria del agresor[17].

La última reforma que afecta a la orden de protección se produjo en virtud de la ley orgánica 8/2021[18]. Dicha modificación afectó a los apartados 6 y 7 del artículo 544 *ter* en el sentido de proteger a las personas sometidas a la patria potestad, tutela, curatela, guarda o acogimiento de la víctima. Además, en el supuesto de que al dictarse una orden de protección, con medidas de contenido penal, y existieran indicios fundados de que los hijos e hijas menores de edad hubieran presenciado, sufrido o convivido con la comisión de un delito contra la vida, integridad física o moral, libertad sexual, libertad o seguridad, la

[16] Ley 27/2003, *reguladora de la Orden de protección de las víctimas de la violencia doméstica*, de 31 de julio de 2003.

[17] Sobre la orden de protección es de interés, sin ánimo de exhaustividad, C. MOSQUERA ORDOÑEZ, *Medidas civiles de la orden de protección* en J. C. VEGAS AGUILAR, S. SEMPERE FAUS (a cura di), *La protección de las víctimas en el espacio europeo*, Valencia, 2023, pp. 239-278; M. J. JORDÁN DÍAZ-RONCERO, *El papel del letrado o la letrada en la aplicación de las órdenes de protección* en J. C. VEGAS AGUILAR, S. SEMPERE FAUS, (a cura di), cit. pp. 47-74; C. POLLOS CALVO, *Orden de protección, prohibición de aproximación/comunicación y el Tribunal Supremo sobre redes sociales* en *Diario La Ley*, 2022, n. 10106; A. ARROYO BLANCO, *La orden de protección*, Tesis Doctoral dirigida por Teresa San Segundo Manuel, UNED: Universidad Nacional de Educación a Distancia, 2022.

[18] Ley orgánica 8/2021, *de protección integral a la infancia y la adolescencia frente a la violencia*, de 4 de junio de 2021.

autoridad judicial, de oficio o a instancia de parte, se suspenderá el régimen de visitas, estancia, relación o comunicación del inculpado respecto de los menores que dependan de él.

Por consiguiente, se establece como regla general la suspensión de una serie de derechos, propios de las relaciones paterno-filiales, en el caso de que los menores sufran o hayan presenciado algún acto de violencia de género o familiar. Esta suspensión quedará sin efecto si se solicita a instancia de parte y, además, la autoridad judicial observa motivos suficientes para ello siempre en interés superior del menor y previa evaluación de la situación de la relación paternofilial.

Tras la ley 27 /2003 se promulgó la LOVG. Esta ley orgánica representó –y representa en la actualidad– "un paso adelante en materia de violencia por razón de género y un cambio de mentalidad al intentar el legislador conceptuar estas agresiones como actos fruto de la violencia que se ejerce contra un género (…). El valor indiscutible de esta ley es la llamada de atención que realiza sobre la propia naturaleza y complejidad del conflicto, afrontando su lucha desde una perspectiva transdisciplinar"[19]. La LOVG dedica su Capítulo IV a regular una serie de medidas de judiciales de protección y de seguridad de las víctimas, las cuales serán expuestas *infra*.

Otra norma de interés en la protección de las víctimas en general y de las de violencia de género en particular es la ley 4/2015, del estatuto de la víctima del delito, de 27 de abril de 2015.

2.3. *Ley 4/2015, del estatuto de la víctima del delito, de 27 de abril de 2015*

Esta norma dedica su Título III a establecer medidas de protección de las víctimas, sobre las que volveremos en el apartado siguiente. Íntimamente relacionada con esta norma podemos hallar la ley orgánica 10/2022[20]. Esta ley orgánica tiene como finalidad la adopción y puesta en práctica de políticas efectivas, globales y coordinadas entre

[19] E. MARTÍNEZ GARCÍA, *La tutela judicial de la violencia de género*, Madrid, 2008, pp. 23-24.

[20] Ley orgánica 10/2022, *de garantía integral de la libertad sexual*, de 6 de septiembre de 2022.

las distintas administraciones públicas competentes, a nivel estatal y autonómico, que garanticen la sensibilización, prevención, detección y la sanción de las violencias sexuales, e incluyan todas las medidas de *protección integral* pertinentes que garanticen la respuesta integral especializada frente a todas las formas de violencia sexual, la atención integral inmediata y recuperación en todos los ámbitos en los que se desarrolla la vida de las mujeres, niñas, niños y adolescentes, en tanto víctimas principales de todas las formas de violencia sexual.

Así, en la norma es posible hallar una gran variedad de medidas encaminadas a proteger a este tipo víctimas de violencia sexual, entre las que podemos destacar, por estar íntimamente ligadas al objeto de esta publicación, las previstas en los artículos 45 y 46.

El artículo 45 establece disposiciones para la protección efectiva de las víctimas en riesgo, dirigidas a las Fuerzas y Cuerpos de Seguridad y las policías autonómicas y locales competentes, las cuales deberán desplegar sistemas de evaluación del riesgo y de protección orientados a garantizar la no repetición de la violencia y a brindar protección efectiva ante represalias o amenazas. Estas medidas se podrán mantener, si se valora su necesidad, en los casos de sobreseimiento provisional, siempre respetando el derecho a la intimidad de las víctimas.

Asimismo, en el mismo sentido, a través de las unidades especializadas se deberá vigilar y controlar el cumplimiento exacto de las medidas acordadas por los órganos judiciales, encaminadas a la protección de la víctima, a través de la vigilancia de los investigados o condenados o el control de localización, a través de dispositivos telemáticos de control del cumplimiento de penas y medidas de seguridad de alejamiento, cuando su utilización sea acordada mediante resolución judicial.

El artículo 282 de la LECrim establece, en este sentido, que cuando las víctimas entren en contacto con la Policía Judicial, esta llevará a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal.

Por su parte, el artículo 46 prevé la adopción de acuerdos, entre el Gobierno con las comunidades autónomas y las Entidades Locales,

para promover la formación y la colaboración de las policías autonómicas y locales, con la finalidad de mejorar la respuesta policial frente a las distintas formas de violencia sexual, especialmente en lo relativo a la primera atención y a la protección de víctimas en situación de riesgo. Para ello, revisará y actualizará los acuerdos y protocolos en materia de colaboración entre los diferentes Cuerpos y Fuerzas de Seguridad.

Como última norma a destacar debemos analizar la citada directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, de 24 de mayo de 2024[21].

2.4. *Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*

El artículo primero de esta norma establece normas mínimas relativas a, entre otros aspectos, "la protección y el apoyo a las víctimas, la prevención y la intervención temprana".

Así, los artículos 14 al 24 prevén una serie de medidas interesantes de protección de las víctimas y acceso a la justicia, entre las que podemos destacar las siguientes:

- Posibilidad de denunciar actos de violencia contra las mujeres o de violencia doméstica a las autoridades competentes a través de canales accesibles, fáciles de usar, seguros y con disponibilidad inmediata.
- Derecho de denunciar en línea o a través de otras TIC accesibles y seguras, al menos en lo que respecta a los ciberdelitos, sin perjuicio de las normas procesales nacionales relativas a la formalización de denuncias en línea[22].

[21] Esta directiva recoge un elenco de ciberdelitos de violencia contra las mujeres o de violencia doméstica (Arts. 5-8).

[22] Este derecho puede chocar frontalmente con lo dispuesto en la reciente ley orgánica 1/2025, *de medidas en materia de eficiencia del Servicio Público de Justicia*, de 2 de enero de 2015, la cual modifica el artículo 266 de la LECrim prohibiendo la denuncia telemática de aquellos hechos que se hayan producido con violencia o intimidación, ni si tienen autor conocido, ni si existen testigos, ni si el denunciante es menor

- A que la opción de denunciar en línea o a través de otras TIC accesibles y seguras incluya la posibilidad de aportar pruebas.
- Derecho al acceso a asistencia jurídica gratuita de conformidad con el artículo 13 de la directiva 2012/29/UE.
- Cuando sean menores quienes denuncien actos de violencia contra las mujeres o de violencia doméstica, los Estados miembros se asegurarán de que los procedimientos de denuncia sean seguros y confidenciales y estén concebidos de manera accesible y adecuada para los menores, en un lenguaje accesible y adecuado para ellos, en función de su edad y su madurez.
- Derecho a una evaluación individual en la fase más temprana posible del proceso, con el fin de determinar sus necesidades especiales de protección.

Asimismo, como medidas de protección la directiva permite la adopción de órdenes urgentes de alejamiento, de prohibición o de protección. Así, el artículo 19 prevé que en aquellas situaciones de peligro inmediato para la salud o la seguridad de la víctima o de las personas a cargo, las autoridades competentes dispongan de la facultad de dictar, sin demora indebida, órdenes dirigidas al autor o sospechoso de un acto de violencia, de los recogidos en la propia directiva, para que abandone el domicilio de la víctima o de las personas a cargo durante un período de tiempo suficiente y para prohibir que el autor o sospechoso entre en el domicilio, o se acerque a una distancia de dicho domicilio inferior a la ordenada, o entre en el lugar de trabajo de la víctima o se comunique en modo alguno con ella o con las personas a cargo. Estas órdenes tendrán efecto inmediato y no dependerán de que la víctima denuncie el delito.

De manera conjunta, la directiva señala que se establece un derecho de información de la víctima sobre la existencia de la posibilidad de solicitar tales órdenes, así como de pedir el reconocimiento transfronterizo de las órdenes de protección de conformidad con la directiva *sobre la orden europea de protección*[23] o con el reglamento *relativo*

de edad, ni si se ha cometido delito flagrante, ni aquellos hechos de naturaleza violenta o sexual.

[23] Directiva 2011/99/UE del Parlamento europeo y del Consejo, *sobre la orden europea de protección*, de 13 de diciembre 2011, en DOUE de 21 de diciembre de 2011.

al reconocimiento mutuo de medidas de protección en materia civil[24].

El incumplimiento de estas órdenes debe conllevar sanciones de naturaleza penal o no, efectivas, proporcionadas y disuasorias. Además, los Estados miembros garantizarán que se ofrezca a las víctimas la oportunidad de ser notificadas, sin demora indebida, del incumplimiento de una orden urgente de alejamiento, de prohibición o de protección que pueda afectar a su seguridad.

Por último, señalar que el artículo 23 regula medidas para eliminar material en línea tal como imágenes, vídeos o similares que representen actividades sexualmente explícitas o las partes íntimas de una persona sin su consentimiento, cuando sea probable que tal conducta cause graves daños a esa persona; así como ese mismo tipo de imágenes que, sin ser de la propia víctima, hagan parecer que una persona está practicando actividades sexualmente explícitas, sin el consentimiento de dicha persona, cuando sea probable que tal conducta cause graves daños a esa persona[25]. También se prevé la eliminación de material en línea que sirva para cometer delitos de ciberacoso o Incitación a la violencia o al odio por medios cibernéticos[26].

Una vez examinada la evolución de las medidas de protección a la víctima dentro del proceso penal, como cumplimiento del principio de protección a la víctima, vamos a examinar algunas de esas concretas medidas de protección.

[24] Reglamento (UE) nº 606/2013 del Parlamento Europeo y del Consejo, *relativo al reconocimiento mutuo de medidas de protección en materia civil*, de 12 de junio de 2023, en DOUE 181, de 29 de junio de 2013.

[25] A nadie se nos escapa que los nuevos programas basados en Inteligencia Artificial se generan todo tipo de imágenes que pueden atentar contra la libertad sexual o la propia imagen de la víctima.

[26] El plazo para que los Estados miembros pongan en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en esta directiva se ha fijado como límite el 14 de junio de 2027.

3. *Orden de alejamiento y orden de protección*

La orden de alejamiento, tal y como se dijo *supra*, se estableció en nuestro ordenamiento en virtud de la ley orgánica 14/1999, la cual introdujo el artículo 544 *bis* en la LECrim.

Como ya se ha señalado anteriormente, este precepto autoriza al Juez o Tribunal a, en el caso de los delitos de homicidio, aborto, lesiones, contra la libertad, de torturas y contra la integridad moral, trata de seres humanos, contra la libertad e indemnidad sexuales, la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el honor, el patrimonio, el orden socioeconómico y las relaciones familiares; imponer cautelarmente al inculpado la prohibición de residir en un determinado lugar, barrio, municipio, provincia u otra entidad local, o Comunidad Autónoma. Asimismo, en iguales condiciones podrá imponerle cautelarmente la prohibición de acudir a determinados lugares, barrios, municipios, provincias u otras entidades locales, o Comunidades Autónomas, o de aproximarse o comunicarse con determinadas personas.

Así, se acuerda como medida de protección de la víctima tanto la orden de alejamiento como la de prohibición de comunicación, la cual se adoptará cuando resulte estrictamente necesario para lograr el fin de la protección. En el caso de que el investigado y/o acusado incumpla alguna de estas prohibiciones, el Juez o Tribunal convocará la comparecencia regulada en el artículo 505 de la LECrim para sustanciar la posibilidad de acordar una medida cautelar más grave como puede ser la prisión provisional o, en su caso, dictar una orden de protección u otra medida cautelar más restrictiva con su libertad personal.

Según señala Llorente Sánchez-Arjona, las medidas que se estipulan en este precepto "tienen como objetivo común el distanciamiento físico y de comunicación entre agresor y víctima para garantizar la adecuada protección de esta última" [27]. Estas medidas, siguiendo a la citada autora, "se reconducen a cuatro tipos, a saber, prohibición de residir en un determinado lugar, prohibición de acudir a determinados

[27] M. LLORENTE SÁNCHEZ-ARJONA, *Medidas cautelares en los procesos por violencia de género* en M. LLORENTE SÁNCHEZ-ARJONA, R. ZAFRA ESPINOSA DE LOS MONTEROS (a cura di), *La violencia de género en la sombra*, Navarra, 2023, p. 268.

lugares, prohibición de aproximarse a determinadas personas y prohibición de comunicación"[28].

Otra medida encaminada a una mejor protección de la víctima es, precisamente, la orden de protección regulada en el artículo 544 *ter* de la LECrim. Este instrumento confiere a la víctima un estatuto integral de protección, el cual comprende una serie de medidas penales, civiles, asistenciales, de protección social, etc.[29]. La orden de protección se dictará siempre que existan indicios fundados de la comisión de un delito o falta contra la vida, integridad física o moral, libertad sexual, libertad o seguridad de alguna de las personas mencionadas en el artículo 173.2 del Código Penal y, además, resulte una *situación objetiva de riesgo* para la víctima.

De este modo, uno de los aspectos más controvertidos a la hora de adoptar la orden de protección es establecer la existencia de una *situación objetiva de riesgo para la víctima*. Para determinar este riesgo "el atestado puede ser un instrumento muy importante para que el Juez deduzca, siquiera indiciariamente, la existencia de una situación objetiva de riesgo para la misma, sobre la que fundamentará la adopción, en su caso, de una orden de protección"[30]. Para ello las Fuerzas y

[28] *Ibid.*

[29] En el año 2023 se solicitaron en los órganos judiciales un total de 50.806 órdenes de protección. De ellas, fueron acordadas 35.551. Los órganos judiciales acordaron también, derivadas de las órdenes de protección y de otras medidas cautelares, un total de 64.914 medidas judiciales penales de protección de las víctimas (mujeres y menores). En el ámbito penal, las más frecuentes fueron las órdenes de alejamiento (25.137), que representaron el 67,37 % del total de órdenes de protección y medidas cautelares acordadas, y la prohibición de comunicación (24.270), un 65,25 por ciento. Por otra parte, los órganos judiciales dictaron un total de 20.757 medidas cautelares civiles, cuya finalidad es la protección de la mujer y de los menores en tanto se resuelve el proceso penal. Las más frecuentes fueron las relacionadas con la prestación de alimentos (6.471), seguidas por las relacionadas con la atribución de la vivienda (4.550), la suspensión del régimen de visitas (4.026) y la suspensión de la guardia y custodia (2.411). Así lo indica la comunicación: PODER JUDICIAL DE ESPAÑA, *Las 194.658 víctimas de la violencia de género de 2023, 533 mujeres cada día, suponen un aumento del diez por ciento con respecto al año anterior*, 2024.

[30] E. MARTÍNEZ GARCIA, A. MONTESINOS GARCÍA, J. C. VEGAS AGUILAR, A. PLANCHADELL GARGALLO, *Tomo XXXI Esquemas sobre procesos por violencia de género,* 3ª Edición, Valencia, 2022, p. 162.

Cuerpos de Seguridad cuentan con una herramienta valiosa como es la de la Valoración Policial del Riesgo.

Así, esta Valoración Policial del Riesgo se regula por la Instrucción 4/2019, de la Secretaria de Estado de Seguridad, por la que se establece un nuevo protocolo para la valoración policial del nivel de riesgo de violencia de género (LOVG), la gestión de la seguridad de las víctimas y seguimiento de los casos a través del sistema de seguimiento integral de los casos de violencia de género (sistema VIOGÉN)[31], cuyo objetivo es regular la articulación de medidas policiales de protección a mujeres víctimas de violencia y menores a su cargo, conforme a lo establecido en la LOVG.

Esta Instrucción quedará sin efecto en virtud de la Instrucción 1/2025, de la secretaría de estado de seguridad, por la que se establece un nuevo protocolo para la valoración y gestión policial del nivel de riesgo de violencia de género y seguimiento de los casos a través del sistema VioGén-2[32] —Esta Instrucción entrará en vigor a partir del del 30 de junio de 2025—. En este Protocolo se sigue teniendo en cuenta, como no podía ser de otra forma, la denominada violencia de género digital, siendo consciente de que, en la actualidad, muchos delitos de violencia de género, se cometen, total o parcialmente, a través de las nuevas tecnologías de la información y comunicación. Así, en lo que a *violencia de género digital o ciberviolencia de género*, establece que "cuando se detecten este tipo de conductas mediante amenazas, coacciones, acoso u otras formas de agresiones, se pondrá especial atención en la tramitación de los atestados siempre conforme al presente Protocolo, incluyendo la valoración policial de riesgo. En estos supuestos será preceptivo, en el tratamiento de las evidencias digitales, que se observen todas las garantías y se adopten las medidas oportunas para asegurar su adecuada recogida, preservación y custodia, lo que permitirá su presentación en el proceso judicial como elemento probatorio".

[31] PODER JUDICIAL DE ESPAÑA, *Instrucción 4/2019, de la Secretaria de Estado de Seguridad, por la que se establece un nuevo protocolo para la valoración policial del nivel de riesgo de violencia de género (Ley Orgánica 1/2004), la gestión de la seguridad de las víctimas y seguimiento de los casos a través del sistema de seguimiento integral de los casos de violencia de género (Sistema VIOGÉN),* 2019.

[32] MINISTERIO DEL INTERIOR, *Interior diseña un nuevo modelo de respuesta policial a la violencia de género*, en *Prensa*, 2025.

Como novedad del citado protocolo, desaparece el riesgo "no apreciado", con lo que los casos se distribuyen en cuatro niveles de riesgo: "Bajo", "Medio", "Alto" y "Extremo". En todos los casos de violencia de género, la valoración del nivel de riesgo de nueva agresión contra la mujer (Valoración Policial del Riesgo, VPR) y su evolución (Valoración Policial de la Evolución del Riesgo, VPER) se realizará empleando una serie de formularios en los que se valora la información relativa al caso concreto.

El Sistema VioGén-2, una vez que se haya realizado la valoración en el caso concreto, asignará automáticamente uno de los siguientes niveles de riesgo: "no apreciado", "bajo", "medio", "alto" o "extremo", el cual podrá ser modificado por los agentes al alza si, a su juicio y atendiendo a indicios que no se reflejen en los indicadores de riesgo del formulario de valoración, consideran que resulta necesario para una mejor protección de la víctima. El resultado se comunicará a la Autoridad Judicial y Fiscal mediante el informe que genera el propio Sistema. Dicho Informe, con todo su contenido, se incluirá en el Atestado policial, con lo que la autoridad judicial podrá contar con información valiosa para determinar esa *situación objetiva de riesgo* que se requiere para adoptar la orden de protección.

Por último, señalar que el citado protocolo establece una serie medidas de protección en función del riesgo detectado. En cuanto a las medidas relacionadas con la ciberviolencia destacar que, para el *riesgo bajo*, las recomendaciones a la víctima en relación con su ciberseguridad son las siguientes, a saber: Mantener sus perfiles privados para tener más control sobre quien accede a las fotos, datos y publicaciones; No aceptar solicitudes de seguimiento de usuarios que no reconozca; Evitar publicar información personal y la ubicación de los lugares a los que vaya, para evitar que el agresor la pueda localizar; Concienciar, a sus personas cercanas, del riesgo que corre al ser mencionada o etiquetada en redes sociales las fotografías en las que se pueda obtener información sobre lugares o personas con las que tiene una relación frecuente, dicha información puede constituir una merma de su seguridad personal; Cambiar las contraseñas de las diferentes aplicaciones que puedan facilitar información personal o su localización.

Para el *riesgo medio* se recomienda a la víctima el bloqueo de per-

files que puedan ser usados por el agresor para acceder a su perfil o contactar con ella. Y denunciar a través de las propias redes sociales cualquier mensaje ofensivo o sospechoso, realizando previamente la salvaguarda de los datos digitales de los citados mensajes. Para el *riesgo alto* se recomienda la eliminación de los perfiles actuales de las redes sociales y el cambio de número de teléfono, que deberá compartir solo con su Círculo de Fortaleza. Y para el *riesgo extremo* se aconseja la creación de una nueva identidad digital.

Otro instrumento de interés en este sentido es el Protocolo de valoración forense urgente del riesgo de violencia de género[33]. Mediante este protocolo los médicos forenses realizan esa valoración del riesgo. Una importante diferencia con el anterior protocolo es que la valoración forense se realiza, en la mayor parte de los casos, a petición de la autoridad judicial o del Ministerio Fiscal como diligencia de investigación. Mientras que el protocolo de valoración policial se activa desde el momento en el que las Fuerzas y Cuerpos de Seguridad tengan conocimiento de un caso de violencia de género[34].

Si concurren los dos elementos para acordar la orden de protección, esta será dictada por el juez de oficio o a instancia de la víctima o alguna de las personas mencionadas en el artículo 173.2 del Código Penal, o del Ministerio Fiscal. Además, se establece un obligación de denunciar – más allá de la obligación que establece el artículo 262 de la LECrim – de las entidades u organismos asistenciales, públicos o privados, las cuales, en cuanto tengan conocimiento de algún suceso relacionado con la violencia de género o familiar, deberán ponerlos

[33] PODER JUDICIAL DE ESPAÑA, *Protocolo de valoración forense urgente del riesgo de Violencia de Género*, Madrid, 2020.

[34] Sobre estos instrumentos de medición del riesgo es de interés, sin ánimo de exhaustividad, A. ANDRÉS-PUEYO, S. REDONDO ILLESCAS, *Predicción de la violencia: entre la peligrosidad y la valoración del riesgo de violencia* en *Papeles del psicólogo*, 2007, n. 28(3), pp. 157-173; A. ANDRÉS-PUEYO, S. LÓPEZ, *SARA Manual para la valoración del riesgo de violencia contra la pareja*, Barcelona, 2005; J. C. VÁZQUEZ SALGADO, *Protocolos de actuación policial ante la violencia de género* en R. CASTILLEJO MANZANARES (a cura di), *Violencia de género, justicia restaurativa y mediación*, Madrid, 2011, pp. 161-208; E. MARTÍNEZ GARCÍA, J. Mª GÓMEZ VILLORA, R. BORGES BLÁZQUEZ, *Protocolos sobre violencia de género: guía sistemática sobre actuación ante los juzgados de violencia sobre la mujer y en los procedimientos de violencia de género* 2ª edición, Valencia, 2009.

inmediatamente en conocimiento del juez de guardia o del Ministerio Fiscal; con el fin de que se pueda incoar o instar el procedimiento para la adopción de la orden de protección.

La orden de protección podrá solicitarse directamente ante la autoridad judicial o el Ministerio Fiscal, o bien ante las Fuerzas y Cuerpos de Seguridad, las oficinas de atención a la víctima o los servicios sociales o instituciones asistenciales dependientes de las Administraciones públicas. Dicha solicitud habrá de ser remitida de forma inmediata al juez competente. En caso de suscitarse dudas acerca de la competencia territorial del juez, deberá iniciar y resolver el procedimiento para la adopción de la orden de protección el juez ante el que se haya solicitado ésta, sin perjuicio de remitir con posterioridad las actuaciones a aquel que resulte competente; todo ello con el objetivo de proteger a la víctima desde el primer momento en el que se encuentre en peligro.

Los servicios sociales y las entidades u organismos asistenciales, públicos o privados, facilitarán a las víctimas, a las que hubieran de prestar asistencia, la solicitud de la orden de protección debiendo, además, poner a su disposición con esta finalidad información, formularios y, en su caso, canales de comunicación telemáticos con la Administración de Justicia y el Ministerio Fiscal.

Una vez recibida la solicitud de orden de protección, el Juez de guardia convocará a una audiencia urgente a la víctima o su representante legal, al solicitante y al presunto agresor, asistido, en su caso, de Abogado. Asimismo, será convocado el Ministerio Fiscal. Cuando, excepcionalmente, no fuese posible celebrar la audiencia durante el servicio de guardia, el Juez ante el que hubiera sido formulada la solicitud la convocará en el plazo más breve posible. En cualquier caso, la audiencia habrá de celebrarse en un plazo máximo de setenta y dos horas desde la presentación de la solicitud.

Durante la audiencia, el Juez de guardia adoptará las medidas oportunas para evitar la confrontación entre el presunto agresor y la víctima, sus hijos y los restantes miembros de la familia. A estos efectos dispondrá que su declaración en esta audiencia se realice por separado.

Una vez celebrada la audiencia, el Juez de guardia resolverá mediante auto lo que proceda sobre la solicitud de la orden de protec-

ción, así como sobre el contenido y vigencia de las medidas que incorpore. Sin perjuicio de ello, el Juez de instrucción podrá adoptar en cualquier momento de la tramitación de la causa las medidas previstas en el artículo 544 bis –prohibición de acercamiento o de comunicación–. La orden de protección podrá hacerse valer ante cualquier autoridad y Administración pública.

Las medidas cautelares de carácter penal podrán consistir en cualesquiera de las previstas en la legislación procesal criminal. Las medidas de naturaleza civil deberán ser solicitadas por la víctima o su representante legal, o bien por el Ministerio Fiscal cuando existan hijos menores o personas con la capacidad judicialmente modificada, determinando su régimen de cumplimiento y, si procediera, las medidas complementarias a ellas que fueran precisas, siempre que no hubieran sido previamente acordadas por un órgano del orden jurisdiccional civil, y sin perjuicio de las medidas previstas en el artículo 158 del Código Civil[35]. Cuando existan menores o personas con discapacidad nece-

[35] El Juez, de oficio o a instancia del propio hijo, de cualquier pariente o del Ministerio Fiscal, dictará:

1.º Las medidas convenientes para asegurar la prestación de alimentos y proveer a las futuras necesidades del hijo, en caso de incumplimiento de este deber, por sus padres.

2.º Las disposiciones apropiadas a fin de evitar a los hijos perturbaciones dañosas en los casos de cambio de titular de la potestad de guarda.

3.º Las medidas necesarias para evitar la sustracción de los hijos menores por alguno de los progenitores o por terceras personas y, en particular, las siguientes:

a) Prohibición de salida del territorio nacional, salvo autorización judicial previa.

b) Prohibición de expedición del pasaporte al menor o retirada del mismo si ya se hubiere expedido.

c) Sometimiento a autorización judicial previa de cualquier cambio de domicilio del menor.

4.º La medida de prohibición a los progenitores, tutores, a otros parientes o a terceras personas de aproximarse al menor y acercarse a su domicilio o centro educativo y a otros lugares que frecuente, con respecto al principio de proporcionalidad.

5.º La medida de prohibición de comunicación con el menor, que impedirá a los progenitores, tutores, a otros parientes o a terceras personas establecer contacto escrito, verbal o visual por cualquier medio de comunicación o medio informático o telemático, con respeto al principio de proporcionalidad.

6.º La suspensión cautelar en el ejercicio de la patria potestad y/o en el ejercicio de la guarda y custodia, la suspensión cautelar del régimen de visitas y comunicaciones

sitadas de especial protección que convivan con la víctima y dependan de ella, el Juez deberá pronunciarse en todo caso, incluso de oficio, sobre la pertenencia de la adopción de estas medidas civiles.

Estas medidas civiles podrán consistir en la forma en que se ejercerá la patria potestad, acogimiento, tutela, curatela o guarda de hecho, atribución del uso y disfrute de la vivienda familiar, determinar el régimen de guarda y custodia, suspensión o mantenimiento del régimen de visitas, comunicación y estancia con los menores o personas con discapacidad necesitadas de especial protección, el régimen de prestación de alimentos, así como cualquier disposición que se considere oportuna a fin de apartarles de un peligro o de evitarles perjuicios.

Cuando se dicte una orden de protección con medidas de contenido penal y existieran indicios fundados de que los hijos e hijas menores de edad hubieran presenciado, sufrido o convivido con este tipo de violencia, la autoridad judicial, de oficio o a instancia de parte, suspenderá el régimen de visitas, estancia, relación o comunicación del inculpado respecto de los menores que dependan de él. No obstante, a instancia de parte, la autoridad judicial podrá no acordar la suspensión mediante resolución motivada en el interés superior del menor y previa evaluación de la situación de la relación paternofilial.

Las medidas de carácter civil contenidas en la orden de protección tendrán una vigencia temporal de treinta días. Si dentro de este plazo fuese incoado a instancia de la víctima o de su representante legal un proceso de familia ante la jurisdicción civil, las medidas adoptadas permanecerán en vigor durante los treinta días siguientes a la presentación de la demanda. En este término las medidas deberán ser ratifi-

establecidos en resolución judicial o convenio judicialmente aprobado y, en general, las demás disposiciones que considere oportunas, a fin de apartar al menor de un peligro o de evitarle perjuicios en su entorno familiar o frente a terceras personas.

En caso de posible desamparo del menor, el juzgado comunicará las medidas a la entidad pública. Todas estas medidas podrán adoptarse dentro de cualquier proceso judicial o penal o bien en un expediente de jurisdicción voluntaria, en que la autoridad judicial habrá de garantizar la audiencia de la persona menor de edad, pudiendo el Tribunal ser auxiliado por personas externas para garantizar que pueda ejercitarse este derecho por sí misma.

cadas, modificadas o dejadas sin efecto por el Juez de primera instancia que resulte competente.

La orden de protección será notificada a las partes, y comunicada por el Letrado de la Administración de Justicia inmediatamente, mediante testimonio íntegro, a la víctima y a las Administraciones públicas competentes para la adopción de medidas de protección, sean éstas de seguridad o de asistencia social, jurídica, sanitaria, psicológica o de cualquier otra índole.

La orden de protección implicará el deber de informar permanentemente a la víctima sobre la situación procesal del investigado o encausado, así como sobre el alcance y vigencia de las medidas cautelares adoptadas. En particular, la víctima será informada en todo momento de la situación penitenciaria del presunto agresor. A estos efectos se dará cuenta de la orden de protección a la Administración penitenciaria.

Esta orden de protección se podrá dictar a lo largo de todo el proceso penal, en aquellos casos en que durante su tramitación surja una situación de riesgo para alguna de las personas vinculadas con el investigado o encausado.

Entre las medidas de protección destacadas para las víctimas de violencia de género se encuentran las establecidas en los artículos 61 y siguientes de la LOVG. Según el artículo 61, estas medidas son compatibles con cualquier medida cautelar y de aseguramiento que pueda adoptarse en los procesos civiles y penales.

En todos los procedimientos relacionados con la violencia de género, el juez competente deberá pronunciarse, de oficio o a instancia de las víctimas, sus hijos, las personas que convivan con ellas o estén bajo su guarda o custodia, el Ministerio Fiscal o la Administración responsable de los servicios de atención a las víctimas; sobre la pertinencia de adoptar las medidas cautelares y de aseguramiento contempladas en el capítulo IV de la citada norma. En dicho pronunciamiento, deberá resolver sobre el plazo y régimen de cumplimiento, y, si procede, sobre las medidas complementarias necesarias.

El artículo 62 establece la posibilidad de adoptar una orden de protección, remitiéndose a lo establecido en el artículo 544 *ter* de la LECrim. El artículo siguiente prevé la obligación de proteger la intimidad de las víctimas, especialmente sus datos personales, los de sus

descendientes y los de cualquier otra persona bajo su guarda o custodia. Los jueces competentes podrán acordar, de oficio o a instancia de parte, que las vistas se desarrollen a puerta cerrada y que las actuaciones sean reservadas.

El artículo 64 prescribe medidas sobre la salida del domicilio, alejamiento o suspensión de las comunicaciones. El juez podrá ordenar la salida obligatoria del inculpado del domicilio familiar y prohibir su regreso. Excepcionalmente, el juez podrá autorizar que la persona protegida concierte, con una agencia o sociedad pública, la permuta del uso de la vivienda familiar por otra vivienda, durante el tiempo y en las condiciones que se determinen.

Asimismo, el juez podrá prohibir al inculpado acercarse a la persona protegida, su domicilio, lugar de trabajo o cualquier otro lugar frecuentado por ella. Para el cumplimiento de esta medida podrá utilizarse tecnología adecuada para verificar su incumplimiento[36]. La medida de alejamiento podrá acordarse independientemente de que la persona afectada haya abandonado previamente el lugar.

También se podrá prohibir al inculpado cualquier tipo de comunicación con la persona protegida, bajo apercibimiento de responsabilidad penal. Estas medidas podrán adoptarse acumulada o separadamente.

Estas medidas deberán complementarse con lo establecido en la citada directiva sobre violencia contra las mujeres y violencia doméstica para situaciones de peligro inmediato para la salud o la seguridad de la víctima o de las personas a cargo. Como se ha dicho anteriormente, pero que nos parece interesante recordar, en tales supuestas las autoridades competentes podrán dictar, sin demora indebida, órdenes dirigidas al sospechoso de un acto de violencia para que abandone el domicilio de la víctima o de las personas a cargo durante un período de tiempo suficiente y para prohibir que el autor o sospechoso entre en el domicilio, o se acerque a una distancia de dicho domicilio inferior a la ordenada, o entre en el lugar de trabajo de la víctima o se comunique en modo alguno con ella o con las personas a cargo. Estas

[36] Para consultar estos tipos de dispositivos es de interés el siguiente enlace https://violenciagenero.igualdad.gob.es/informacion-3/recursos/ dispositivoscontroltelematico/

órdenes tendrán efecto inmediato y no dependerán de que la víctima denuncie el delito.

En otro orden de cosas, el artículo 65 prevé medidas de suspensión de la patria potestad o la custodia de menores. Si no se adoptan estas suspensiones, el juez deberá pronunciarse sobre la forma en que se ejercerá la patria potestad, guarda y custodia, acogimiento, tutela, curatela o guarda de hecho de los menores. Asimismo, adoptará las medidas necesarias para garantizar la seguridad, integridad y recuperación de los menores y de la mujer, realizando un seguimiento periódico de su evolución.

El artículo 66 regula medidas de suspensión del régimen de visitas, estancia, relación o comunicación con los menores. Si, en interés superior del menor, no se acuerda la suspensión, el juez deberá pronunciarse sobre la forma en que se ejercerá el régimen de estancia, relación o comunicación del inculpado respecto de los menores. Adoptará las medidas necesarias para garantizar la seguridad, integridad y recuperación de los menores y de la mujer, a través de servicios de atención especializada, y realizará un seguimiento periódico de su evolución en coordinación con dichos servicios. La última medida prevista en este capítulo es la suspensión del derecho a la tenencia, porte y uso de armas, con la obligación de depositarlas según la normativa vigente.

Todas estas medidas deberán adoptarse mediante auto motivado que aprecie su proporcionalidad y necesidad, con intervención del Ministerio Fiscal y respeto a los principios de contradicción, audiencia y defensa. Asimismo, podrán mantenerse tras la sentencia definitiva y durante la tramitación de los eventuales recursos, debiendo constar en la sentencia dicho mantenimiento.

4. *La protección de las víctimas en la ley 4/2015, del estatuto de la víctima del delito, de 27 de abril de 2015*

En el Título III de la ley 4/2015 se prescriben una serie de derechos encaminados a la efectividad frente a represalias, intimidación, victimización secundaria, daños psíquicos o agresiones a la dignidad durante los interrogatorios y declaraciones como testigo.

El primero de estos derechos se regula en el artículo 19, y obliga a las autoridades y funcionarios encargados de la investigación, persecución y enjuiciamiento de los delitos a adoptar las medidas necesarias para garantizar la vida de la víctima y de sus familiares, su integridad física y psíquica, libertad, seguridad, libertad e indemnidad sexuales, así como para proteger adecuadamente su intimidad y su dignidad, particularmente cuando se les reciba declaración o deban testificar en juicio, y para evitar el riesgo de su victimización secundaria o reiterada.

Con el fin de lograr una eficaz protección, la norma remite a que se adopten las medidas previstas en la LECrim, sobre las que ya hemos tratado. Así, se deberán dictar, en su caso, la orden de alejamiento o la orden de protección – como quiera que estas herramientas han sido tratadas *supra*, nos remitimos a lo ya dicho al respecto –. Asimismo, el art. 258 *bis*. 3 garantiza que la declaración de ciertas víctimas, entre las que se hallan las de violencia de género y violencia sexual, se puede realizar de forma telemática, salvo que el Juez o Tribunal, mediante resolución motivada en atención a las circunstancias del caso concreto, estime necesaria su presencia física.

El artículo 20 de la ley 4/2015 reconoce el derecho a que se evite el contacto entre víctima e infractor. Esta medida de protección está íntimamente ligada a la anterior, aunque el legislador amplía su alcance a cualquier dependencia en las que se desarrollen los actos del procedimiento penal, incluida la fase de investigación, las cuales estarán dispuestas de modo que se evite el contacto directo entre las víctimas y sus familiares, de una parte, y el sospechoso de la infracción o acusado, de otra. Por consiguiente, abarcaría dependencias policiales, judiciales, etc.

El artículo 21 regula medidas encaminadas a la protección de la víctima durante la investigación penal. Así, se impone una obligación a las autoridades y funcionarios encargados de la investigación penal de velar por el cumplimiento de las mismas, en la medida que ello no perjudique la eficacia del proceso. Para ello deberán recibir la declaración a las víctimas, cuando resulte necesario, sin dilaciones injustificadas. Que dichas declaraciones se realicen el menor número de veces posible, y únicamente cuando resulte estrictamente necesario para los fines de la investigación penal. Que las víctimas estén acompañadas por una persona de su elección durante la práctica de aquellas diligencias en

las que deban intervenir, además de por su representante procesal y, en su caso, el representante legal. Y que los reconocimientos médicos de las víctimas solamente se lleven a cabo cuando resulten imprescindibles para los fines del proceso penal, y se reduzca al mínimo el número de los mismos.

Como se puede observar, más que medidas encaminadas a la protección de la víctima son instrumentos cuyo objetivo es evitar la victimización secundaria entendida como aquella "que sufre la víctima cuando, a consecuencia del delito, tiene que comparecer ante los profesionales sanitarios, policiales o judiciales, y que supone una nueva agresión (especialmente psicológica) no deliberada pero no por ello menos dañina en ocasiones que la victimización primaria"[37].

Otro derecho de las víctimas es el de la protección de la intimidad, regulado en el artículo 22. Este precepto ordena a los Jueces, Tribunales, Fiscales y las demás autoridades y funcionarios encargados de la investigación penal, así como todos aquellos que de cualquier modo intervengan o participen en el proceso; la adopción de las medidas necesarias para proteger la intimidad de todas las víctimas y de sus familiares y, en particular, para impedir la difusión de cualquier información que pueda facilitar la identificación de las víctimas menores de edad o de víctimas con discapacidad necesitadas de especial protección.

Este artículo debemos conectarlo con lo previsto en los artículos 301 bis, 681, 682 y 709 de la LECrim. El primero de los preceptos establece la posibilidad de que el Juez, de oficio o a instancia del Ministerio Fiscal o de la víctima, adopte cualquiera de las medidas a que se refiere el apartado 2 del artículo 681 cuando resulte necesario para proteger la intimidad de la víctima o el respeto debido a la misma o a su familia.

Así, el artículo 681 regula la posibilidad de que todos o alguno de los actos o las sesiones del juicio se celebren a puerta cerrada, cuando así lo exijan, entre otros motivos, el derecho a la intimidad de la víctima, el respeto debido a la misma o a su familia, o resulte necesario pa-

[37] INSTITUTO ANDALUZ DE LA MUJER, *Protocolo para evitar la victimización secundaria en mujeres víctimas de violencia de género*, León, 2021.

ra evitar a las víctimas perjuicios relevantes que, de otro modo, podrían derivar del desarrollo ordinario del proceso.

Asimismo, podrá acordar la adopción de las siguientes medidas para la protección de la intimidad de la víctima y de sus familiares:

a) Prohibir la divulgación o publicación de información relativa a la identidad de la víctima, de datos que puedan facilitar su identificación de forma directa o indirecta, o de aquellas circunstancias personales que hubieran sido valoradas para resolver sobre sus necesidades de protección.

b) Prohibir la obtención, divulgación o publicación de imágenes de la víctima o de sus familiares.

Además, en virtud del artículo 682, el Juez o Tribunal podrá restringir la presencia de los medios de comunicación audiovisuales en las sesiones del juicio y prohibir que se graben todas o alguna de las audiencias cuando resulte imprescindible para preservar, entre otros motivos, el derecho a la intimidad de las víctimas, el respeto debido a la misma o a su familia, o la necesidad de evitar a las víctimas perjuicios relevantes que, de otro modo, podrían derivar del desarrollo ordinario del proceso.

A estos efectos, podrá prohibir:

a) Que se grabe el sonido o la imagen en la práctica de determinadas pruebas, o determinar qué diligencias o actuaciones pueden ser grabadas y difundidas.

b) Que se tomen y difundan imágenes de alguna o algunas de las personas que en él intervengan.

c) Que se facilite la identidad de las víctimas, de los testigos o peritos o de cualquier otra persona que intervenga en el juicio.

Por último, el artículo 709 protege a la víctima de que se le formulen preguntas innecesarias relativas a la vida privada, en particular a la intimidad sexual, que no tengan relevancia para el hecho delictivo enjuiciado.

Por otro lado, el artículo 23 de la ley 4/2015 establece la evaluación individual de la víctima para determinar sus necesidades especiales de protección, la cual se realizará tras una evaluación de sus circunstancias particulares. Esta valoración considerará especialmente las características personales de la víctima, así como la naturaleza del delito y las circunstancias del delito, en particular si se trata de delitos vio-

lentos. A estos efectos se valorarán especialmente las necesidades de protección de, entre otras, las víctimas de violencia de género. De este modo, la citada evaluación está en consonancia con lo previsto en la propia directiva 2024/1385 anteriormente citada.

Dicha evaluación recae sobre el Juez de Instrucción o al de Violencia sobre la Mujer durante la fase de investigación, y al Juez o Tribunal correspondiente durante la fase de enjuiciamiento. Los servicios de asistencia a la víctima solo podrán facilitar información a terceros con el consentimiento previo e informado de la víctima, salvo en casos de traslado reservado a la autoridad competente. Cualquier modificación relevante de las circunstancias evaluadas determinará una actualización de la valoración y, en su caso, la modificación de las medidas de protección.

Por último, el artículo 25 establece una serie de concretas medidas de protección tanto en la fase de investigación como en la de enjuiciamiento. Así, durante la fase de investigación se pueden adoptar medidas tales como recibir declaración en dependencias adaptadas, por profesionales con formación especial, y que todas las declaraciones sean realizadas por la misma persona, salvo excepciones. En casos de víctimas de delitos específicos, entre los que se encuentran las de violencia de género, la declaración puede ser tomada por una persona del mismo sexo que la víctima, si así lo solicita. Durante la fase de enjuiciamiento, se pueden adoptar medidas para evitar el contacto visual entre la víctima y el autor, garantizar que la víctima sea oída sin estar presente en la sala, evitar preguntas irrelevantes sobre la vida privada de la víctima, y celebrar la vista oral sin público. También se pueden adoptar medidas de protección según la ley orgánica 19/1994[38].

Por último, vamos a tratar un instrumento que, a nuestro parecer, es fundamental para la protección de las víctimas en el ámbito de la Unión europea. Como veremos, se trata de una herramienta con bastantes limitaciones, pero que debería de ser el germen de un verdadero estatuto de protección a las víctimas en el seno de la Unión.

[38] Ley orgánica 19/1994, *de protección a testigos y peritos en causas criminales*, de 23 de diciembre de 1994.

5. *La orden europea de protección*

La orden europea de protección se encuentra regulada en la directiva 2011/99/UE anteriormente citad. En la mencionada directiva, se establece que la Unión Europea se ha propuesto el objetivo de preservar y fomentar un espacio de libertad, seguridad y justicia. Conforme al considerando sexto de la directiva, en un espacio judicial común sin fronteras internas, es imperativo asegurar que la protección brindada a una persona física en un Estado miembro se mantenga y persista en cualquier otro Estado miembro al que dicha persona se traslade o haya trasladado. Asimismo, es esencial garantizar el ejercicio legítimo del derecho de los ciudadanos de la Unión a circular y residir libremente en el territorio de los Estados miembros.

De este modo, con el fin de alcanzar los objetivos de mantener y desarrollar un espacio de libertad, seguridad y justicia –según lo estipulado en el considerando séptimo de la directiva–, se establecen normas que permiten que la protección derivada de determinadas medidas de protección, dictadas conforme al derecho de un Estado miembro ("Estado de emisión")[39], pueda extenderse a otro Estado miembro en el que la persona protegida decida residir o permanecer ("Estado de ejecución")[40].

En virtud del artículo 2 de la norma, una orden europea de protección es una resolución adoptada por una autoridad judicial o equivalente de un Estado miembro en relación con una medida de protección, mediante la cual una autoridad judicial o equivalente de otro Estado miembro adopta las medidas oportunas conforme a su propio derecho nacional para mantener la protección de la persona protegida.

El Estado ejecutor deberá reconocer sin demora indebida la orden, con el fin de adoptar una resolución que dicte cualquiera de las medidas de protección previstas en su derecho nacional para un caso análogo, garantizando así la protección de la persona protegida.

[39] La directiva considera al *Estado de emisión* como aquel Estado miembro en el que se haya adoptado una medida de protección que constituya la base para la emisión de una orden europea de protección.

[40] La directiva entiende al *Estado de ejecución* como aquel Estado miembro al que se haya transmitido una orden europea de protección con vistas a su reconocimiento.

Se considera medida de protección a una resolución en materia penal, adoptada en el Estado de emisión conforme a su legislación y procedimientos nacionales, por la cual se impone a una persona causante de peligro una o más de las prohibiciones o restricciones previstas en el artículo 5, con el objetivo de proteger a la persona protegida de actos delictivos que puedan poner en peligro su vida, integridad física o psicológica, dignidad, libertad individual o integridad sexual.

De este modo, la orden europea de protección busca proteger a las víctimas que pretendan desplazarse por el territorio de la Unión Europea adoptando alguna de las siguientes medidas, a saber:

a) Prohibición de entrar en determinadas localidades, lugares o zonas definidas en las que la persona protegida reside o que frecuenta;

b) Prohibición o reglamentación de cualquier tipo de contacto con la persona protegida, incluidos los contactos telefónicos, por correo electrónico o postal, por fax o por cualquier otro medio, o

c) Prohibición o reglamentación del acercamiento a la persona protegida a una distancia menor de la indicada en la medida.

La persona protegida, según la directiva, es la persona física objeto de la protección derivada de una medida de protección adoptada por el Estado de emisión. La persona causante del peligro es la persona física a la que se le haya impuesto una o más de las prohibiciones o restricciones contempladas en el artículo 5 anteriormente citado.

Como se puede apreciar, son medidas a nuestro parecer insuficientes, aunque en su día fue un primer paso —continuado por la directiva sobre violencia contra las mujeres y violencia doméstica— para lograr un verdadero *estatuto integral de protección* en todo el seno de la Unión que haga efectivo ese espacio de libertad, seguridad y justicia que se proclama.

Abstract

La protección a la víctima debe ser un objetivo primordial en cualquier ámbito de la sociedad en general y del proceso penal en particular. Por tal motivo, es necesario la implementación de medidas cautelares que coadyuven en una eficaz protección de la misma para evitar una nueva victimización y, además, garantizar un proceso con todas las garantías también para ella.

En el presente trabajo se van a abordar las medidas cautelares que tanto el ordenamiento jurídico español como el europeo implementan, con el objetivo de conseguir una protección eficaz de las víctimas de violencia de género, teniendo en cuenta la especial idiosincrasia de este género delictivo.

PALABRAS CLAVE: Protección de la víctima – orden de alejamiento – orden de protección – orden europea de protección – victimología

MISURE CAUTELARI NAZIONALI E TRANSNAZIONALI RELATIVE ALLA PROTEZIONE DELLE VITTIME DI VIOLENZA INFORMATICA DI GENERE

La protezione della vittima deve essere un obiettivo primario in qualsiasi ambito della società in generale e nel procedimento penale in particolare. Per questo motivo, è necessario attuare misure cautelari che contribuiscano all'effettiva protezione della vittima, al fine di evitare ulteriori vittimizzazioni e, inoltre, di garantire un processo con tutte le garanzie per la vittima.
Questo articolo tratterà delle misure cautelari che i sistemi giuridici spagnoli ed europei mettono in atto, con l'obiettivo di ottenere una protezione efficace per le vittime di violenza di genere, tenendo conto delle particolari idiosincrasie di questo tipo di reato.

KEYWORDS: Protezione della vittima – ordine restrittivo – ordine di protezione – ordine di protezione europeo – vittimologia

LA PRUEBA EN LOS PROCESOS POR VIOLENCIA DIGITAL DE GÉNERO

Mª José Jordán Díaz-Roncero[*]

SUMARIO: 1. Introducción: la irrupción de las TIC en la comisión, en la acreditación de delitos en violencia digital de género y en la protección de sus víctimas. – 2. La problemática de la práctica y valoración de la prueba en el ámbito de los delitos de violencia contra la mujer y muy especialmente en la violencia digital de género. – 3. Problemas probatorios tradicionales: la declaración de la víctima como única prueba de cargo y la dispensa del art. 416 LECRIM. – 4. La problemática de la prueba de la violencia de género con empleo de TIC. – 5. La prueba de la violencia de género digital: Ilícitos penales cometidos a través de comunicaciones instantáneas bidireccionales o multidireccionales. – 5.1. Los contenidos de mensajes de WhatsApp o en plataformas similares como medio de prueba. – 5.2. Ilícitos penales cometidos a través de webs o redes sociales. – 5.2.1. Eliminación de las publicaciones en el momento de ser notificado el autor del delito la existencia una investigación penal: necesidad de acreditar el contenido web o de la red social antes de interponer la correspondiente denuncia. – 5.2.2. Acreditación tras impugnación del contenido de la web, o de la concreta publicación o de la titularidad de la cuenta: la problemática de las comisiones rogatorias y el riesgo de prescripción delictiva. – 5.3. Ilícitos penales cometidos a través de correos electrónicos. – 6. La necesaria práctica de prueba indiciaria en la valoración de la prueba con perspectiva de género. – 7. Aplicación de tecnología *blockchain* en prueba electrónica para garantizar la cadena de custodia.

1. *Introducción: la irrupción de las TIC en la comisión, en la acreditación de delitos en violencia digital de género y en la protección de sus víctimas*

Vivimos en un permanente estado de alerta ante los casos de violencia contra la mujer cometidos por razones discriminatorias de género, si bien, últimamente, se aprecian actos de violencia de género per-

[*] PDI Ayudante Doctora, Universitat de València, mail: maria.jose.jordan@uv.es

petrados de una forma diferente a la tradicional a la que estaba acostumbrada la sociedad, como consecuencia del empleo de las Tecnologías de la Información y la Comunicación (TIC) en la comisión del delito.

Internet es una herramienta que continúa aún en expansión, que se encuentra al alcance de cualquier persona, lo que provoca que se haga un empleo de forma intensa, junto con el resto de utilidades digitales como redes sociales o aplicaciones de servicios de mensajería instantánea o de geolocalización, entre otros[1].

Esta irrupción en nuestras vidas de dichas tecnologías, que forman parte de nuestro quehacer diario y que, sin duda, una gran parte de la población no puede concebir su vida personal y laboral sin ellas, está propiciando la aparición de conductas relacionadas con la violencia de género con uso o empleo de dichas tecnologías, en la medida que no podemos entender nuestra forma de relacionarnos en sociedad sin ellas.

El fenómeno de la ciberdelincuencia, no solo ha comportado la aparición de nuevos tipos delictivos (como el *phising*, el *cracking* o el *hacking*), que forzosamente necesitan de un espacio virtual para su comisión, sino también la reformulación de otros ya existentes mediante el abuso de las tecnologías[2], con el añadido que las consecuencias del delito pueden tener una mayor trascendencia al desarrollarse en el ciberespacio, al estar libre de todo límite territorial[3].

Resulta paradójico que, a pesar los avances que supone la implementación de las tecnologías en nuestra sociedad, se sigan reproduciendo en espacios virtuales, comportamientos sexistas o discriminatorios por razones de género, con el peligro adicional que la violencia

[1] M. BUENO BENEDÍ, *La prueba en los procedimientos de violencia. Sobre la mujer cometidos a través de las nuevas Tecnologías*, en *Revista Acta Judicial*, 2021, n. 7, p. 18.

[2] E. CERRATO GURI, *Ciberviolencia de género: influencia internacional y europea en la obtención y conservación de prueba electrónica*, en *Revista General de Derecho Europeo*, 2023, n. 61, p. 166.

[3] Véase en este sentido el Informe explicativo del Consejo de Europa del Convenio sobre la ciberdelincuencia de 8 de noviembre de 2001, (disponible en: https://rm.coe.int/16802fa403, fecha de consulta: 31 de julio de 2023). E. CERRATO GURI, *op. cit.* p. 166.

desarrollada a través de estos procedimientos, tiene más posibilidades de diluirse como parte de un ambiente de normalidad[4].

Naciones Unidas, en 2015, alertaba de la necesidad de combatir la violencia contra mujeres y niñas cometida en línea en la medida que el 95% de las conductas agresivas, el acoso, el lenguaje insultante y las imágenes denigrantes que tenían lugar en ese momento en el ciberespacio, estaban dirigidas hacia mujeres y eran ejecutadas por hombres[5], formulando en 2018 en su Informe sobre la violencia en línea contra las mujeres, una definición de ciberviolencia de género, consistente en los actos de violencia de género cometidos a través de las nuevas tecnologías de la información y la comunicación (teléfonos móviles, redes sociales virtuales, etcétera)[6].

A día de hoy, la violencia de género que se ejercita a través de las tecnologías, de redes sociales o de Internet se conoce ya como violencia de género digital, pudiéndose definir la ciberviolencia de género como aquel tipo de violencia que se desarrolla por un hombre mediante el empleo de TIC, contra una mujer, con la intención de someterla, rebajarla o controlarla con base en estereotipos de género[7].

Entre las formas de violencia cometida a través de medios o en entornos digitales más destacadas, encontramos la violación de la privacidad, el acoso, las amenazas o los discursos de odio[8]. De este modo, en la macroencuesta de violencia contra la mujer del año 2019, se con-

[4] M. LLORENTE SÁNCHEZ-ARJONA, *La ciberviolencia de género: nuevas formas de victimización*, en C. ARANGÜENA FANEGO, M. DE HOYOS SANCHO, E. PILLADO GONZÁLEZ (dirs.)*, El proceso penal ante una nueva realidad tecnológica europea*, Pamplona, p. 414. M. LORENTE ACOSTA, *Virtualidad ficticia y violencia de género*, en T. DONOSO VÁZQUEZ, A. REBOLLO CATALÁN (coords.) *Violencias de género en entornos virtuales*, Octaedro, Barcelona, 2018, p. 8.

[5] Informe disponible en: https://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release (fecha de consulta: 8 de enero de 2025).

[6] Informe disponible en: https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and (fecha de consulta: 8 de enero de 2025).

[7] M. LLORENTE SÁNCHEZ-ARJONA, *op. cit.*, p. 415.

[8] Podemos enumerar como comportamientos ciberviolentos más conocidos los siguientes: sexting, sextorsión, cyberstalking, doxing, outing, fraping o pornovenganza, entre otros (A. GARCÍA COLLANTES, M.J. GARRIDO ANTÓN, *Violencia y Ciberviolencia de Género*, Valencia, 2021, p. 58).

cluyó que: (i) un 18,4% de las mujeres encuestadas había recibido insinuaciones inapropiadas, humillantes, intimidatorias u ofensivas en redes sociales como Facebook, Instagram o Twitter; (ii) a un 24,9% de las mujeres encuestadas le habían hecho propuestas inapropiadas en Internet o en redes sociales; (iii) un 4,3% de las citadas mujeres había sido objeto de publicación de fotos, vídeos o información muy personal en redes sociales como Facebook o Instagram[9].

Fuente: elaboración propia

Es decir, el 46,4% de las mujeres encuestadas habían manifestado haber sufrido violencia digital.

En definitiva, estamos ante una realidad preocupante, motivo por el que en la reciente directiva (UE) 2024/1385, del Parlamento europeo y de Consejo, de 14 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica[10], se establece un mandato dirigido a los Estados para regular los ciberdelitos más cometidos, como son el sexting, el ciberacecho, ciberacoso y los delitos de odio perpetrados por medios cibernéticos.

[9] La citada Macroencuesta es susceptible de consulta en: https://violenciagenero.igualdad.gob.es/wp-content/uploads/Macroencuesta_2019_estudio_investigacion.pdf (fecha de consulta: 8 de enero de 2025).

[10] Directiva 2024/1385/UE del Parlamento europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica,* de 14 de mayo de 2024, en DOUE 1385 de 24 de mayo de 2024, pp. 1-36.

La realidad de la ciberviolencia ha llegado a nuestro tribunales y en el ámbito de los procesos penales por violencia de género de carácter digital nos encontramos con una problemática esencial y fundamental: conseguir prueba de cargo suficiente para desvirtuar la presunción de inocencia, a los efectos de cumplir con una de las medidas que debe incluirse en la política criminal de un Estado para actuar con la diligencia debida en materia de violencia de género, a saber, la prevención, la persecución efectiva de estos delitos así como su intento de minorar la tasa de criminalidad existente. Sin el castigo de estos delitos, no cumplimos con las obligaciones positivas del Estado[11], tal y como desarrolla la profesora Martínez García en un capítulo destinado a tal efecto en esta obra colectiva.

A los efectos de lograr prueba de cargo suficiente en violencia de género digital, nos encontramos con diferentes problemáticas: (i) la propia dificultad probatoria en materia de violencia contra la mujer, ya sea violencia digital o violencia tradicional; las dificultades para acreditar los hechos delictivos cometidos a través de las TIC o en entornos digitales; (iii) la escasez de recursos y medios disponibles para perseguir y practicar determinados medios prueba que dificultan la obtención de una prueba de cargo suficiente para fundar una sentencia condenatoria.

No obstante, precisamente la irrupción de las TIC en nuestras vidas, también ofrecen la posibilidad de apoyarnos en ellas, con el objetivo de tratar de acreditar la comisión del delito, ayudándonos a localizar al autor de los mismos a través de informes periciales de carácter tecnológico o herramientas como la geolocalización.

Así mismo, debemos apoyarnos en el empleo de las citadas TIC, para ofrecer una mayor protección a la víctima y evitar la tan temida victimización secundaria, como, por ejemplo, llevar cabo su declaración a través de mecanismos como la Cámara Gesell, pero no sólo en

[11] Sobre la obligación de los Estados de actuar con la diligencia debida en materia de violencia contra las mujeres, ver, E. MARTÍNEZ GARCÍA, *Juzgar en el siglo XXI*, Valencia, pp. 163-216. Hay que tener en cuenta que, en caso de no actuar con la diligencia debida en esta materia, el Estado puede incurrir en responsabilidad patrimonial (J.C. VEGAS AGUILAR, *La responsabilidad del Estado desde la perspectiva de género*, en E. MARTÍNEZ GARCÍA (dir.)*, Análisis de la justicia desde la perspectiva de género*, Valencia, 2018, pp. 201-228).

víctimas menores -tal y como explica la profesora Borges Blázquez en el capítulo destinado en esta obra a víctimas menores de edad-, sino también en mujeres adultas[12], preconstituyendo prueba o llevar a cabo su deposición a través de sistemas como la videoconferencia con el fin de evitar su confrontación visual con su agresor.

2. La problemática de la práctica y valoración de la prueba en el ámbito de los delitos de violencia contra la mujer y muy especialmente en la violencia digital de género

Desde que se tienen estadísticas, hasta diciembre de 2024, se han contabilizado en España 1.293 mujeres asesinadas por violencia de género.

[12] En países como Costa Rica, se prevé la necesidad de llevar a cabo las declaraciones de las víctimas adultas de violencia sexual a través de Cámara Gesell (información disponible en: https://ministeriopublico.poderjudicial.go.cr/images/phocadownload/CircularesAdministrativas/Otros/20-Anexo1.pdf, fecha de consulta: 9 de enero de 2025). En el caso de España, no existe una regulación normativa que permita expresamente esta posibilidad, si bien el Código ético y de buenas prácticas de las unidades de valoración forense integral del Ministerio de Justicia del año 2020 (disponible en: https://violenciagenero.igualdad.gob.es/wp-content/uploads/etico_buenas_practicas.pdf, fecha de consulta 9 de enero de 2025) así como el Protocolo de actuación médico-forense ante la violencia sexual en los Institutos de Medicina Legal y Ciencias Forenses (disponible en: https://www.mjusticia.gob.es/es/ElMinisterio/OrganismosMinisterio/Documents/ProtocoloViolenciaSexual.pdf, fecha de consulta: 9 de enero de 2025), promueven el empleo por parte del personal del Instituto de Medicina Legal de la Cámara Gesell en casos de violencia sexual cuyas víctimas son personas adultas y no sólo con respecto a menores de edad, con el objetivo de evitar la victimización secundaria, desplazamientos innecesarios, repeticiones redundantes del relato de los hechos, duplicidad de exploraciones y demora en la emisión de informes. De ahí que, sería conveniente realizar un cambio normativo en nuestra ley de enjuiciamiento criminal, que promoviera el empleo de esta tecnología en las exploraciones de las víctimas de agresiones sexuales, tanto adultas como menores de edad.

Fuente: Delegación del Gobierno para la Violencia de género

Si nos atenemos a las cifras oficiales facilitadas por el Consejo General del Poder Judicial, en 2023, se presentaron 199.282 denuncias por hechos delictivos relacionados con la violencia de género en el sentido tradicional de la violencia ejercitada en las relaciones de pareja y a falta de determinarse aún el tercer trimestre de 2024, hasta septiembre de 2024, se presentaron 149.582 denuncias.

Resulta muy difícil de asimilar que un país como el nuestro, supuestamente civilizado cuyos valores superiores de nuestro ordenamiento jurídico son la igualdad y la dignidad personal, se interpongan más de 500 denuncias diarias por violencia de género.

Es evidente que algo está fallando, pues la violencia contra la mujer, una cuestión esencial de derechos humanos, no puede resolverse exclusivamente con el derecho penal.

La política criminal de un país, ha de basarse en medidas, criterios y argumentos para prevenir y reaccionar frente a un concreto fenómeno criminal con el objetivo de tratar de disminuir hasta lo tolerable la estadística criminal, por ello, aunque el derecho penal y el derecho procesal penal, van a ocupar un lugar preeminente porque constituye la base de la definición de aquello que se considera delito frente a la conducta lícita, no serán las únicas formas de prevenir y de hacer frente al crimen, pues serán necesarias medidas de carácter económico, educativo, social o incluso cultural, para ciertos sectores de la criminalidad[13], como por ejemplo, la violencia contra la mujer por razones discriminatorias de género.

No hay duda que la solución frente a la violencia de género habrá de llegar, esencialmente, por vía educacional, si bien, la correcta y justa

[13] E. BORJA JIMÉNEZ, *Curso de política criminal,* Valencia, 2021, p. 21.

aplicabilidad del sistema sancionatorio contribuirá en el avance en este camino, por ello, no solo es necesario tipificar las conductas delictivas y fijar las penas en que incurrirá quien cometa el delito, sino que será necesario también favorecer un sistema probatorio que se adapte a las peculiares características de este tipo de violencia, a fin de que esas penas se puedan aplicar y no se generen posibles bolsas de impunidad con la consiguiente desprotección para las víctimas[14].

A los efectos de tratar de no generar dichas bolsas de impunidad, el Observatorio contra la violencia doméstica y de género del Consejo General del Poder Judicial, realizó en marzo de 2016, un estudio sobre la aplicación de la Ley integral contra la violencia de género, analizando 500 sentencias dictadas por Audiencias Provinciales, entre enero de 2012 y diciembre de 2014[15].

En dicho estudio se advirtieron los siguientes problemas relacionados con la prueba, que condujeron a sentencias absolutorias: (i) el acogimiento de la víctima a la dispensa de no declarar del art. 416 LECRIM; (ii) la priorización del silencio de la víctima en el juicio oral sobre la denuncia inicial; (iii) la retractación de la víctima en el juicio oral respecto de la denuncia anterior; (iv) constar únicamente la declaración incriminatoria de la víctima, sin corroboraciones periféricas; (v) la falta absoluta de pruebas; (vi) la existencia de móviles espurios en la denuncia.

En materia de violencia de género, nos encontramos con la problemática habitual de la acreditación de la situación de violencia padecida, esencialmente, por un lado, por tratarse de una violencia de carácter intrapersonal en la que la declaración de la víctima será la única prueba de cargo suficiente para enervar la presunción de inocencia, tanto si estamos en supuestos de violencia contra la mujer por razones de género en las relaciones de pareja o en los supuestos de violencia ajenos a las relaciones sentimentales – como trata de seres humanos, matrimonios forzados, entre otros –; y, por otro lado, por las alteraciones en la declaración de las

[14] O. FUENTES SORIANO, *Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías*, en *Revista General de Derecho de Derecho Procesal*, 2018, n. 44.

[15] Estudio disponible en: https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Grupos-de-expertos/Estudio-sobre-la-aplicacion-de-la-Ley-integral-contra-la-violencia-de-genero-por-las-Audiencias-Provinciales--Marzo-2016- (fecha de consulta: 9 de enero de 2025).

víctimas que ha cambiado de opinión por miedo a represalias o por la gran dependencia emocional que tiene hacia su ofensor, por lo que concurrirán, en muchos casos, motivos psicosociales que desencadenan la voluntad de la víctima de no querer seguir adelante con el procedimiento, pues no desea que su agresor sea condenado.

A estos problemas, se deben añadir en materia de violencia digital, la dificultad probatoria del delito cuando se emplean tecnologías de comunicación o mecanismos digitales en la comisión de los actos de violencia de género.

3. *Problemas probatorios tradicionales: la declaración de la víctima como única prueba de cargo y la dispensa del art. 416 LECRIM*

Aunque en este trabajo, nos vamos a centrar en la prueba de la violencia digital de género, es necesario abordar los problemas tradicionales comunes a la violencia contra la mujer de toda clase, para poder comprender mejor la temática aquí planteada.

En materia de violencia contra la mujer, en no pocas ocasiones, aunque dispongamos de elementos que evidencien la conducta penal denunciada, como por ejemplo, un informe de lesiones que acredite la agresión recibida o un informe del Instituto de Medicina Legal que indique que las lesiones apreciadas son compatibles con una agresión sexual y que los restos de ADN hallados en el interior de la víctima son de la persona denunciada, si la víctima no indica quién es su agresor, no se podrá conectar el informe con la autoría y, por tanto, no tendremos prueba de cargo suficiente para enervar la presunción de inocencia.

También nos hallamos con frecuencia, con la problemática de la voluntad de la víctima de no seguir con el procedimiento, bien por su voluntad de volver a retomar la relación con su agresor, bien por las presiones del propio ofensor o de su entorno, también por el miedo a las represalias que pueda tener tanto hacia ella como hacia sus familiares más allegados e incluso el propio entorno familiar de la mujer que es sujeto pasivo del delito influye negativamente en la voluntad de continuación del proceso[16].

[16] M.J. CALA CARRILLO (dir.), *La renuncia a continuar en el procedimiento judicial en mujeres víctimas de violencia de género: Un estudio en la Comunidad Autónoma* An-

El mecanismo empleado por la víctima para lograr la absolución del sujeto activo del delito, será acogerse a la dispensa del art. 416 LECRIM, que prevé, como bien sabemos, una dispensa a la obligación de declarar que tienen todos los y las testigos, en los supuestos en los que el autor del delito sea ascendiente, descendente, cónyuge o que tenga o haya tenido una relación equivalente al matrimonio (relación de noviazgo o unión de hecho), sin la declaración de la víctima en el juicio oral, no habrá prueba de cargo y, por tanto, se tendrá que absolver al agresor por falta de pruebas.

En torno a este precepto, ha existido una jurisprudencia muy cambiante en el ámbito de la violencia de género, siendo la última postura doctrinal establecida en por la Sala Segunda del Tribunal Supremo, n. 389/2020, de 10 de julio, rec. 3884/2018 en la que se manifiesta que la dispensa del art. 416 LECRIM es un derecho del testigo, no del acusado, que dimana de las garantías del art. 24 de la Constitución Española (CE) y tiene su razón de ser en la voluntad de proteger los vínculos de solidaridad entre testigo y acusado y las relaciones familiares proclamadas en el art. 39 CE, protegiendo así la intimidad en el ámbito familiar. No obstante, y este es el punto importante, matizó que en los casos en que este testigo (que tiene derecho a no declarar) es también la víctima del delito y ésta haya formulado denuncia, no regirá tal dispensa, especialmente cuando el/la testigo esté personado o personada como acusación particular. De hecho, incluso si abandona esta posición, seguirá sin recobrar este derecho a no declarar.

Dicha postura doctrinal fue introducida en la LECRIM mediante la Ley Orgánica 8/2021, de 4 de junio, reformando el citado art. 416 LECRIM. Con esta modificación el primer apartado del artículo incluye cinco excepciones en las cuales no habrá dispensa de la obligación de declarar, siendo la cuarta y la quinta los supuestos expresamente previstos por el Tribunal Supremo que ahora mencionábamos. Es decir, no tendrán dispensa de declarar ni el testigo o la testigo que esté o haya estado personado como acusación particular, ni el testigo o la testigo que haya declarado ya durante el procedimiento a pesar de haber sido informado que tenía derecho a no hacerlo[17], es decir, con la de-

daluza, Instituto Andaluz de la Mujer, Sevilla, 2012.

[17] En este sentido, la sentencia del Tribunal Supremo, n. 656/2022, de 29 de ju-

nuncia y su ratificación, aunque no se haya personado como acusación particular, la víctima no puede acogerse a dicha dispensa.

De esta forma el Tribunal Supremo, viene a poner orden en una cuestión que se daba habitualmente en los procedimientos judiciales, a saber, las presiones por parte del entorno del maltratador, para que la mujer dejara de ejercer la acusación particular y de este modo el día de la Vista acogerse a su dispensa de no declarar, por lo que, sin su declaración, aunque existieran como se ha comentado anteriormente, otras pruebas que acreditarían la agresión, como un parte de lesiones, no habría posibilidad de prueba de cargo al no poder conectar la lesión con su autor.

Y este problema lo seguiremos manteniendo en la prueba en materia de violencia digital, pues habrá evidencias que demuestren la agresión pero que necesitarán ser confirmadas por la víctima para obtener una prueba de cargo suficiente enervadora de la presunción de inocencia con base tanto en prueba testifical -la de la víctima- como en prueba indiciaria, pues no debemos olvidar, como nos indica nuestro Alto Tribunal[18], que las víctimas de violencia contra la mujer no son un mero testigo, son un testigo cualificado, la víctima, no es tan solo la persona que "ha visto" un hecho y puede testificar sobre él, sino que es quien ha visto y ha sufrido la actuación ilícita del sujeto activo del delito, por lo que su categorización probatoria está en un grado mayor que el mero testigo ajeno y externo al hecho[19].

nio, rec. n. 2111/2020 ha mantenido que en los casos de víctima constituida como acusación particular es indiferente que en el momento de declarar se mantenga el vínculo matrimonial. Incluso, la sentencia del Tribunal Supremo n. 927/2022, de 30 de noviembre, rec. n. 10018/2022 ha establecido que cuando es el testigo quién por iniciativa propia se dirige a las dependencias policiales o al órgano judicial con el propósito de interponer la denuncia, el testigo no tendrá que ser prevenido de esta dispensa, pues según el Tribunal, este testigo ya ha resuelto el conflicto de intereses a favor de interponer la denuncia. Diferente será en los casos en que sea la autoridad judicial la que requiera al testigo para comparecer a declarar, ya que, en estos supuestos, el testigo sí que deberá ser advertido.

[18] Cfr. por todas, la sentencia del Tribunal Supremo, Sala de lo Penal, sentencia n. 282/2018, de 13 de junio, rec. 10776/2017.

[19] La Sala de lo Penal de nuestro Alto Tribunal, ha venido considerando que la declaración de la víctima pueda servir como única prueba de cargo, siempre y cuando se cumplan una serie de requisitos (cfr. por todas, sentencia del Tribunal Supremo,

4. *La problemática de la prueba de la violencia de género con empleo de TIC*

La irrupción de las tecnologías en nuestra sociedad, estableciéndose nuevas formas de comunicación unidireccionales y bidireccionales, traen consigo la necesaria adopción de nuevas formas de prueba judicial diferentes a las tradicionales.

Las comunicaciones electrónicas y/o digitales pueden ser el instrumento de la comisión de conductas que deben tener relevancia penal y que no han de quedar impunes, con el problema añadido del acelerado avance tecnológico en dichas comunicaciones, perfeccionándolas o creando nuevas formas de comunicación que dificultan la elaboración de respuestas jurídicas y procesales a las cuestiones probatorias que se pueden suscitar.

De este modo, hay que analizar el valor probatorio de las citadas

Sala de lo Penal, n. 546/2008, de 23 de septiembre, rec. 2569/2007): (i) ausencia de incredibilidad subjetiva derivada de las previas relaciones acusado-víctima que pongan de relieve un posible móvil espurio o de venganza que pueda enturbiar la sinceridad del testimonio; (ii) verosimilitud del testimonio, que ha de estar corroborado por otros datos objetivos obrantes en el proceso; (iii) persistencia en la incriminación, que ha de ser prolongada en el tiempo, reiteradamente expresada y expuesta sin ambigüedades o contradicciones en lo fundamental. Algunos autores, consideran que sería interesante introducir en el procedimiento herramientas basadas en inteligencia artificial, a través de los llamados "potenciales evocados", que no poseen naturaleza invasiva y que, a través del estudio de la actividad eléctrica neuronal de la persona conectada, comprueban el funcionamiento de determinados estímulos visuales, táctiles, auditivos, cerebrales etc., a los efectos de poder determinar si la persona que está declarando como investigada está contestando verazmente a las preguntas que se le formulan (E. VELASCO NÚÑEZ, *Inteligencia artificial: aspectos penales y procesales*, en A.J. PÉREZ-CRUZ MARTÍN, S. CALAZA LÓPEZ (dirs.) *Desafíos del Derecho Procesal del siglo XXI: Prueba prohibida, inteligencia artificial y digitalización de la Administración de Justicia*, Madrid, 2024, p. 178), lo que permitiría emplear esta valoración objetiva llevada a cabo por inteligencia artificial y no con base en el criterio de un Juez o de una Jueza a través del principio de inmediación, como elemento corroborador de la declaración de la víctima para que ésta sirva como prueba de cargo. No debemos olvidar que la Inteligencia Artificial, como apunta Segarra, ha demostrado ser una herramienta versátil y poderosa capaz de analizar grandes volúmenes de datos en tiempo real, proporcionando un conocimiento valioso en la toma de decisiones (R. SEGARRA, *IA en Ciberseguridad*, en *Guía básica de la IA*, Smart Digital, Madrid, 2024, p. 167).

comunicaciones electrónicas, en el sentido de determinar qué deben aportar las partes al proceso para valorar el contenido de dichas comunicaciones electrónicas y qué es lo que debe o puede valorar el juez o la jueza encargados de la instrucción y, en su caso, del posterior enjuiciamiento, teniendo en cuenta que según los diferentes supuestos a considerar en cada caso, la incorporación como prueba del contenido de la concreta comunicación electrónica así como de la persona responsable de la misma que la emitió con ánimo de menoscabar la integridad física o psicológica de la víctima – bienes jurídicos afectados en el ámbito de la violencia contra la mujer –, pueden quebrantar, no sólo al derecho al secreto de las comunicaciones (art. 18.3 CE), sino también los derechos al honor a la intimidad personal y a la propia imagen (art. 18.1 CE), e incluso al derecho a la protección de datos personales (art. 18.4 CE)"[20].

Con independencia del mecanismo o sistema de comunicación utilizado, realizado el proceso comunicador (sea por WhatsApp, Instagram, Facebook, X-Twitter, correo electrónico, etc.) éste puede haber sido utilizado con fines intimidatorios, insultantes, injuriosos o agresivos exteriorizando conductas susceptibles de la comisión de algún hecho delictivo y la exteriorización de tales actitudes presuntamente delictivas, habrá que introducirlas en el proceso con el fin de comprobar si pueden tener valor probatorio y, en tal caso, se debe determinar qué valor probatorio podrán alcanzar, por lo que se hace imprescindible traer al ámbito tecnológico la distinción clásica entre fuentes y medios de prueba[21].

De este modo, la fuente de prueba vendrá constituida por la información que se transmite por estos medios o dispositivos electrónicos – el contenido de los mensajes en redes sociales, la publicación de fotografías en blogs, la información obtenida por un geolocalizador de seguimiento –, el medio de prueba será el mecanismo procesal específicamente habilitado por el ordenamiento para introducir válidamente y con todas las garantías, sin vulneración derecho fundamental alguno, dicha información en el proceso[22].

[20] Tribunal Constitucional, sentencia n. 5/2013, de 9 de mayo, rec. 1246/2011.

[21] O. FUENTES SORIANO, *op. cit.*, p. 18.

[22] S. BARONA VILAR, *Proceso penal: Derecho Procesal III*, Valencia, 2024, p. 442.

En el informe de GREVIO referente a España del año 2024[23], dicho Grupo de Expertos concluyó que se deben redoblar los esfuerzos para garantizar la aplicación práctica de medidas preventivas sobre todas las formas de violencia contra las mujeres, incluida la violencia sexual, la mutilación genital femenina, el matrimonio forzado, la violencia en nombre del llamado honor y cualquier manifestación digital de violencia contra las mujeres, implicando en dichos esfuerzos a las organizaciones especializadas en los derechos de las mujeres[24].

Aunque ya se ha superado la anomia situada en nuestro ordenamiento procesal penal ante la inexistencia de regulación de los mecanismos de introducción en el proceso de las fuentes de prueba tecnológicas[25], gracias a la reforma operada por Ley Orgánica n. 13/2015, de 5 de octubre de la Ley de Enjuiciamiento Criminal, introduciendo medidas de investigación tecnológica[26], disponemos de formas de in-

Sin olvidar que nos movemos en la delgada línea que separa la lícita voluntad de recopilar información que acredite una conducta delictiva y el respeto a la protección de los derechos fundamentales de la persona investigada, mediante instrumentos de prueba lícita, así como el derecho a la presunción de inocencia y al debido proceso. J. PICÓ I JUNY, *Retos del derecho probatorio ante las nuevas tecnologías*, en S. CALAZA LÓPEZ, M. LLORENTE SÁNCHEZ-ARJONA (dirs.), *Inteligencia artificial legal y administración de justicia*, Pamplona, 2022, p. 443.

[23] Para el seguimiento de los compromisos adquiridos con la ratificación del Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, hecho en Estambul el 11 de mayo de 2011, se creó un Grupo de expertos en la lucha contra la violencia contra la mujer y la violencia doméstica (GREVIO), integrado por un mínimo de 10 y un máximo de 15 miembros de países diferentes (información disponible en: https://violenciagenero.igualdad.gob.es/marco-internacional/ambito-internacional/consejo-europa/grevio/, fecha de consulta: 9 de enero de 2025).

[24] Informe disponible en: https://violenciagenero.igualdad.gob.es/wp-content/uploads/GREVIO202411_First-thematic-evaluation-report_Spain_ES.pdf (fecha de consulta: 9 de enero de 2025).

[25] La problemática de la falta de regulación de la introducción de determinadas fuentes de prueba en el proceso penal, como, por ejemplo, la información obtenida a través de la interceptación de las comunicaciones, ha sido objeto de fuertes críticas por parte del Tribunal Supremo (cfr. por todas las sentencias del Tribunal Supremo, Sala de lo Penal, n. 487/2007, de 29 de mayo, rec. 2234/2006 o n. 363/2008, de 23 de junio, rec. 2135/2007, entre otras muchas).

[26] Siguiendo a Fuentes Soriano, de forma muy sintética, las novedades introduci-

troducción de las fuentes de prueba de las comunicaciones electrónicas, a los efectos de valorar como prueba las conductas penales cometidas a través de medios y entornos electrónicos y/o digitales.

Por ello, será preciso un sistema judicial que entienda la trascendencia de la prueba electrónica[27], que esté comprometido en la persecución del delito, sin recelo alguno al empleo de medios tecnológicos en la introducción en el proceso de fuentes de prueba tecnológicas.

5. *La prueba de la violencia de género digital: ilícitos penales cometidos a través de comunicaciones instantáneas bidireccionales o multidireccionales*

A los efectos de generar prueba de la violencia de género digital, será necesario reconocer la fuente de dónde propone la prueba, con el objetivo de poder comprobar su autenticidad e identificar los elementos que puedan cuestionar su validez, dicha fuente de prueba será incorporada al proceso a través de los medios de prueba documental y pericial.

Por ello, si la comunicación que se desea transmitir se encuentra o ha estado alojada en una página web – por ejemplo, un blog –, habrá que acudir a herramientas que certifiquen de forma fehaciente su contenido – actas notariales, pericial tecnológica o programas de testigo en línea[28].

das por esta reforma se podían resumir en las siguientes: (i) el reconocimiento de las exigencias constitucionales para la válida interceptación de las comunicaciones, con constancia expresa de sus correspondientes excepciones y matices; (ii) la regulación de los hallazgos casuales; y (iii) la regulación de nuevas diligencias de investigación tecnológica que suponen, en la práctica totalidad de los casos, nuevas formas de intervención tecnológica de comunicaciones. O. FUENTES SORIANO, *Comunicaciones telemáticas: práctica y valoración de la prueba*, en O. FUENTES SORIANO (coord.), *El proceso penal. Cuestiones fundamentales,* Valencia, 2017, p. 257.

[27] B. ROMO SABANDO, *La prueba digital en violencia de género*, en E. CERRATO GURI (dir.), *La prueba de la violencia de género y su problemática judicial*, Madrid, p. 286.

[28] P. ARRABAL PLATERO, *La prueba tecnológica: aportación, práctica y valoración*, Valencia, 2020, p. 398. Es importante tener presente que "la fe notarial acreditará, en su caso, la fiel coincidencia del documento aportado con aquél que al Notario se le

Si el contenido se halla en un correo electrónico, en chats de WhatsApp u otras plataformas de mensajería instantánea, se tendrá que acudir a herramientas para certificar su contenido – cotejo del Letrado o la Letrada de la Administración de Justicia – y para descartar posibles manipulaciones – pericial tecnológica.

Si la fuente de prueba se encuentra en un equipo informático, habrá que realizar un clonado del disco duro, no una copia[29].

Si la comunicación electrónica viene referida a audios, vídeos o imágenes – fotografías esencialmente –, habrá que analizar los metadatos de dichos archivos, comprobar su fecha, hora y lugar de envío o recepción y, en la medida que los metadatos pueden ser alterados por la persona usuaria del terminal, habrá que comprobar la coherencia de los mismos y descartar manipulaciones a través de pericial informática[30].

Si, finalmente, el contenido se encuentra en el metaverso[31], bien

mostró en pantalla, pero en modo alguno la originalidad, veracidad e integridad de este último" (O. FUENTES SORIANO, *El valor probatorio de los correos electrónicos*, en J.M. ASENCIO MELLADO (dir.) *Justicia penal y nuevas formas de delincuencia*, Valencia, 2017, p. 202), por lo que será necesario en caso de impugnación llevar a cabo prueba pericial tecnológica.

[29] Una vez que se ha procedido a la adquisición de cualquier evidencia digital, es muy importante la preservación de las mismas, de ahí que cualquier informe forense que se precie debe contener una descripción detallada de las herramientas y procesos utilizados en el análisis de la prueba, una de las herramientas que se empleará será un clonado de un disco duro (proceso por el cual se hace una copia idéntica del disco duro, sobre la que siempre se trabajará y no sobre el original). Información disponible en: https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/pericia-informatica/ (fecha de consulta: 9 de enero de 2025).

[30] M.C. STAMM, K.J. RAY LIU, *Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints*, en *IEEE Transactions on information forensics and security*, 2010, n. 3, pp. 492-506.

[31] La delincuencia en el metaverso es una realidad, dentro de los delitos más comunes en violencia de género nos encontramos con la vulneración de la reputación de una persona a través de falsificaciones que emplean *softwares* que manipulan los rasgos de una persona, generan o intercambian rostros o se recrean voces (*deepfakes*), otras veces con falsificaciones más superficiales con herramientas de edición más básicas (*shallowfakes*), creando material pornográfico (porno de venganza o *revenge porn*) o llevando a cabo actitudes de ciberacoso, por ejemplo, desde Meta – perteneciente a la compañía norteamericana de Facebook –, se denunció públicamente que a comien-

en versión de realidad aumentada, bien en versión de realidad virtual, habrá que atender a las características específicas de cada uno de ellos para analizar si existen registros de interacciones o de creación de contenidos, pudiendo valorar en su momento, debido a la reciente creación de los mismos, la implantación de un registro de terceros de confianza externo o propio[32].

A continuación, se va a exponer la forma de incorporar la fuente de prueba de las comunicaciones electrónicas más conocidas para cometer violencia digital a través de los oportunos medios de prueba[33], así como los problemas de valoración a los efectos de lograr obtener una prueba de cargo suficiente para desvirtuar la presunción de inocencia en la violencia de género de carácter digital.

Actualmente, no podemos concebir nuestras vidas sin las comunicaciones a través de chats, bien por medio de programas de mensajería instantánea como WhatsApp o Telegram, bien a través de chats integrados en redes sociales como Facebook, Instagram, TikTok o Tinder, dónde entablaremos conversaciones de texto o remitiremos, fotografías, audios o vídeos, lo que convierte a dichos mecanismos de comunicación como medios idóneos para cometer actos de violencia y, muy especialmente, actos de violencia contra la mujer por razones discriminatorias de género.

Así, por ejemplo, podemos encontrar mensajes de WhatsApp en los que se insulte a la expareja, o se reconozca la comisión de un hecho

zos del 2022, algunos avatares femeninos eran contactados para abusar de ellos sexualmente (ver: https://www.bbc.com/mundo/noticias-60282549, fecha de consulta: 9 de enero de 2025), teniendo siempre en cuenta que las agresiones vividas por los avatares pueden producir secuelas similares a las que ocurren en el mundo real. (S. VERDUGO GUZMÁN, *Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos*, Valencia, 2023, pp. 174-175).

[32] B. ROMO SABANDO, *op. cit*, p. 287.

[33] Siguiendo a Perrino Pérez, se puede concluir que los ciberdelitos que más se cometen en el ámbito de la violencia de género digital son las amenazas, el acoso, violencia sexual, corrupción de menores, descubrimiento y revelación de secretos, calumnias e injurias, difusión a terceros de imágenes o grabaciones audiovisuales no consentidas, delitos de odio, todos ellos a través de canales de comunicación como programas de mensajería instantánea, webs, blogs o aplicaciones de redes sociales (A. L. PERRINO PÉREZ, *El Derecho penal y las nuevas tecnologías: aspectos sustantivos y procesales de la ciberdelincuenca*, CUNIEP, Córdoba, 2024).

delictivo, por ejemplo, pedir perdón a la mujer maltratada por el golpe propinado el día anterior, también se podrán emplear estas herramientas como mecanismos de acoso, al remitir cientos de mensajes a la mujer acosada que perturba su paz y bienestar o, se podrán utilizar las redes sociales como mecanismos de captación de trata de seres humanos con fines de explotación sexual.

5.1. *Los contenidos de mensajes de WhatsApp o en plataformas similares como medio de prueba*

En el ámbito de la violencia contra la mujer, las conversaciones de WhatsApp o de Telegram, son una prueba esencial en el procedimiento, tendente a erigirse como un elemento periférico corroborador de la declaración de la víctima como prueba de cargo.

La sensación de anonimato que producen estos chats, conduce a que los agresores tiendan a remitir mensajes humillantes, denigrantes, amenazantes, coaccionadores o vejatorios a través de estas aplicaciones móvil, incluso tienden a pedir perdón a sus víctimas por episodios de violencia pasados, los que los convierte en una fuente de prueba esencial para desvirtuar la presunción de inocencia de los agresores.

Proponer como medio de prueba el contenido de un mensaje de WhatsApp, o de cualquier otro sistema de mensajería instantánea, es lo mismo que proponer como prueba un mensaje de correo electrónico, o la grabación de una conversación telefónica. Estamos ante medios de reproducción de la palabra, la imagen y el sonido, y nos encontramos en todos los casos ante medios de prueba electrónica que se componen del soporte material, el teléfono smartphone, de la información que contiene el soporte, y de su posible relevancia jurídica[34].

Es evidente que, para que el contenido de estos mensajes sea admitido como prueba en el proceso, han de haberse obtenido de forma lícita[35]. La forma de introducirse estos mensajes será normalmente por medio de copia en papel, en caso de conversaciones de texto, o por

[34] Audiencia Provincial de Valencia, Sección 4ª, sentencia n. 276/2017, de 25 de abril, rec. 28/2017.

[35] Sentencia del Tribunal Supremo, Sala Tercera de lo Contencioso-Administrativo, n. 375/20218, de 19 de julio, rec. 2918/2016.

medio de CDs o pendrives, en caso de audios, fotografías o vídeos. Posteriormente se llevará a cabo una diligencia de cotejo por el letrado o letrada de la Administración de Justicia – al poseer fe pública judicial – del teléfono móvil de la víctima dónde se identificará el número de teléfono desde el que fueron remitidos los chats, vídeos, fotografías o audios, con identificación del día y la hora de recepción de estas comunicaciones.

Por parte del acusado, nos podemos encontrar con dos estrategias de defensa frente a la evidencia delictiva que se desprende de estas comunicaciones.

La primera, manifestar que no es la persona titular de la línea que figuran en las comunicaciones y, por tanto, que él no las remitió. En este caso, se podrá consultar directamente en la web de la Comisión Nacional de los Mercados y la Competencia a qué concreto operador jurídico pertenece dicha línea[36], o bien se podrá oficiar por el juez, la jueza, magistrado o magistrada que se encargue de la instrucción a dicho Organismo para que remita esa información a autos y con esa información se remitirá oficio a la concreta compañía a los efectos de que indique quién es el usuario o abonado que emplea dicha línea telefónica, pues existe una obligación por parte de las compañías que operan en nuestro país de identificar y conservar los datos de la persona usuaria o abonada de las líneas de telefonía fija y móvil que comercializan (art. 3 Ley n. 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones)[37].

La segunda actitud de defensa puede consistir en negar la veracidad de los mensajes aportados al procedimiento como prueba.

Hay que tener en cuenta que existen programas que permiten manipular o editar conversaciones de mensajerías instantáneas o incluso crear conversaciones ficticias, como, por ejemplo, WhatsApp Tool-

[36] A través de este enlace se pueden consultar públicamente a qué concreta compañía pertenece una determinada línea móvil o de teléfono fijo: https://numeracionyoperadores.cnmc.es/portabilidad/movil (fecha de consulta: 9 de enero de 2025).

[37] Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, de 18 de octubre, en BOE 251 de 19 de octubre de 2007.

box, Fake SMS Sender, SQLite Editor, entre otras, de muy fácil acceso para cualquier persona usuaria de internet y sin necesidad de poseer conocimientos técnicos específicos.

De ahí que nuestro Alto Tribunal, iniciara una doctrina jurisprudencial por medio de la sentencia del Tribunal Supremo, Sala de lo Penal, n. 300/2015, de 19 de mayo, rec. 2387/2014, en la que señala que la prueba de una comunicación bidireccional mediante cualquier sistema de mensajería instantánea debe ser abordada con mucha cautela, por lo que, en caso de impugnación de la autenticidad de cualquiera de estas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria, por lo que será en este caso indispensable la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y en definitiva, la integridad de su contenido.

La particularidad de los mensajes remitidos por plataformas como WhatsApp o Telegram, aparte de transmitir información de forma bidireccional o multidireccional, es que no son almacenados en un servidor externo[38], pues con el objetivo de preservar la privacidad de los usuarios o usuarias, es política de estas plataformas, no almacenar ningún mensaje ni multimedia en sus servidores online, por ello, los datos cifrados se pueden guardar en el teléfono localmente o en un almacenamiento externo, como un disco duro en una computadora o un servicio en la nube[39].

Por tanto, si se impugna la autenticidad de estos mensajes, habrá que llevar a cabo prueba pericial de carácter informática, que acredite que los datos almacenados en el teléfono local en el que se recibieron las comunicaciones objeto de prueba, no han sido manipulados por la persona usuaria de dicho teléfono, ello, sin necesidad de tener que acceder al terminal del agresor desde el que salieron las comunicaciones, con el añadido que, existen modernas herramientas que permiten re-

[38] J.L. RODRÍGUEZ LAINZ, *Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (a propósito de la STS, Sala II, 300/2015, de 19 de mayo)*, en *Diario la Ley*, 2015, n. 8569, pp. 6-7.

[39] Disponible en: https://www.adslzone.net/esenciales/whatsapp/carpeta-copias-seguridad/ (fecha de consulta: 9 de enero de 2024).

cuperar mensajes que fueron borrados por las víctimas y que corroborarían el delito que han denunciado[40].

El método más eficiente es el de la extracción física del terminal, aunque es un método invasivo, lo cierto es que permite asegurar al perito o la perito que lleva a cabo su dictamen, afirmar sin ningún género de duda que los mensajes de WhatsApp o remitidos a través de cualquier otra aplicación de mensajería instantánea no han sido manipulados y, por tanto, son auténticos; incluso a través de este método, como se ha comentado anteriormente, se pueden recuperar mensajes que hayan sido borrados recientemente del terminal[41], pues, aunque nos resulte increíble y sorprendente, muchas víctimas eliminan las conversaciones hirientes o humillantes, como mecanismo de autodefensa de su integridad moral.

De conformidad con la doctrina iniciada en la sentencia del Tribunal Supremo, Sala de lo Penal, n. 300/2015, de 19 de mayo, rec. 2387/2014, si el investigado-acusado, impugna en tiempo y forma la autenticidad de las comunicaciones remitidas por vía WhatsApp o programa similar, la parte acusadora deberá probar que dichas comunicaciones son auténticas y no han sido manipuladas o creadas *ex professo* para el procedimiento.

En la sentencia del Tribunal Supremo, Sala de lo Penal, n. 32/2019 de 27 junio, rec. 10732/2018, valida la aportación al proceso de este tipo de pruebas digitales mediante acta notarial, o adveración de teléfonos móviles y sus contenidos ante el letrado de la Administración de Justicia, o meros pantallazos como fotografías de un "hilo" de mensajes de WhatsApp, si bien, indica que en los casos en los que la defensa impugne esta "prueba digital" en el escrito de defensa, motiva y obliga a la acusación a proponer prueba pericial informática acerca de la veracidad del contenido de estos mensajes y que estos no han sido alterados, sin que sea necesario que esta impugnación se haga en la

[40] C. COSCOLLANO, *Análisis forense en dispositivos móviles*, en *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, 2019, n. 84, pp. 54-56.

[41] Sobre los diferentes métodos de análisis de forense de los terminales móviles véase: https://www.redseguridad.com/especialidades-tic/activos-de-informacion/ investigacion-forense-de-dispositivos-moviles-metodologias-y-herramientas_20201021.html (fecha de consulta: 9 de enero de 2025).

fase de instrucción, pues es lícito y legítimo efectuar la impugnación en la fase propia de la calificación provisional debiendo contrarrestar la acusación esta impugnación por la oportuna pericial informática.

Sin embargo, hubo un cambio de doctrina en la sentencia del Tribunal Supremo, Sala de lo Penal, n. 744/2022, de 21 de julio, rec. 4877/2020, en la que se estableció que el acusado, al impugnar las conversaciones tanto de WhatsApp como de SMS que sirvieron de prueba de cargo para condenarle por un delito de amenazas a su expareja, debió acreditar él que, efectivamente, estábamos ante una prueba falsa a través de la correspondiente pericial, es decir, hay una inversión de la carga de la prueba en estos casos, no debiendo recaer en la parte acusadora sino en la parte impugnante de los mensajes.

Con todo, a pesar de este cambio doctrinal, si se impugnan los citados mensajes en cuanto a su autenticidad, será conveniente realizar la citada pericial informática, a los efectos de evitar interpretaciones garantistas que consideren que la parte acusada no ha de probar nada y que ha de ser la parte acusadora la que acredite la existencia y veracidad de dichos mensajes.

Sin embargo, en caso de impugnación de la autenticidad de dichas comunicaciones, nos podemos encontrar con dos situaciones problemáticas, que hay que tratar de anticipar.

En primer lugar, el momento procesal de la impugnación puede generar que no exista capacidad de reacción a los efectos de presentar una pericial informática. Si la parte acusada no reconoce expresamente los mensajes durante la fase de instrucción y llegado el trámite de calificación provisional, en su escrito de defensa impugna la autenticidad de dichos mensajes, la prueba se debe proponer en el escrito de acusación, por tanto, si no se ha dicho nada y se impugnan los mensajes en el escrito de defensa, es posible que no dispongamos de un trámite para solicitar dicha prueba.

En el procedimiento abreviado, se podría aportar prueba el mismo día de la Vista por la acusación particular, como cuestión previa, encargando un dictamen pericial de parte y gestionando la propia parte la citación al perito encargado de la elaboración del informe para que acuda al juicio (art. 786.2 LECRIM).

En el ámbito del procedimiento ordinario, en lo que se refiere a la proposición de pruebas si acudimos al tenor literal de la Ley, el mo-

mento previsto está constituido por el escrito de conclusiones provisionales sin que exista previsión legal alguna de presentación o petición de prueba en un momento posterior a este trámite y antes del inicio del juicio oral (arts. 650 y 728 LECRIM). Con todo, nuestro Alto Tribunal abrió la posibilidad en su sentencia del Tribunal Supremo, Sala de lo Penal, n. 1060/2006, de 11 de octubre, rec. 10082/2006, a proponer y admitir prueba con posterioridad al correspondiente escrito de calificación provisional y de forma previa al inicio del juicio oral, en aquéllos supuestos en los que existan razones justificadas para ello y siempre que dicha proposición de prueba no suponga fraude procesal alguno ni tampoco constituya un obstáculo al principio de contradicción y de igualdad de partes, teniendo en cuenta que ha de tratarse de una prueba no conocida o no accesible en el momento de la calificación[42].

En definitiva, podemos pedir como prueba pericial informática judicial antes del juicio oral o aportar una pericial de parte, como consecuencia de la impugnación sorpresiva, pero legítima, de la parte acusada en su escrito de defensa, tanto si estamos en un procedimiento abreviado como en un procedimiento ordinario, si bien, estaremos en manos del órgano enjuiciador para admitir o no dicha prueba, lo cual es un riesgo, pues puede no admitir dicha prueba y después validar el argumento de la defensa de que no existe suficiente prueba de cargo para condenar, al haber impugnado la autenticidad de las comunicaciones.

Por ello, de cara a evitar esta incertidumbre, sería conveniente en la fase de instrucción, requerir a la persona investigada para que se pronuncie si reconoce o no dichos mensajes. Se puede hacer por vía de

[42] De hecho, la sentencia del Tribunal Supremo, Sala de lo Penal, n. 912/2016, de 1 de diciembre, rec. 355/2016, nos indica en cuanto a esta posibilidad de proponer prueba tras los escritos de conclusiones provisionales y antes de inicio del juicio oral en los procedimientos ordinarios que "en cuanto a la no admisión de planteamiento de cuestiones previas para alegar vulneraciones de derechos fundamentales y proponer nuevas pruebas en el sumario, debemos precisar que en orden a las exigencias temporales el proceso penal como todo proceso que se integra por una relación ordenada de fases aparece regido por el principio de preclusión, tal principio no tiene un fin en sí mismo, sino que tiene una naturaleza instrumental para permitir la sucesión de fases bajo los principios, entre otros, de igualdad e interdicción de la indefensión".

su interrogatorio, preguntándole expresamente por esta cuestión y si se acoge a su derecho a no declarar y, por tanto, no podríamos hacerle esta pregunta, se podría solicitar por vía de un requerimiento formal por parte del juez a instancias de la parte acusadora, a los efectos de que se pronunciase sobre la veracidad o no de dichos mensajes.

Existen dudas razonables acerca de la obligación o no de la persona investigada de cumplimentar este tipo de requerimientos, pues podría entroncar "con una de las manifestaciones del derecho a la presunción de inocencia: la que sitúa en la acusación la carga de la prueba; esta carga no se puede trocar fácticamente haciendo recaer en el imputado la obligación de aportar elementos de prueba que supongan una autoincriminación" (sentencia del Tribunal Constitucional, n. 161/1997, de 2 de octubre, rec. 4198/1996).

Ahora bien, tendríamos dos consecuencias jurídicas importantes en caso de que no cumplimentase el requerimiento.

La primera, la posibilidad de solicitar como prueba una pericial judicial o aportar una pericial de parte, con el objetivo de realizar una extracción física del terminal y dejar claro que no hubo manipulación.

La segunda, para el caso de que no se pueda practicar dicha pericial, las consecuencias del silencio de la persona investigada a la luz de la doctrina iniciada por el Tribunal Europeo de Derechos Humanos (TEDH), Gran Sala, sentencia de 8 de febrero de 1996, recurso n. 18731/1991, *Murray c. Reino Unido*, en la que se establece que, si bien el silencio no puede ser considerado en sí mismo como un indicio de culpabilidad, cuando los cargos de la acusación – corroborados por una sólida base probatoria – estén suficientemente acreditados, el Tribunal puede valorar la actitud silenciosa del acusado, señalando que "el Tribunal nacional no puede concluir la culpabilidad del acusado simplemente porque éste opte por guardar silencio. Es solamente cuando las pruebas de cargo requieren una explicación, que el acusado debería ser capaz de dar, cuando la ausencia de explicación puede permitir concluir, por un simple razonamiento de sentido común, que no existe ninguna explicación posible y que el acusado es culpable"[43].

[43] Cfr. por todas, Tribunal Constitucional, sentencia n. 202/2000, de 24 de julio, rec. n. 2409/1997 o Tribunal Supremo, Sala de lo Penal, sentencia n. 679/2013, de 25 de julio, rec. n. 10182/2013.

Por tanto, su silencio debe ser valorado con el resto de pruebas, en este caso los mensajes de teléfono cotejados y la declaración de la víctima, de forma que una mera impugnación no debería servir para invalidar dicha prueba, pues el investigado en fase de instrucción debió dar alguna explicación al respecto, máxime cuando se le requirió formalmente a ello.

La segunda problemática que nos encontramos viene referida a víctimas sin recursos para litigar, pues en caso de no aceptarse pericial judicial o no poder presentarse dicha pericial tras una impugnación por los escasos márgenes de tiempo para su petición y aprobación por el juzgado, no posee recursos económicos a los efectos de sufragar una pericial de parte. Por ello, se erige dentro del código de buenas prácticas de los letrados y letradas que asisten a este tipo de víctimas, vigilar y actuar con diligencia, anticipándose a posibles impugnaciones extemporáneas o sorpresivas por parte de los acusados de dichos mensajes, pues serán vitales para obtener prueba de cargo suficiente enervadora de la presunción de inocencia.

También será vital un cuidado extremo en el derecho a la información que reciben las víctimas, informándoles del derecho que les asiste a personarse como acusación particular y al beneficio de la justicia gratuita, pues para poder controlar y llevar a cabo correctamente esta prueba, será fundamental que la víctima esté personada en el procedimiento como acusación particular, pues el Ministerio Fiscal, dado el gran volumen de trabajo existente, estará prácticamente ausente en la fase de instrucción, por lo que el abogado o abogada dela víctima será quién mejor se encargue de guiar a Su Señoría en la proposición de diligencias, al tener acceso a toda la información de la víctima, diligencias que constituirán las futuras pruebas del juicio.

De hecho, tenemos ya alguna resolución judicial que declara la nulidad de una sentencia condenatoria en materia de violencia contra la mujer, devolviendo los autos a la fase de instrucción, por haberse acreditado que la víctima no fue informada de su derecho a constituirse como parte en el proceso penal y a solicitar asistencia jurídica gratuita, entendiéndose vulnerados los derechos de los arts. 3, 6, 16 del Estatuto de la Victima, en relación con el art. 24.2 CE[44].

[44] Ver, en este sentido, Tribunal Superior de Justicia de la Comunidad Valencia-

Todas estas cuestiones, las estamos planteando para el supuesto de que se pudiera producir una impugnación sorpresiva de la autenticidad de las comunicaciones en el escrito de defensa, pero hay que matizar, que en el caso de que la impugnación se produjera en el informe final de la defensa, una vez ya se ha practicado toda la prueba, dicha impugnación no tendría validez y, por tanto, las comunicaciones aportadas al proceso, si bien están sometidas el criterio de libre valoración de la prueba, con toda probabilidad al no existir ninguna impugnación válida por extemporal, su contenido, hará plena prueba de cargo[45].

5.2. *Ilícitos penales cometidos a través de webs o redes sociales*

En relación con las comunicaciones llevadas a cabo a través de redes sociales, como Facebook, Instagram, X-Twitter o en Blogs, podemos encontrarnos ante varias situaciones.

Un escenario, serían las comunicaciones que se hayan podido llevar a cabo por medio de los correspondientes chats existentes hoy en día en todas las redes sociales – Facebook, Instagram, TikTok, son los más empleados –, con un contenido similar al comentado anteriormente para mensajes de WhatsApp y aplicaciones similares (insultos, vejaciones, amenazas, reconocimiento de hechos delictivos, entre otros).

Otra situación que podemos encontrar es la publicación en el muro del perfil de una concreta persona en una red social o en el post de un blog, fotografías o vídeos en los que la víctima vea comprometida su intimidad y reputación – las conductas más comunes consisten en publicar fotos o vídeos de índole sexual sin autorización alguna –, audios o comentarios denigrantes, humillantes, vejatorios o con amenazas de algún mal – por ejemplo, amenaza de muerte.

Estos ilícitos son los que más problemas nos van a dar en determinadas situaciones a los efectos de poder acreditarlos.

na, Sala de lo Civil y Penal, Sección Apelación, sentencia n. 308/2021, de 9 de noviembre, rec. 323/2021.

[45] Cfr. en este sentido, entre otras, Audiencia Provincial de Badajoz, Sección Primera, sentencia n. 81/2023, de 13 de junio, rec. 65/2002.

5.2.1. Eliminación de las publicaciones en el momento de ser notificado el autor del delito la existencia una investigación penal: necesidad de acreditar el contenido web o de la red social antes de interponer la correspondiente denuncia

Antes de proceder a interponer la correspondiente denuncia penal o, en caso de actuarse de oficio por parte de las Autoridades tras descubrir un ilícito penal en red, es importante acreditar el contenido ante la posibilidad de que el mismo sea eliminado por el autor del delito.

Una forma de acreditar dicho contenido será mediante acta notarial o mediante pericial informática, pero debemos tener en cuenta que la información en la Red, circula y cambia con gran rapidez y puede desaparecer entre el descubrimiento y el encargo al notario o perito informático para buscar la evidencia digital.

Por ello, en estos casos, se muestran de una gran utilidad los servicios conocidos como "testigo online".

Los "prestadores de servicios electrónicos de confianza", que es el nombre oficial que recibe esta figura reconocida por el Ministerio de Industria y Turismo[46], actúan como un "tercero de confianza" que mediante desarrollos basados en firma digital acreditan con un *timestamp*, es decir, con un sello de tiempo, que un conjunto de datos existió en una fecha y hora concretas y que ninguno de estos datos ha sido modificado desde entonces. El mercado de estos "terceros de confianza" es cada vez más amplio y conviene acudir al listado oficial del Ministerio para comprobar qué empresas están cualificadas o no, una de las herramientas más populares existentes al respecto es e Garante[47], recomendada por organismos oficiales como la Guardia Civil o el Instituto Nacional de Ciberseguridad (INCIBE)[48], por su fiabi-

[46] Ver definición y listado en la página web del citado Ministerio, disponible en: https://sede.serviciosmin.gob.es/es-es/firmaelectronica/paginas/Prestadores-de-servicios-electronicos-de-confianza.aspx (fecha de consulta: 9 de enero de 2025).

[47] Servicio susceptible de consultarse en: https://www.egarante.com/ (fecha de consulta: 9 de enero de 2025).

[48] La Guardia Civil, llegó a implementar el programa eGarante en su portal de colaboración ciudadana "Colabora" a los efectos de poder de certificar los contenidos de una página web de la que quiera informar por contener algún tipo de contenido delictivo (información disponible en: https://www.defensa.com/espana/guardia-civil-

lidad y por contar con un servicio gratuito limitado para particulares[49].

Además de eGarante, disponemos de otras herramientas gratuitas como Waybak Machine[50], que permite acreditar el contenido de webs que ya no existen, muy útil si no hemos sido capaces de llegar a tiempo para garantizar su contenido mediante actas notariales, periciales tecnológicas o testigos en línea, pues la mayoría de páginas web se actualizan de forma diaria y esta información en red se pierde con una gran facilidad.

La jurisprudencia ha venido abalando como prueba informes del portal Wayback Machine[51], en la medida que nos permite viajar al pasado en la red y acceder al contenido de un dominio web en una fecha y hora concretas.

Con estas herramientas gratuitas, disponibles a nuestro alcance, podemos certificar de forma eficaz el contenido de una web en un momento determinado y, por tanto, la existencia del ilícito penal publicado en dicha web.

espanola-presenta-nueva-herramienta-egarante-para (fecha de consulta: 9 de enero de 2025). Sobre las recomendaciones de INCIBE acerce del empleo de eGarante ver: https://www.incibe.es/ciudadania/blog/testigos-online-y-obtencion-de-pruebas-te-explicamos-su-utilidad (fecha de consulta: 9 de enero de 2025).

[49] Sobre el empleo de testigos en línea para acreditar el acoso ver: https://www.xataka.com/legislacion-y-derechos/egarante-asi-actua-testigo-online-frente-al-acoso-ataques-red (fecha de consulta: 9 de enero de 2025).

[50] Wayback Machine es una herramienta gratuita gestionada por una organización estadounidense sin ánimo de lucro, a saber, Internet Archive, dedicada a la preservación de archivos digitales, recopilando toda la información digital posible, incluidos los sitios webs, que nos permite viajar al pasado en la red y acceder al contenido de un dominio web en una fecha y hora concretas. Esta herramienta gratuita la podemos localizar en: https://web.archive.org/ (fecha de consulta: 9 de enero de 2025).

[51] Ver, en este sentido, Audiencia Provincial de Zaragoza, Sección 5ª, sentencia n. 450/2019, de 31 mayo, rec. 763/2018; Audiencia Provincial de Barcelona, Sección 15ª, sentencia n. 156/2018, de 12 marzo, rec. 397/2017 o Audiencia Provincial de Guipúzcoa, Sección 1ª, sentencia de 16 de junio de 2022, rec. 1087/2016.

5.2.2. Acreditación tras impugnación del contenido de la web, o de la concreta publicación o de la titularidad de la cuenta: la problemática de las comisiones rogatorias y el riesgo de prescripción delictiva

En redes sociales, a diferencia de programas de mensajería instantánea como WhatsApp o similares, el almacenamiento de los datos sí se guardan en sus servidores y se mantienen según estas compañías, como Facebook o Instagram, durante un período de 90 días en caso de eliminarse[52].

Por tanto, en caso de impugnación del contenido de la comunicación efectuada a través de redes sociales, se podrá requerir a estas compañías para que aporten a autos el concreto contenido publicado y, de esta forma, acreditar que el contenido es auténtico. También se les podrá solicitar, en caso de negar que sean estas personas las titulares y/o usuarias de los concretos perfiles a través de los que se cometió el delito, su identificación.

Sin embargo, nos topamos con la problemática de la sede social de estas compañías, pues la mayoría se encuentran en Estados Unidos, motivo por el que habrá que solicitar una comisión rogatoria, requiriendo el auxilio judicial de dicho país, lo que hace prácticamente inviable cumplir con el objetivo de dicha comisión rogatoria, pues a pesar de la perseverancia en los requerimientos de los juzgados españoles para su cumplimiento, suelen resultar infructuosos y, por tanto, prácticamente imposible la obtención de esta información por este medio[53].

Hay que tener en cuenta que, mientras se está intentado llevar a cabo dicha comisión rogatoria, el plazo de prescripción del delito, aunque se haya incoado un proceso penal por esos hechos, sigue corriendo[54].

[52] Información disponible en: https://www.facebook.com/help/instagram/494561080557017/?locale=es_LA (fecha de consulta: 9 de enero de 2025).

[53] Ver en este sentido Auto Juzgado Central de Instrucción, de 29 de marzo de 2016, rec. 4/2015.

[54] Sobre la importancia de la observancia de los plazos para no incurrir en absolución por prescripción del delito, véase J. PÉREZ GIL, *Respuesta judicial frente a la corrupción: Reflexiones recientes con vistas al futuro*, en *Revista General de Derecho Pro-*

Como nos dice el Tribunal Supremo, queda fuera de dudas que cuando se trata de un procedimiento ya iniciado, para entender que éste se dirige contra el culpable interrumpiendo el plazo de prescripción, se ha de exigir una actuación procesal de contenido sustancial, que signifique la iniciación o la continuación de las actuaciones judiciales encaminadas a la averiguación de unos determinados hechos, contra una o varias personas identificadas, total o parcialmente, aunque siempre de forma mínimamente suficiente, a las que se considere responsables de aquellos[55]. Las resoluciones o diligencias que se practiquen en una causa, para tener virtualidad interruptora, han de poseer un contenido sustancial propio de la puesta en marcha y prosecución del procedimiento demostrativas de que la investigación o tramitación avanza y progresa, consumiéndose las sucesivas etapas previstas por la ley o que demanden principios constitucionales o normas con influencia en derechos fundamentales de naturaleza procesal, superando la inactividad y la paralización[56].

En este sentido, la resolución que acuerde la práctica de la comisión rogatoria, interrumpirá el plazo de prescripción del delito, ahora bien, si tras dicha resolución no se lleva a cabo ninguna diligencia más de investigación, las meras resoluciones de trámite recordando al órgano de destino la petición de la comisión y su cumplimentación, no tendrán efectos interruptivos. Por ello, si estamos, por ejemplo, ante un delito leve que prescribe al año o un delito menos grave que prescribe a los 5 años, si desde la última actuación procesal que tenga efecto interruptivo, no se ha llevado a cabo otra actuación procesal que posea dicho efecto, comenzará a computarse de nuevo el plazo de prescripción desde dicha última actuación procesal, por lo que el delito puede prescribir si nos obcecamos en tratar de cumplir con la citada comisión rogatoria y con ello se extinguiría la responsabilidad penal de conformidad con lo dispuesto en el art. 130.1.6º CP[57] o bien, se po-

cesal, 2016, n. 40.

[55] Cfr. por todas, Tribunal Supremo, Sala de lo Penal, sentencia n. 312/2005, 9 de marzo, rec. 1349/2004.

[56] Tribunal Supremo, Sala de lo Penal, sentencias n. 149/2009, 24 de febrero, rec. 155/2008; n. 975/2012, de 5 de noviembre, rec. 10761/2012 o n. 177/2022, 24 de febrero, rec. 999/2020.

[57] Cfr. por todas, Tribunal Supremo, Sala de lo Penal, sentencia n. 516/1993, de

dría aplicar una circunstancia super atenuante de la pena, como sería la atenuante por analogía de cuasiprescripción[58], en la que el culpable del delito vería considerablemente reducida la pena que le correspondía, para desesperación y desazón de la víctima[59], máxime si tenemos en cuenta la grave saturación judicial existente en este momento en nuestro país[60].

Otro problema que se nos plantea es el empleo de la Dark Web o Darknet, para no dejar rastro de la dirección IP desde la que se ha creado la web desde la que se comete el delito, por ejemplo, un blog

10 de marzo, rec. 2147/1991 o n. 644/1997, de 9 de mayo, rec. 1351/1996

[58] La cuasiprescripción es una atenuante creada por la jurisprudencia del Tribunal Supremo, introducida por vía del art. 21.7ª CP, a los efectos de minorar la responsabilidad penal de la persona condenada, por la existencia de períodos de tiempo transcurridos – antes y/o durante – el proceso que se han quedado próximos a la prescripción y que no se hallan incluidos dentro de los supuestos de la atenuante genérica de dilaciones indebidas (D.M. SANTAN VEGA, *La atenuante analógica de cuasiprescripción. Especial referencia a los delitos de corrupción*, en *Estudios Penales y Criminológicos*, 2019, vol. XXXIX, p. 114).

[59] Cfr. por todas, Tribunal Supremo, Sala de lo Penal, sentencia n. 841/2015, de 30 de diciembre, rec. n. 1166/2015.

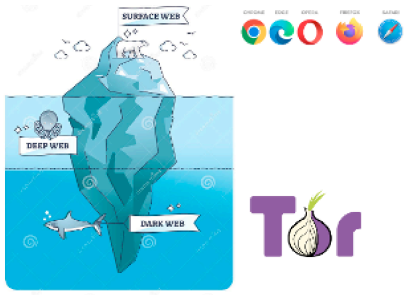
[60] Véase como ejemplo, la noticia publicada en el Diario El País, en la que se denuncia la saturación judicial, titulada: *La dilación perpetua de la Justicia: algunas causas tardan en resolverse el doble que hace 10 años* (disponible en: https://elpais.com/espana/2023-02-21/la-justicia-se-sume-en-la-dilacion-perpetua.html; fecha de consulta: 9 de enero de 2025). En concreto, alude en su denuncia, a un homicidio por violencia de género. Raúl Díaz Cachón, según las investigaciones judiciales, hizo creer a la familia de su mujer, Romina Celeste Núñez, que ella se había ido de casa tras una discusión, sin embargo, este hombre, presuntamente mató y descuartizó a su esposa el 1 de enero de 2019 en Lanzarote y entró en prisión preventiva el día 13 de ese mes. Según denuncia el diario El País, la eficacia con la que arrancó la investigación se fue desinflando hasta perderse del todo en un galimatías de informes periciales, estudios psicológicos y pruebas eternas que, cuatro años después, motivaron poner en libertad al sospechoso, a pesar de los claros indicios de delito, al haber cumplido el tiempo máximo que puede estar en prisión preventiva una persona en España (en total 4 años). De hecho, nuestro Tribunal Constitucional, ha dado la razón a aquéllas personas que han iniciado un proceso en busca de recabar el auxilio judicial a los efectos de restablecer sus derechos e intereses vulnerados, considerando que se les ha producido una vulneración del derecho a la tutela judicial efectiva en caso de existir una demora en el señalamiento de juicios o Vistas (cfr. por todas, Tribunal Constitucional, sentencia n. 25/2022, de 10 de octubre, rec. n. 8133/202).

en el que se llevan a cabo situaciones de *sexting* y ser imposible rastrear el titular del servidor.

La Dark Web es una red que forma una pequeña parte de la llamada Deep Web, donde todo es anónimo y está cifrado, de tal manera que no es posible entrar en ella con navegadores o buscadores normales, sino con un navegador llamado TOR[61]. Esta red permite que los cibercriminales puedan compartir fácilmente contenidos ilegales sin poder ser rastreados[62].

[61] Internet tiene un gran tamaño, con millones de páginas web, bases de datos y servidores que funcionan las 24 horas del día, pero el denominado Internet "visible" o "Clear Web" (sitios que se pueden encontrar a través de motores de búsqueda, como Google) solo es la punta del iceberg. Si continuamos visualizando toda la web como un iceberg, la web abierta sería la parte superior que está encima del agua. Aquí se encuentran todos los sitios web disponibles al público a los que se accede a través de los navegadores tradicionales como Google Chrome, Internet Explorer, Safari o Firefox. Por su parte, la Deep Web se encuentra debajo de la superficie y representa aproximadamente el 90 % de todos los sitios web. Esta sería la parte de un iceberg debajo del agua, mucho más grande que la web superficial. De hecho, esta web oculta es tan grande que es imposible determinar con exactitud cuántas páginas o sitios web están activos en un momento dado. Esta web profunda también incluye la parte que conocemos como la web oscura, Darknet o Dark Web. La web oscura o Dark Web se refiere a los sitios que no están indexados y a los que solo se puede acceder a través de navegadores web especializados. Las nuevas tecnologías, como el cifrado y el software de navegador de anonimización, Tor (proyecto "The Onion Routing), hacen posible que cualquiera persona profundice si le interesa, al poder ser descargado gratuitamente por cualquier, permitiendo a los usuarios conectarse a la web profunda sin que sus acciones se rastreen o a que su historial de navegación se exponga. Los sitios en la web profunda también se utiliza este navegador para mantener su anonimato, es decir, no es posible averiguar quién los administra ni dónde se alojan. En contra de lo que pueda parecer, no es ilegal acceder a la web oscura. Los beneficios que busca el usuario con su navegación son esencialmente los siguientes: anonimato del usuario, servicios y sitios prácticamente imposibles de rastrear, capacidad de adoptar medidas ilegales tanto para los usuarios como para los proveedores. Información disponible en: https://www.kaspersky.es/resource-center/threats/deep-web (fecha de consulta: 9 de enero de 2024) y A. RICO FRANCO, *Desmitificando a la deep web a través de un fugaz viaje por la dark web*, en *Revista ingeniería, matemáticas y ciencias de la información,* n. 15, 2021, pp. 13-32.

[62] S.M. BARÓN QUINTERO, *Los delitos realizados mediante la Dark Net*, en *Revista Penal de México*, núm. 23, 2023, p. 179.



En consecuencia, si se crea una página web, como un blog, en la parte oscura de Internet, esto es, en la Dark Web, es imposible rastrear la dirección IP o su servidor, a los efectos de determinar el titular o posible usuario y, por tanto, localizar al autor del delito. Sin embargo, en el caso de la violencia de género digital, se conocerá por la víctima al autor del delito, pues sólo una determinada persona podrá publicar fotos en situación comprometida – pues únicamente las poseía esa persona – o proferir amenazas o coacciones online – ya que, por ejemplo, se trata de su exnovio, quién normalmente empleaba el mismo lenguaje de forma verbal y no ha soportado que la víctima deje su relación por el maltrato psicológico y/o físico recibido.

Por ello, en atención a estas circunstancias, como veremos más adelante, será necesario acudir a prueba indiciaria.

5.3. *Ilícitos penales cometidos a través de correos electrónicos*

En relación con los ilícitos penales cometidos a través de correos electrónicos, nos podemos encontrar con dos situaciones.

La primera de ellas, vendrá dada por la comunicación electrónica remitida a la víctima por su agresor, profiriendo amenazas, coacciones, insultos o vejaciones.

La segunda de ellas, puede consistir en la falsificación de mails a través del mecanismo del *spoofing*, haciendo aparentar que la mujer víctima de violencia que ha denunciado a su agresor, le envió mensajes de correo electrónicos amenazantes, con carácter previo a la denuncia, por ejemplo, porque no ha soportado que él haya puesto fin a su relación y, de esta forma, siembra la duda en la declaración de la víctima como prueba de cargo, de forma que al existir un posible móvil espu-

rio no puede ser tenida en cuenta esta prueba y lograr así el agresor con esta contradenuncia falsa su absolución[63].

Las contradenuncias falsas interpuestas por maltratadores hacia sus víctimas como estrategia de defensa en procesos penales por violencia de género dirigidos contra ellos, es una cuestión que ha sido advertida por Amnistía Internacional en su informe "¿Qué es la justica especializada?", del año 2012[64], así como por el Observatorio de la Violencia Doméstica y de Género del Consejo General del Poder Judicial en su Guía práctica de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género del Consejo General del Poder Judicial del año 2016[65].

Es necesario que estos casos se analicen desde una perspectiva de género[66], teniendo en cuenta que, además, hay estudios que consideran

[63] Podemos encontrar varias formas de spoofing. Por un lado, tenemos el mail spoofing, en cuya virtud, el remitente falsifica los encabezados del correo electrónico para que el software cliente muestre la dirección de remitente fraudulenta, aparentando ser otra persona quien envía dicho correo electrónico, con la finalidad de que las persona que lo visionen lo acepten tal y como la ven, sin darse cuenta que el remitente es falso, salvo que se inspeccione el encabezado para descubrir el engaño (sobre mail spoofing ver S. GUTIÉRREZ, G. TERCIADO, Mail spoofing: amenazas cada vez más dirigidas, en Seguritecnia, n. 493, 2022, pp. 196-197 o M. ROBLES CARRILLO, M. ALMEIDA ROS, Email Spoofing: un enfoque técnico-jurídico, en Actas de la XVI Reunión Española sobre Criptología y Seguridad de la Información (RECSI), 2021, pp. 139-144). Por otro lado, tenemos el call spoofing, en el que se emplean herramientas tecnológicas que permiten modificar el número de origen que aparece en el dispositivo del usuario haciendo aparentar que es otro número el que está llamando, generando confianza en sus víctimas para que cojan el teléfono o, en el caso de contradenuncias falsas por los maltratadores, pretenden hacer aparentar que reciben un sinfín de llamadas de sus exaparejas para denunciar un falso acoso (J.G. FERNÁNDEZ TERUELO, *Capacidad de respuesta penal frente a los clásicos y nuevos fraudes en los sistemas de banca online: propuestas interpretativas*, en Revista General de Derecho Penal, n. 41, 2024).

[64] Informe susceptible de consultarse en: https://sosvics.eintegra.es/Documentacion/00-Genericos/00-04-Legislacion/00-04-009-ES.pdf (fecha de consulta: 9 de enero de 2025).

[65] Guía disponible en: https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Guias-y-Protocolos-de-actuacion/Guias/Guia-practica-de-la-Ley-Organica-1-2004--de-28-de-diciembre--de-Medidas-de-Proteccion-Integral-contra-la-Violencia-de-Genero--2016- (fecha de consulta: 9 de enero de 2025).

[66] Sobre la necesaria y obligada aplicación de la perspectiva de género a la hora de resolver un procedimiento judicial por el órgano instructor u órgano enjuiciador,

que, en caso de estas denuncias cruzadas, no se analizan correctamente si estamos ante una "contradenuncia" falsa por el maltratador, dándose un mayor rigor punitivo a las mujeres en este ámbito de denuncias cruzadas que a los hombres. No se trata de asumir que todas las contradenuncias interpuestas por maltratadores contra sus parejas o exparejas tras ser denunciados sean falsas, se trata de analizar con perspectiva de género estos asuntos, para que la respuesta penal contra la violencia de género no se vuelva en contra de la mujer inocente víctima de una agresión[67], pues sufriría una doble revictimización, por un lado, la falta de respuesta del Estado ante su agresión y, por otro asumir una condena por un delito que no ha cometido.

De hecho, nuestro Tribunal Supremo, ya ha anulado sentencias absolutorias por delitos relacionados con la violencia de género, si la valoración de la prueba que condujo al órgano enjuiciador a la absolución, no se ha llevado a cabo con perspectiva de género[68].

En relación con la primera cuestión, habrá que estar a las mismas consideraciones que hemos explicado respecto de los mensajes de WhatsApp o similares, en cuanto a la impugnación de su autenticidad.

En este sentido debemos tener en cuenta que, en los mismos plazos procesales que comentamos al hablar de las comunicaciones por mensajería instantánea, lo conveniente sería llevar a cabo una pericial informática, si bien, en este caso, en lugar de realizar una extracción física, analizaremos las cabeceras de los mails, que nos permitirá acreditar que dichos correos electrónicos no han sido manipulados.

Las cabeceras extraídas de los mensajes de correo electrónico, nos proporcionan toda la información relativa al emisor, al receptor, la trayectoria que ha seguido, entendiendo por tal, los diferentes servidores

véase: M.C. GIMENO PRESA, *¿Qué es juzgar con perspectiva de género?*, Pamplona, 2020 o R. BORGES BLAZQUEZ, *Programar, investigar y juzgar con filtro morado: la perspectiva de género en las herramientas de valoración del riesgo*, en L. FONTESTAD PORTALÉS, M.N. JIMÉNEZ LÓPEZ (dirs.), *Justicia, proceso y tutela judicial efectiva en la sociedad postpandemia*, Pamplona, 2022.

[67] M. OTURBAY FUENTES, *Cuando la respuesta penal a la violencia sexista se vuelve contra las mujeres: las contradenuncias*, en Oñati Socio-Legal Series, 2015, n. 2, pp. 645-668.

[68] Tribunal Supremo, Sala de lo Penal, sentencia n. 852/2021, de 4 de noviembre, rec. 4725/20194.

por los que ha podido pasar hasta llegar al destinatario. Para ello, se analizará fundamentalmente el campo "*return-path*" que aparece en dichas cabeceras. Se debe indicar que este campo se corresponde con la cuenta de correo electrónico para devolver el mail en el caso de que el mensaje enviado no pudiera ser entregado a su destinatario, pudiéndose, por tanto, a través de este campo identificar el efectivo emisor del correo electrónico y con su identificación, podemos saber quién es el titular de dicho mail.

En relación con la segunda cuestión que se plantea, esto es, la falsificación de un mail para hacer aparentar que es la víctima la que lo ha enviado, se analizará por el perito también el campo *return-path* en la cabecera y podrá acreditar que el correo electrónico supuestamente remitido por la víctima no coincidirá con el que aparece en el campo *return-path*. Por ejemplo, en la bandeja de entrada aparecerá un mail recibido por el agresor, en el que figura que ha sido enviado por la cuenta mjosejordan@gmail.com, pero, sin embargo en el campo *return-path*, aparece anonyme@orbit.eternalimpact.info, al no coincidir, dicho mail no ha sido enviado por mjosejordan@gmail.com, sino desde otra cuenta que no pertenece a la mujer víctima[69].

Por tanto, ya tenemos acreditado que ha habido una manipulación del mail, el siguiente paso sería tratar de averiguar la dirección IP de envío del mail y al dominio que aparecerá en el campo "*received*"[70], a los efectos de tratar de acreditar que tanto el servidor del mail remitente como el servidor del mail de destino, pertenecen a la misma persona, a saber, el agresor que ha decidido manipular pruebas falsas[71].

[69] De hecho, la Audiencia Provincial de Valencia, Sección 5ª, en Auto n. 697/2019, de 25 de junio, rec. 611/2019, ordenó la reapertura de un procedimiento penal que había sido archivado por posible manipulación de correos electrónicos que según la mujer querellante no fueron remitidos por ella y que produjeron que fuera condenada por un delito que no había cometido según ella, denunciando una contradenuncia falsa realizada por su exnovio, que los falsificó haciendo aparentar que ella le había enviado dichos mails, pero que realmente se los había auto-enviado él, basándose dicha decisión de reapertura, ante la existencia de una pericial informática que acreditaría que podrían haber sido manipulados por el investigado.

[70] El campo "*received*", hace referencia a todos los servidores/ordenadores por las que el correo ha viajado para llegar al destinatario, esto es, nos va indicar dónde se originó el correo electrónico.

[71] Los titulares de los dominios se pueden consultar libremente a través de la he-

La problemática la volveremos a tener, como ya se indicó anteriormente, en el hecho de que la dirección IP de envío o el servidor, estuvieran ocultas por haber empleado servidores Tor en la Dark Web.

Por ello, como veremos a continuación, es necesario aplicar prueba indiciaria, precisamente por aplicación de la valoración de la prueba con perspectiva de género.

6. La necesaria práctica de prueba indiciaria en la valoración de la prueba con perspectiva de género

La prueba indiciaria, también llamada prueba indirecta, circunstancial o conjetural, es aquélla en cuya virtud se pretende demostrar la certeza de unos hechos (indicios) que no son constitutivos del delito objeto de acusación, pero de los que, a través de la lógica y de las reglas de la experiencia, pueden inferirse los hechos delictivos y la participación del acusado[72].

Como viene indicando nuestro Alto Tribunal, la prueba indiciaria sirve como prueba de cargo para enervar la presunción de inocencia, no gozando necesariamente de menor valor o fuerza que la prueba directa, sin que su admisibilidad obedezca al fruto de la resignación para evitar intolerables impunidades, pues la doctrina indiciaria no encierra una relación de las exigencias de la presunción de inocencia y, de hecho, la prueba indiciaria es muchas veces fuentes de certezas muy superiores a las que brindaría una pluralidad de pruebas directas unidireccionales y concordantes[73], declarándose además por nuestro Tribunal Constitucional, su constitucionalidad, en doctrina ya consolidada[74].

rramienta mxtoolbox, disponible en: https://mxtoolbox.com/ (fecha de consulta: 9 de enero de 2025) o en el Ministerio de Industria.

[72] J. MARTÍNEZ JIMÉNEZ, *La prueba indiciaria*, en A. RIVES SEVA (dir.) *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo*, Tomo I, Pamplona, 2021, p. 441.

[73] Cfr. por todas, Tribunal Supremo, Sala de lo Penal, sentencia n. 64/2024, de 24 de enero, rec. 10706/2023, n. 337/2023, de 10 de mayo, rec. 10725/2022 o n. 1054/2024, de 20 de noviembre, rec. 10428/2024.

[74] Entre otras cfr. Tribunal Constitucional, sentencias n. 174/1985, de 17 de di-

El órgano enjuiciador no puede fundamentar el fallo en un simple y puro convencimiento subjetivo, debiendo existir una adecuada motivación acerca de la concurrencia de los indicios, que no deben ser confundidos con meras sospechas, apreciándose una certeza subjetiva que conduce a la convicción judicial con un juicio de inferencia como actividad intelectual que sirve de enlace a un hecho acreditado y su consecuencia lógica[75].

En el ámbito de la violencia de género digital será en ocasiones necesario acudir a este tipo de prueba, pues va a ser muy difícil acreditar con prueba directa, sobre todo si es difícil o complicado asegurar que el usuario o titular del dominio, del perfil de la red social o de la web es la persona agresora, pero es evidente que se dispondrá de otros indicios suficientes que se podrán acreditar y que no constituirán meras sospechas: por ejemplo, que las fotografías únicamente fueron enviadas a esa concreta persona y por tanto, sólo él las podía subir a un blog a los efectos de cometer un delito de sextorsión, que exista un proceso penal por violencia de género abierto, que la dirección IP localizada pertenece a su lugar de trabajo, que la víctima declare que ése es el correo electrónico o el perfil de la concreta Red de su expareja[76], entre otros muchos hechos indiciarios ciertos que se pueden acreditar[77].

ciembre, rec. 558/1983; n. 109/2009, rec. 6939/2005; n. 126/2011, rec. 6988/2024 o n. 146/2014, de 22 de septiembre, rec. 3794/2012.

[75] Tribunal Supremo, Sala de lo Penal, sentencia n. 532/2019, de 4 de noviembre, rec. 10207/2019, en la que se fijan 20 criterios para considerar la prueba indiciaria como prueba de cargo suficiente para enervar la presunción de inocencia y que ha defendido este tipo de prueba, aunque no exista prueba directa para condenar al acusado.

[76] Teniendo en cuenta que la declaración de la víctima no debe ser considerada como prueba indiciaria sino como prueba directa (cfr. Tribunal Supremo, Sala de lo Penal, sentencia n. 339/2007, de 30 de abril, rec. 1715/2006 o n. 1376/2011, rec. 861/2011).

[77] Por ejemplo, la Audiencia Provincial de Barcelona, a través de la sentencia n. 11/2024, de 14 de febrero, rec. 61/2023, condena a un maltratador por un delito de homicidio con base en prueba indiciaria, tomando en consideración varios indicios acreditados, entre otros: la eliminación de chats de WhatsApp de la víctima de forma posterior a su muerte, la discusión que hubo entre ellos, la ruptura de la relación sentimental, la existencia relatada por familiares de una situación de maltrato perpetrado

Si tenemos en cuenta que tenemos este de tipo de prueba, a falta de prueba directa dados los obstáculos advertidos anteriormente para la obtención de dicha prueba directa, los indicios acreditados que permiten alcanzar una certeza absoluta, deben ser tomados en consideración por los juzgados y tribunales, a los efectos de cumplir con la obligación positiva de perseguir la violencia de género, teniendo en cuenta que la valoración de dichos indicios probatorios, han de realizarse, como hemos indicado anteriormente con perspectiva de género y no permitir situaciones de impunidad injustificadas.

7. *Aplicación de tecnología* blockchain *en prueba electrónica para garantizar la cadena de custodia*

En materia de prueba electrónica, no se debe olvidar que se tiene que respetar escrupulosamente el proceso de cadena de custodia, para garantizar la integridad y autenticidad y que los estudios de los indicios se realizan sobre las pruebas obtenidas[78] teniendo en cuenta que, en materia de evidencias digitales, no sólo hay que acreditar que el estudio se realiza sobre el mismo dispositivo, sino que la información de este no ha sido alterada desde su aportación a la causa, esto es lo que se conoce como el principio de la "mismisidad" (sentencia del Tribunal Constitucional, n. 170/2003, de fecha 29 de septiembre, rec. 446/2001)[79].

Precisamente, para garantizar la cadena de custodia en la prueba digital, se está valorando la introducción de la tecnología *blockchain* como herramienta que garantizaría dicha custodia.

La tecnología *blockchain*, conocida principalmente por su papel en las criptomonedas como el *Bitcoin*, está encontrando aplicaciones más allá del ámbito financiero. Una de las áreas en las que está comenzando a demostrar su valor es en la gestión de evidencias digitales dentro del ámbito legal, en la medida que la integridad de la prueba digi-

por la persona condenada o la geolocalización de su teléfono móvil en el lugar del homicidio en el momento de la hora de la defunción de la mujer asesinada.

[78] Tribunal Supremo, sentencia n. 1072/2012, de 11 de diciembre, rec. 767/2012.

[79] J.C. FERNÁNDEZ MARTÍNEZ, *Prueba digital*, en *Diario La ley*, 2020, n. 38.

tal es esencial para obtener una prueba de cargo, con el objetivo de descartar que, durante su custodia en el procedimiento, fue manipulada o alterada[80].

De esta forma, la tecnología *blockchain*, aplicada a la cadena de custodia digital, asegura que no ha existido ninguna manipulación desde su aprensión hasta su presentación en un tribunal, pues el *blockchain* permite registrar cada paso en la transferencia de una evidencia digital, creando un rastro digital inmutable que puede ser auditado en cualquier momento. Esto no solo mejora la transparencia del proceso, sino que también protege la evidencia contra accesos no autorizados o manipulaciones.

La aplicación de esta tecnología es interesante, no sólo desde la perspectiva de la evidencia digital en la comisión de ilícitos penales a nivel nacional, sino que se muestra como muy conveniente en la delincuencia transnacional, pues la ciberdelincuencia implica en su mayoría investigaciones transfronterizas, ya que las víctimas y los delincuentes, así como los prestadores de servicios, suelen estar localizados en diferentes Estados, lo que plantea un desafío a los investigadores, ya que normalmente los países entre sí tienen una regulación sustantiva y procesal distinta en torno al ciberdelito, lo que la Interpol define como "complejidad interjurisdiccional", que desemboca en asimetrías y descoordinaciones[81].

En el ámbito de la prueba de violencia de género digital, resultará

[80] La tecnología *blockchain* puede definirse como una tecnología que se fundamenta en una "base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente" (A. PREUKSCHAT, *Blockchain: la revolución industrial de internet*, Barcelona, 2017, pp. 14 y 15). Es una base de datos descentralizada, creada por Satoshi Nakamoto para realizar pagos sin terceros de confianza con criptomonedas, que no puede ser alterada, que se basa en un modelo que permite a sus usuarios, sin necesidad de que confíen plenamente los unos en los otros, mantener un consenso acerca de la existencia, el estado y la evolución de la cadena de bloques de que se trate, así como de la información que en ella se contiene, prescindiendo de instituciones intermediarias o "autoridades centrales (A. MARTIN MENESES, *Blockchain e implicaciones procesales en materia probatoria*, en *Ius et Scentia*, 2023, n. 2, pp. 136-156).

[81] J. CRIADO ENGUIX, *Blockchain como medio de prueba electrónico en el marco de un proceso penal transfronterizo frente al ciberdelito*, en *Revista de estudios europeos*, 2025, n. 85, p. 495.

interesante aplicar tecnología *blockchain* a la cadena de custodia en ilícitos penales en materia de trata de seres humanos con fines de explotación sexual[82], al poseer en la gran mayoría de casos un origen transfronterizo.

De hecho, el grupo GRETA[83], ha mostrado su preocupación sobre el fuerte impacto de la tecnología en dos fases del proceso de trata: la captación y la explotación. En concreto, en dicho informe se identifican tendencias emergentes señalando el uso de la tecnología en la captación, el chantaje, el control así como la explotación en sus víctimas[84].

Por tanto, en materia de trata de seres humanos, nos encontraremos con una concreta organización criminal en la que se empleará la captación de víctimas a través, por ejemplo, de redes sociales en un concreto país y que explotará a la víctima en otro Estado diferente, controlándola precisamente a través también de tecnologías, como,

[82] La trata de seres humanos con fines de explotación sexual o de matrimonios forzados, es considerada de manera pacífica como una forma de violencia de género. Así se ha venido reconociendo en el citado Convenio de Estambul de 11 de mayo de 2011, también en la Exposición de Motivos de la directiva 2011/36/UE del Parlamento europeo y del Consejo, *relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas,* de 5 de abril de 2011, en DOUE 101 de 15 de abril de 2011, pp. 1-11, o en el informe de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) del año 2020, en el que se concluyó que 2 de cada 3 víctimas de trata de seres humanos son mujeres (informe disponible en: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf, fecha de consulta: 9 de enero de 2025).

[83] GRETA es el grupo que grupo de expertos que monitorea la adecuada implementación del Convenio de lucha contra la trata del Consejo de Europa Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos, hecho en Varsovia el 16 de mayo de 2005 (ratificado por España en BOE n. 219, de 10 de septiembre de 2009), es uno de los principales instrumentos jurídicos de lucha contra la trata de seres humanos.

[84] GRETA, *Online and technology – facilitated trafficking in human beings Summary and recommendations –,* marzo de 2022, disponible en: https://bit.ly/3yweWMA (fecha de consulta: 9 de enero de 2025). Sobre el aumento del empleo de las tecnologías de la información y la comunicación en las redes de tratas de seres humanos ver informe de la ONG Accem, titulado: El impacto de las nuevas tecnologías en la trata de seres humanos, disponible en: https://www.accem.es/impacto-las-nuevas-tecnologias-la-trata-seres-humanos (fecha de consulta: 9 de enero de 2025).

por ejemplo, la geolocalización. Todas esas evidencias de captación, control y explotación de carácter digital, aprendidas en un determinado país y que deben ser trasladadas al Estado cuya jurisdicción será competente para conocer de dichos delitos, corren el riesgo de que no se pueda acreditar correctamente la cadena de custodia, por lo que, en caso de existir algún problema o duda en dicha custodia, invalidaría la prueba y con ello se obtendría una sentencia absolutoria por tratarse de una prueba ilícita e insuficiente para enervar la presunción de inocencia. Sin embargo, con la aplicación de la tecnología *blockchain*, no corremos ese riesgo y se garantizará de forma fehaciente dicha cadena de custodia.

Abstract

En el presente trabajo se va a analizar cuestiones relacionadas con la prueba en el ámbito de la violencia de género digital, con el objetivo de armar y conseguir prueba de cargo suficiente para desvirtuar la presunción de inocencia, a los efectos de cumplir con una de las medidas que debe incluirse en la política criminal de un Estado para actuar con la diligencia debida en materia de violencia de género, a saber, la prevención, la persecución efectiva de estos delitos, así como su intento de minorar la tasa de criminalidad existente.

PALABRAS CLAVE: ciberviolencia de género – prueba digital – prueba electrónica – blockchain – violencia de género digital

LA PROVA NEI PROCESSI PER VIOLENZA DIGITALE DI GENERE

Il presente lavoro analizzerà le questioni relative alla prova nel campo della violenza di genere digitale, con l'obiettivo di acquisire e fornire prove sufficienti per confutare la presunzione di innocenza, ai fini dell'adempimento di una delle misure che devono essere incluse nella politica criminale di uno Stato per agire con la dovuta diligenza in materia di violenza di genere, ovvero, la prevenzione, l'effettiva persecuzione di questi reati e il tentativo di ridurre il tasso di criminalità esistente.

KEYWORDS: Violenza di genere – prova digitale – prova elettronica – blockchain – violenza di genere digitale

CIBERVIOLENCIA DE GÉNERO EN MENORES DE EDAD: VULNERABILIDAD, PRUEBA, SUPRANACIONALIDAD Y HUIDA DEL PROCESO

Raquel Borges Blázquez[*]

SUMARIO: 1. ¿De qué estamos hablando? – 2. Del *sexting* a las *deepfakes.* – 2.1. *Sexting.* – 2.2. *Deepfakes.* – 3. Víctimas especialmente vulnerables a la ciberviolencia. – 3.1. La ciberviolencia en agenda legislativa. – 3.2. El caso de las niñas de Almendralejo. – 4. Cuestiones procesales. – 4.1. Prueba y recursos: ¿qué es veraz y qué es falaz? – 4.2. Perspectiva internacional y medidas cautelares en un mundo globalizado e interconectado. – 4.3. Mediación como ¿solución. – 5. Breves reflexiones.

1. *¿De qué estamos hablando?*

Define la directiva 2024/1385[1] la "violencia contra las mujeres" en su artículo 2 apartado a) como "todo acto de violencia de género dirigido contra una mujer o una niña por el hecho de ser mujer o niña, o que afecten de manera desproporcionada a mujeres o niñas, que causen o sea probable que causen daños o sufrimientos de naturaleza física, sexual, psicológica o económica, incluidas las amenazas de realizar tales actos, la coacción o la privación arbitraria de libertad, tanto si se producen en la vida pública como en la vida privada". Y en el apartado f) del mismo artículo cifra la minoría de edad en "toda persona que tenga menos de 18 años". Dado que la ciberviolencia de género en menores de edad tiene un marcado carácter supranacional, como tendré ocasión de explicar en las próximas páginas, serán estas las dos definiciones que manejaremos en el trabajo. Definiciones que resultarán

[*] Profesora Permanente Laboral de Derecho Administrativo y Procesal, Universidad de Valencia. Raquel.Borges@uv.es Este artículo ha sido redactado en el marco del proyecto de I+D PID2021-123170OB-I00.

[1] Directiva 2024/1385/UE del Parlamento europeo y del Consejo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, de 14 de mayo de 2024, en DOUE 1385 de 24 de mayo de 2024, pp. 1-36.

sencillas de aplicar por parte de nuestros operadores jurídicos tanto por la sensibilidad respecto del factor género como por la mayoría de edad a los 18 años.

La violencia de género es un problema global (con diferenciaciones y particularidades dependiendo de la realidad y el momento histórico en que nos encontremos) cuyos actos tienen como sujeto pasivo a la mitad de la población mundial: las mujeres. La violencia contra las mujeres es multifacética, diversa y compleja y las distintas formas que adoptan responden a las diferentes culturas en que se desarrolle.[2] Y son precisamente estas características las que hacen que nos encontremos con ideas opuestas sobre la situación actual de las mujeres en el mundo.[3] Como indicaba hace ya 20 años la ley orgánica 1/2004[4] en su Exposición de Motivos, "La violencia de género no es un problema que afecte al ámbito privado. Al contrario, se manifiesta como el símbolo más brutal de la desigualdad existente en nuestra sociedad. Se trata de una violencia que se dirige sobre las mujeres por el hecho mismo de serlo, por ser consideradas, por sus agresores, carentes de los derechos mínimos de libertad, respeto y capacidad de decisión". Describe la doctrina de la Fiscalía general del estado esta ley orgánica como "un entramado normativo sin parangón posible en otros ámbitos de la criminalidad, expresivo de la sentida responsabilidad social del legislador y de los demás agentes jurídicos y sociales implicados en la lucha contra tan alarmante fenómeno delictivo".[5]

La ciberviolencia de género contra las mujeres no es nueva, pues se sostiene en las mismas raíces que la violencia contra la mujer fuera de las redes. Así, el patriarcado ha sabido adaptarse a las diversas sociedades y momentos históricos en los que ha tenido cabida,[6] siendo

[2] S. SANZ CERVERA, *¿La violencia contra la mujer, una forma de tortura? El derecho internacional, llamando a las cosas por su nombre,* en R. ABRIL STOFFELS, A. URIBE OTALORA (a cura di), *Mujer derecho y sociedad en el siglo XXI,* Valencia, 2010*,* pp. 168-169.

[3] N. VARELA, *Feminismo para principiantes,* Barcelona, 2019, pp. 147-149.

[4] Ley orgánica 1/2004, *de Medidas de Protección Integral contra la Violencia de Género,* de 29 de diciembre de 2004.

[5] Circular 4/2005, *relativa a los criterios de aplicación de la Ley orgánica de Medidas de Protección Integral contra la violencia de género*, de 18 de julio de 2005.

[6] N. VARELA, cit., p. 146.

que nos encontramos con los mismos problemas que mutan sin desaparecer. Lo novedoso es "el medio para su perpetración, lo que permite la convivencia de las conductas ya existentes con las derivadas de la digitalización".[7] En este sentido, Martínez García refiere muy acertadamente que el patriarcado del siglo XXI "usa unos maquillajes distintos y se une al neoliberalismo económico" para así poder colarse en nuestras maneras de sentir, pensar y actuar a nivel individual, social e institucional. "El paradigma androcéntrico sigue empeñado en gestionar la vida individual y colectiva a través de un sistema que protege las libertades de unos a costa de mantener la sujeción de otras".[8]

Esta situación la hemos observado demasiadas veces a lo largo de la historia. Si bien, solo pondré dos ejemplos, por lo cercano al tiempo. El primero, las violaciones mediante sumisión química. Con la democracia y el ocio nocturno normalizado, nos enfrentamos, entre otras, a violaciones con sumisión química. Cuando las noticias empezaron a sacar a la luz casos de víctimas de agresiones sexuales tras la ingesta de sustancias en la bebida, el machismo imperante en esta sociedad fijó el foco en las víctimas y la necesidad de mantener vigiladas sus copas y no beber de vasos ajenos. Esto hizo que, tras la vuelta a la normalidad tras el confinamiento por COVID-19, los medios nos bombardeasen con alarmantes noticias de que en los festivales y discotecas se pinchaba a las mujeres una serie de calmantes para que perdieran el conocimiento y poder abusar de ellas generando una auténtica psicosis entre las jóvenes. Esto, aunque finalmente no fue tan grave como los periódicos y diversos medios indicaban, logró "atemorizar a las mujeres en los espacios de ocio".[9] Las cautelas y la prevención de las víctimas vigilando sus copas no servía de nada porque aparecían nuevas formas de sumisión. El problema es claro: el mensaje que se lanzó fue erróneo. No eran las víctimas las que debían vigilar sus co-

[7] E. CERRATO GURI, *Ciberviolencia de género: influencia internacional y europea en la obtención y conservación de prueba electrónica*, en *Revista General de Derecho Europeo*, 2023, n. 61, p. 170.

[8] E. MARTÍNEZ GARCÍA, *La igualdad y la violencia de género: elementos para la reflexión en España y en Europa*, en J. HURTADO POZO (a cura di), *Género y Derecho Penal,* Lima, 2017, p. 150.

[9] https://elpais.com/sociedad/2022-08-05/primera-consecuencia-de-los-pinchazos-en-espana-atemorizar-a-las-mujeres-en-los-espacios-de-ocio.html

pas, eran los agresores los que no debían adulterar la bebida de sus víctimas.[10]

El segundo, y al que dedicaremos las futuras líneas de este trabajo, el reenvío masivo de imágenes de mujeres desnudas como forma de extorsión o como forma de agresión. En este supuesto, al igual que en las agresiones sexuales, una vez más se puso el foco en la necesidad de auto protección de la víctima en lugar de en el castigo del agresor. De nuevo se desplazó la responsabilidad a las mujeres y niñas. Igual que con el viejo consejo de no hablar con desconocidos en las puertas de los colegios, se pidieron cautelas a las mujeres: dejar de enviar *nudes* o hacerlo sin rostro porque, de lo contrario, no es posible saber dónde acaba una imagen íntima. Y en esta cultura del miedo se educó a las actuales y futuras generaciones. Pero la responsable del cuidado nunca debió ser la víctima. El responsable del ilícito es aquél que reenvía imágenes sexuales sin consentimiento, pues así es como tipifica el *sexting* nuestro código penal.[11] En el mismo sentido, nuestro Tribunal Supremo en STS 70/2010, remitir una imagen íntima no implica una renuncia a la intimidad ni a la privacidad, pues esto se realiza en una esfera de confianza respecto de quién la traiciona y, consecuentemente, "su gesto de confiada entrega y selectiva a una persona cuya lealtad no cuestiona, no merece el castigo de la exposición al fisgoneo colectivo".[12]

Lo rápido que se extienden los bulos, las malas noticias y, también, los actos denigrantes contra las mujeres hacen que la cadena de reenvíos masivos de imágenes de desnudos de mujeres sea imposible de parar. Y no solo eso, la prueba se convierte en prácticamente imposible por la falta de medios humanos en nuestros juzgados y tribunales

[10] Para más información puede leerse: C. GARCÍA ARROYO, *El nuevo delito de agresión sexual del artículo 178 CP. El valor del consentimiento* en E. NÚÑEZ CASTAÑO, C. GARCÍA ARROYO, A. RODRÍGUEZ MOLINA (a cura di), *Reformas Penales y Estado de Derecho,* Valencia, 2024, pp. 345-369.

[11] Artículo 197.7 C: "Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona".

[12] Tribunal Constitucional, sentencia de 4 de febrero de 2010, n. 70/2010.

para hacer un rastreo eficaz de cuántos móviles han recibido y reenviado las imágenes.[13] La situación para la víctima es devastadora, llegando incluso al suicidio en algunos casos.[14] Es la falta de respuesta institucional[15] la que nos hace creer que dejar de enviar imágenes nos haría estar a salvo. Una vez más, ganó el machismo. La Inteligencia Artificial generativa se ha empleado para desnudar mujeres y reenviar imágenes, en apariencia reales, pero que son completamente falsas. Los viejos problemas que mutan sin desaparecer.

El Tribunal Europeo de Derechos Humanos (TEDH) reconoció en sentencia de 11 de febrero de 2020[16] que la ciberviolencia contra las mujeres (mayores y menores de edad) presenta múltiples formas y es éste un problema que trasciende fronteras nacionales donde, además, observamos una "normalización" de conductas violentas entre los más jóvenes, siendo éstos los que más uso hacen del espacio virtual y los

[13] El Juzgado de lo Penal nº 5 de Alcalá de Henares ha sobreseído provisionalmente el caso por "falta de autor conocido" del delito de revelación de secretos y porque no había denuncia en el delito de trato degradante por el que investigaba la jueza. Vid. M. BORRAZ, L. OLÍAS, *La justicia archiva el caso de la trabajadora de Iveco que se suicidó tras la difusión en su empresa de un vídeo sexual*, en *ElDiario.es*, mayo 2020, https://www.eldiario.es/sociedad/justicia-archiva-trabajadora-iveco-difusion_1_5972443.html

[14] L. F. DURÁN, S. FERNÁNDEZ GARCÍA, L. NÚÑEZ VILLAVEIRÁ, *Una empleada de Iveco se suicida tras viralizarse en la empresa un video sexual*, en *El Mundo*, mayo 2019, https://www.elmundo.es/madrid/2019/05/28/5ced493efdddffb0758b48fb.html; REDACCIÓN BARCELONA, *Trabajo dicta que la difusión del vídeo sexual de la trabajadora de Iveco no influyó en su suicidio,* en *La Vanguardia*, junio 2020, https://www.lavanguardia.com/vida/20200625/481946782843/inspeccion-trabajo-trabajadora-iveco-suicidio-video-sexual.html El informe ha dictaminado que la difusión de este material audiovisual "no le afectó" a la hora de decidir quitarse la vida, sino que lo único que temía era que lo supiera su pareja.

[15] "El Tribunal de Estrasburgo encuadra las obligaciones de tutela penal entre la más basta categoría de las obligaciones positivas de tutela las cuales tienen como objeto no ya la abstención de conductas directamente lesivas del derecho individual por parte de los agentes del Estado, sino la adopción de medidas de tutela del derecho contra las agresiones provenientes de terceros". F. VIGANÒ, *La arbitrariedad del no punir. Sobre las obligaciones de tutela penal de los derechos fundamentales,* en *Política Criminal*, 2014, n. 18, p. 456.

[16] Tribunal Europeo de Derechos Humanos, sentencia de 11 febrero 2020, application n. 56867/15, *Buturugă v. Romania*.

que menos conscientes son del riesgo inherente a éste.[17] Como indica Cuenca Curbelo,[18] esta sentencia "supuso la primera vez que el TEDH abordaba el fenómeno del ciberacoso (*cyberbullying*) como una manifestación de la violencia contra la mujer". En este caso, el TEDH declaró una violación de los artículos 3 y 8 del Convenio contra Rumanía al incumplir sus obligaciones estatales positivas pues, siendo consciente de que el ex marido accedía a cuentas electrónicas y de Facebook de la demandante de forma abusiva así como que había realizado copias de conversaciones privadas, documentos y fotografías, las autoridades competentes desestimaron la petición pues consideraron que dicho material no guardaba relación con las amenazas y la violencia, delitos por los que había una causa penal abierta contra el ex marido de la demandante.[19]

La tecnología ha evolucionado más rápido que nuestras mentalidades y seguimos creyendo que lo que ven nuestros ojos y escuchan nuestros oídos es cierto, aunque sea una manipulación de la imagen y el sonido.[20] Esto se ha empleado por empresas que han querido lucrarse a costa de desgracias ajenas. Empresas que nos han permitido despedirnos de nuestros abuelos o pedir perdón a un familiar o amigo que falleció tras una discusión. Su voz al teléfono no es real, pero lo parece. La IA rescata de conversaciones sus formas de hablar, de hacer pausas, su modo de expresarse, etc. para generar la apariencia de real.

[17] E. CERRATO GURI, cit., pp. 168-169.

[18] S. CUENCA CURBELO, *Crónica de jurisprudencia del Tribunal Europeo de Derechos Humanos,* en *Revista de Derecho Comunitario Europeo,* 2020, n. 66, p. 717.

[19] Tribunal Europeo de Derechos Humanos, sentencia de 11 febrero 2020, application n. 56867/15, *Buturugă v. Romania*: "For a positive obligation to arise, it must be established that the authorities knew or ought to have known at the relevant time of the existence of a real and immediate risk of ill-treatment of an identified individual from the criminal acts of a third party and that they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk (see *Đorđević v. Croatia*, no. 41526/10, § 139, ECHR 2012). In addition, the Court has held that States have a positive obligation to establish and apply effectively a system punishing all forms of domestic violence and to provide sufficient safeguards for the victims (see *Opuz*, cited above, § 145, and *Bălşan*, cited above, § 57 *in fine*)"; S. CUENCA CURBELO, cit., pp. 717-719.

[20] Al respecto, deviene interesante la lectura de: I. SALAZAR, *Cuando ver ya no es suficiente para creer,* en *Telos,* 2021, n. 117.

Pero esto no nos va a devolver a nuestros seres queridos, ni permitir hablar con el más allá. Es solo un parche ante una pérdida. Algo que ya vaticinó *Black Mirror* en su episodio "*Be right back*". A fecha de su estreno, en 2013 se nos helaba la sangre pensando en esta realidad distópica. El presente es la distopía que tanto nos asustaba. Además, la IA generativa ha tenido una cara menos amable y más delictiva: la creación de aplicaciones para desnudar personas. Aquí surgen una serie de interrogantes que afectan también a otras áreas del Derecho y que serán sus profesionales los que den respuestas: ¿tiene responsabilidad el creador de la aplicación?, ¿puede el estado prohibir el uso de estas aplicaciones?, ¿serviría de algo esta prohibición en un mundo global y digitalizado?[21]

Pero al margen de estos interrogantes sí que existen cuestiones que podemos responder desde el proceso penal aplicando una perspectiva de vulnerabilidad. Como indica Martínez García es necesario observar estas diferencias "con "perspectiva", es decir, con cierta distancia para observar lo que desde encima del problema no podemos ver. En este sentido, la perspectiva de género y la perspectiva del interés del menor o personas vulnerables son las dos perspectivas más desarrolladas en España a la hora de mirar con otros ojos la impartición de la justicia."[22] Así, a lo largo de este trabajo, se expondrán las cifras de *deepfakes* que afectan a las mujeres por razones de violencia de género. Dentro de éstas, nos centraremos en las víctimas de violencia de género menores de edad, por mostrar éstas una mayor vulnerabilidad por razón de su corta edad. Por último, teniendo presentes los objetivos del proceso penal de menores donde, además de la sanción, se pretende la reeducación del infractor, se valorará la posibilidad de mediación. Esta cuestión enlaza precisamente con lo apuntado al inicio del trabajo: si pedir a las víctimas que se auto protejan no ha servido de nada, debemos educar en igualdad y en valores desde la infancia a los agresores, para que comprendan el desvalor de sus accio-

[21] Al respecto, me remito a las reflexiones sobre pornografía infantil que realizó el profesor J. MARTÍNEZ OTERO, *¿Resulta constitucional restringir la pornografía en internet? Bases para repensar el Estatuto Jurídico del discurso pornográfico,* en *Revista General de Derecho Constitucional*, 2021, n. 35, pp. 1-38.

[22] E. MARTÍNEZ GARCÍA, *Juzgar en el siglo XXI,* Valencia, 2024, p. 131.

nes y el daño que éstas generan. Porque si queremos acabar con la violencia de género no se hará desde el proceso penal, se hará desde las aulas en todos los niveles educativos.[23]

El proceso penal se accionará para gestionar un fracaso. Y debe seguir accionándose pues, de lo contrario, se mandaría un mensaje erróneo de inactividad estatal. La falta de ejercicio del *ius puniendi* trae consigo una violación de las obligaciones que incumben a cada Estado de "respetar" los Derechos Humanos dentro de su jurisdicción. Así las cosas, el recurso al derecho penal ha sido considerado por el propio Tribunal de Estrasburgo como "una solución necesaria a partir de la lógica de la protección de los derechos humanos, y no en cambio como una opción abierta a la valoración discrecional de las instancias democráticas del Estado parte".[24] Pero cuando entra el proceso penal ya hay una víctima y un agresor claramente diferenciados y un bien jurídico protegido dañados. Por ello, las políticas públicas, sobre todo en menores, deberían centrarse en la prevención más que en la represión.

2. *Del* sexting *a las* deepfakes

Comparto con Carretero Sánchez, "el mundo de internet es todo lo ficticio o irreal que queramos, que la información aportada es de parte, y que el administrador carece de medios para poder parar o no acceder a nadie, es decir, que es un medio tan poco preciso que permite que cualquier pueda utilizarlo de modo no conveniente".[25] La delincuencia informática supone un tipo de criminalidad especial debido a los medios a través de los que se materializan sus conductas. Desde los años ochenta estudios criminológicos apuntan a que el avance de

[23] L. AVILÉS PALACIOS, *La perspectiva de género como técnica jurídica e instrumento necesario para una justicia igualitaria,* en *Análisis de la justicia desde la perspectiva de género,* Valencia, 2018, pp. 279-318.

[24] F. VIGANÒ, *Sobre las obligaciones de tutela penal de los derechos fundamentales en la jurisprudencia del TEDH,* en S. MIR PUIG, M. CORCOY BIDASOLO (da cura di) *Garantías constitucionales y Derecho penal europeo,* Valencia, 2012, p. 312.

[25] S. CARRETERO SÁNCHEZ, *Las redes sociales y su impacto en el ataque a los derechos fundamentales: aproximación general,* en *Diario La Ley,* 2016, n. 8718, p. 2.

las TICs así como su extensión a prácticamente todas las áreas de la vida iban a hacer que los delincuentes también ampliasen su ámbito de actuación a los medios informáticos para la comisión de toda clase de ilícitos penales.[26] Es en esta década cuando comenzaron los primeros delitos informáticos. Desde entonces su tipología se ha diversificado, su importancia ha aumentado a velocidades de vértigo y actualmente la delincuencia informática es más común de lo que pensamos y se extiende a todos los ámbitos de la sociedad.[27]

Podemos distinguir los delitos más perseguidos en el terreno virtual en tres grandes grupos: 1) aquellos relativos a estafas y extorsiones, 2) los que se refieren al sabotaje o daños informáticos y 3) los que afectan a la intimidad y al honor de las personas, debiendo hacer énfasis en aquellas especialmente vulnerables -menores de edad o víctimas de violencia de género-.[28] En los últimos años, este tercer grupo ha aumentado exponencialmente, tanto su comisión como su capacidad para atacar bienes jurídicos de las víctimas. Estos deberían ser tratados como lo que son, puros y simples delitos cometidos por medios telemáticos. Hablemos de inducción al suicidio (art 143 CP y 143bis CP), de delito de coacción (art 172 CP), de acoso sexual (art 184 CP), de amenazas (art 169-171 CP), de calumnias (art 205-207 CP) de injurias (art 208-210 CP), de *child grooming* (art 183 ter CP) y *cyberbulling* (extensión del acoso por medios tecnológicos), del discurso del odio (Recomendación num. (97) 29, del Comité de Ministros del Consejo de Europa de 30 de Octubre de 1997 y art 510 CP), de extorsión (art 243 CP), de violencia doméstica y de género (art 153 y 173.2 y 3 CP), de pornografía infantil (art 189 CP), de *sexting* (art 197.7 CP), de *stalking* (art 172 ter CP) y de lesiones (art 147-156 CP) entre otros muchos delitos que son susceptibles de cometerse a través de la red. Algunos de estos delitos han sido tipificados expresamente para regular un hecho que antes no existía y otros simplemente han cambiado la forma de su comisión. Nuestro legislador es consciente de la gravedad

[26] http://tecnologia.elderecho.com/tecnologia/ciberseguridad/Santos-Puga-aspectos-criminologicos-delitos-informaticos-tecnologia-informacion_11_801805001.html

[27] http://peritoinformaticocolegiado.es/delitos-informaticos/

[28] F. BUENO DE MATA, *Prueba electrónica y proceso 2.0*, Valencia, 2014, p. 141.

de los delitos informáticos y de la importancia de la prueba electrónica en los litigios, y esto ha dado lugar a jurisprudencia asentada en la materia.[29] Observamos como la mayoría de las definiciones respecto de ciberviolencia son neutrales y se asume que la violencia a través de las redes puede afectar a ambos géneros. Esta neutralidad se observa en regulación nacional e internacional. La legislación que defiende el copyright (imágenes) o que persigue los delitos (acoso) no emplea el género como factor y, sin embargo, los datos nos muestran cómo hay diferencias sustanciales entre géneros.[30]

2.1. Sexting

El concepto de *sexting* nace de la fusión de las palabras inglesas *sex* y *texting*. Podemos definirlo como el envío de mensajes, imágenes, vídeos o audios de contenido erótico, producidos por el propio remitente por medio de TICs, a, en general, su pareja o persona con la que mantiene un romance, tonteo o similar con el objetivo de despertarle deseo o atracción sexual.[31] La base de esta práctica, muy habitual entre jóvenes,[32] es el consentimiento en su envío y la confianza en que el uso y disfrute –por así decir- de ese contenido erótico será únicamente para su destinatario, que no lo difundirá ni compartirá con terceros. Los problemas comienzan (y se traspasa la línea de lo delictivo) cuando el receptor decide "vengarse", cuando lo remite a otra persona de su

[29] F. BUENO DE MATA, cit., pp. 141-142.

[30] Traducción libre de: "The definitions identified tend to be gender neutral, due to the understanding that these forms of cyber violence can potentially affect victims of any gender. This neutrality can also be linked to many of the policies reflecting the regulatory framework, where the various forms of cyber violence fall under laws that go from copyright (images) to criminal offences (harassment), whereby gender is not seen as a factor. Data collection is significantly conditioned by this and the disaggregation of data by sex is infrequent". Maping Cyber Violence in the EU-27, EIGE, 2021, p. 4.

[31] J. MARTÍNEZ OTERO, *La difusión de sexting sin consentimiento del protagonista: un análisis jurídico,* en *Derecom,* 2013, n. 12.

[32] Indica AGUSTINA que los jóvenes están siempre a la última en materia de nuevas tecnologías en: J. R. AGUSTINA, *¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el sexting,* en *Revista Electrónica de Ciencia Penal y Criminología,* 2010, n. 12, p. 6.

confianza para compartir lo que sucede sin poder controlar el reenvío "en cascada"[33] o cuando un tercero -ajeno a las dos partes- accede de forma no autorizada a alguno de los dispositivos móviles implicados dando lugar a una pérdida de control[34] del contenido enviado, pérdida que tuvo lugar cuando realizamos el primer envío.[35] En el contexto virtual "el concepto de intimidad se diluye, siendo común que temas de conversación o prácticas íntimas o privadas, que se relacionan con el cuerpo, la sexualidad o los sentimientos, se compartan sin que se perciba riesgo alguno"[36] Como indicaba al inicio del trabajo, ante esta pérdida de control se pidió a las víctimas que fuesen cautas en el envío de imágenes, por las consecuencias negativas que esto podría acarrearles. Pero el autocuidado en esta era digital no sirve si la tecnología *deepfake* es capaz de crear imágenes reales de mujeres desnudas.

2.2. Deepfakes

El concepto de *deepfake* fue empleado por primera vez en 2017 combinando *deep learning* (aprendizaje profundo) y *fake* (falso). Las *deepfakes* utilizan algoritmos que aprenden de patrones que se les

[33] SAP de Granada (Sección 1ª) número 351/2014 de 5 de junio donde se absuelve a los menores denunciados por la difusión de la imagen desnuda de la víctima, también menor de edad, a través de la aplicación de *whatsapp* porque el primer envío lo realizó la propia víctima al que era su novio y no cabía en el tipo delictivo del descubrimiento y revelación de secretos. En este caso el menor que realizó el primer envío se lo pasó a sus compañeros de equipo para que se "motivaran" antes de un partido.

[34] Tras una muestra de 637 adolescentes residentes en la provincia de Valencia se concluyó que el 60% de los adolescentes que practican *sexting* no son conscientes del peligro y un 28% de éstos plantean la posibilidad, aunque de manera remota. C. MOLLA ESPARZA, L. RODRIGUEZ-GARCÍA, E. LÓPEZ GONZÁLEZ, *Sexting en adolescentes ¿conscientes del peligro?* en *Comunicación presentada en el XVI Congreso Nacional y VII Congreso Iberoamericano de Pedagogía,* Madrid, 2016.

[35] Escribí hace años respecto de la prueba del sexting en: R. BORGES BLAZQUEZ, *El sexting, la violencia de género y la prueba electrónica en el proceso penal,* en *Revista General de Derecho Procesal,* 2018, n. 44.

[36] M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia de género: nuevas formas de victimización,* en C. ARANGÜENA FANEGO, M. DE HOYOS SANCHO, E. PILLADO GONZÁLEZ (a cura di), *El proceso penal ante una nueva realidad tecnológica europea,* Valencia, 2023, p. 415.

muestran por medio de imágenes, vídeos y audios, para proceder a su manipulación y recrear imágenes, vídeos y sonidos que no son reales, pero que tienen apariencia de real.[37] Refiere Bello San Juan que la creación de contenido falso no es nada nuevo y que ya a mediados del siglo XIX se intentó manipular una imagen en la que aparecía el presidente estadounidense Abraham Lincoln poniéndole el rostro del político John Calhoun.[38] Algunos datos alarmantes que encontramos en el informe *State of deepfake 2023*[39] son que el 99% del contenido pornográfico *deepfake* tiene mujeres como protagonistas. Además, el 48% de los hombres encuestados[40] afirmaban haber consumido *deepfakes* y el 74% de éstos no se sentían culpables por ello. Los motivos más referidos para no sentirse culpables fueron 1) saber que no es una persona real (36%), 2) no pensar que dañe a nadie pues es para un uso privado (30%), 3) las *deepfakes* son una versión más realista de la imaginación sexual (29%) y 4) lo identifican con el porno (28%). Estas excusas, considero, caen por su propio peso, como observaremos más adelante pues las niñas y mujeres famosas que ven su cara unida a un cuerpo que no es suyo consideran dañado su honor y su propia imagen.

Como indica Salazar "(e)l uso de técnicas de inteligencia artificial para manipular imágenes de vídeos de personajes famosos, políticos y otras autoridades de manera que parezcan reales ha hecho saltar las alarmas respecto a la fiabilidad de lo que, hasta hace poco, era incuestionable. No han sido pocos los personajes públicos que han visto usurpada su identidad —incluyendo no solo su imagen, sino también su voz y sus gestos— muchos de ellos con fines pornográficos, y difundido —el resultado— masivamente a través de las redes sociales. El

[37] https://www.unir.net/revista/derecho/deepfake-que-es/

[38] P. BELLO SAN JUAN, *La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminóloga*, en L. FONTESTAD PORTALÉS (a cura di), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI,* Madrid, 2023, p. 229.

[39] https://www.securityhero.io/state-of-deepfakes/#appendix

[40] Como indica BIGAS FORMATJÉ, este porcentaje bebe de una encuesta de 1.522 participantes masculinos residentes en Estados Unidos que habían consumido pornografía los últimos 6 meses. Vid. N. BIGAS FORMATGÉ, *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos*, en *Universitat Oberta de Catalunya*, noviembre 2023, https://www.uoc.edu/es/news/2023/265-deepfakes-pornograficos-cuando-IA-desnuda-tu-intimidad-vulnera-tus-derechos

peligro es indudable. También el riesgo de no poder identificar como falsas imágenes de vídeos que aparentan ser las verdaderas, aunque no sea con un fin malicioso".[41] Las *deepfakes* forman parte de una nueva forma de violencia psicológica y sexual por el acoso que sufren las víctimas así como el *sexting*, la *sextorsión* y el *grooming online*. No son nuevos bienes jurídicos lesionados, son nuevas estrategias de lesión revictimizando a la víctima de manera constante porque la ciber violencia continúa también cuando las partes se separan. Comparto con Bello San Juan, "los daños infligidos a los sujetos individuales como producto del empleo de las tecnologías *deepfake* presenta una afectación directa sobre la dignidad, amén de las lesiones emocionales o las reputacionales previamente señaladas. Particularmente, esta aplicación de la inteligencia digital cristaliza habitualmente en la elaboración de contenido pornográfico, donde las mujeres son las protagonistas y, en consecuencia, las perjudicadas por estas conductas; de hecho, varios informes revelan que el 96% del contenido *deepfake* que circula en la red son pornográficos, y, de ellos, en el 99% aparecen mujeres".[42]

3. *Víctimas especialmente vulnerables a la ciberviolencia*

De acuerdo con la Encuesta Europea sobre violencia de género del año 2022, "(s)e estima que del total de mujeres residentes en España que tienen entre 16 y 74 años un 6,8% (1.222.407 mujeres) ha sido víctima de violencia sexual en la infancia" interpretando la infancia como las menores de 15 años. De éstas, al 0,6% (109.910 niñas) les hicieron posar desnudas para fotografiarlas, realizarle vídeos o interactuar por medio de *webcam* sin ella querer hacerlo.[43] Así, el estudio *Cyberviolence against women and girls* sobre la ciberviolencia nos muestra que tiene género: la estructural desigualdad entre hombres y mujeres hace que mujeres y niñas sean víctimas de ataques cibernéticos so-

[41] I. SALAZAR, cit., p. 20.

[42] P. BELLO SAN JUAN, *Nuevas tecnologías y pornografía: la redimensión de la violencia sexual a través de la tecnología deepfake,* en *V Simposio de investigación criminológica*, Valencia, 2023, p. 1.

[43] Encuesta Europea de Violencia de Género, Eurostat, 2022, p. 88.

brepasando fronteras nacionales porque internet facilita la globalización. Además, tendemos a pensar que la violencia en línea es menos grave que la física y es esta falsa percepción la que da lugar a su minimización o aceptación.[44] Comparto con Llorente Sánchez-Arjona, las agresiones y el acoso en el mundo virtual tienen como características distintivas la facilidad en el acceso y el anonimato "lo cual dificulta el rastreo de la persona que agrede proporcionándole sensación de impunidad".[45]

3.1. *La ciberviolencia en agenda legislativa*

Observamos como los últimos años tanto documentos europeos como legislación nacional han puesto su foco en las víctimas especialmente vulnerables.[46] Si bien los conceptos de vulnerabilidad y de grupos vulnerables se van introduciendo en el lenguaje jurídico para la protección de derechos humanos, el concepto de vulnerabilidad ha sido un descubrimiento tardío para el derecho.[47] Nuestro ordenamiento jurídico no tiene una definición de víctima vulnerable. No obstante, si acudimos al sentido literal de las palabras define la RAE la palabra vulnerabilidad como "cualidad de vulnerable" y el adjetivo vulnerable como "que puede ser herido o recibir lesión, física o moralmente". Para la jurista y criminóloga Varona Martínez la vulnerabilidad "puede concebirse, de forma general, como un aspecto intrínseco, universal y generador de la condición humana, con todas sus potencialidades, la vida es vulnerable y por ello hay que protegerla, considerando los diferentes contextos y factores existentes. Esto significa que la vulnerabilidad no es ni buena ni mala, sino un hecho de la condición humana, en su finitud, limitaciones, fragilidad y precariedad".[48]

[44] Mapping cyber violence in the EU-27, EIGE, p. 2.

[45] M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia,* cit., p. 414.

[46] Ley 4/2015, *del Estatuto de la víctima del delito*, de 27 de abril de 2015; Ley Orgánica 8/2021, *de protección integral a la infancia y la adolescencia frente a la violencia*, de 4 de junio de 2021; etc.

[47] L. BURGORGUE-LARSEN, *La vulnerabilidad comprendida desde la filosofía, la sociología y el derecho. De la necesidad de un diálogo interdisciplinario,* en *Revista del Posgrado en Derecho de la UNAM,* 2019, n. 1, p. 126.

[48] G. M. VARONA MARTÍNEZ, *Victimización secundaria, en particular en delitos con-*

Definen las reglas de Brasilia[49] el concepto de las personas en situación de vulnerabilidad indicando que, "se consideran en condición de vulnerabilidad aquellas personas que, por razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales, encuentran especiales dificultades para ejercitar con plenitud ante el sistema de justicia los derechos reconocidos por el ordenamiento jurídico". Siguen estas reglas indicando que "podrán constituir causas de vulnerabilidad, entre otras, las siguientes: la edad, la discapacidad, la pertenencia a comunidades indígenas o a minorías, la victimización, la migración y el desplazamiento interno, la pobreza, el género y la privación de libertad" y "se considera en condición de vulnerabilidad aquella víctima del delito que tenga una relevante limitación para evitar o mitigar los daños y perjuicios derivados de la infracción penal o de su contacto con el sistema de justicia, o para afrontar los riesgos de sufrir una nueva victimización. La vulnerabilidad puede proceder de sus propias características personales o bien de las circunstancias de la infracción penal. Destacan a estos efectos, entre otras víctimas, las personas menores de edad, las víctimas de violencia doméstica o intrafamiliar, las víctimas de delitos sexuales, los adultos mayores, así como los familiares de víctimas de muerte violenta". (La negrita es propia)

Resulta muy interesante esta diferenciación porque las propias reglas refieren que la vulnerabilidad puede darse *per se* en la propia víctima exista o no infracción penal (menores de edad) y en otras víctimas la vulnerabilidad surgirá *ad hoc* consecuencia de las circunstancias de la infracción penal (víctimas de violencia de género), generando así una diferenciación básica entre las víctimas vulnerables *per se* y las víctimas vulnerables *ad hoc* (todos y todas ante una situación concreta, siendo que esta situación requerirá de medidas de corrección). Por lo que a los objetivos de esta investigación respecta, acudiremos al artículo 23.2 EVD. En realidad éste no define ni determina claramente qué son las víctimas vulnerables. No obstante, incluye una lista de quién

tra la seguridad vial, sistema de justicia y la creencia en seres mitológicos, en *Cuadernos Penales José María Lidón,* 2018, n. 14, p. 252.

[49] Reglas de Brasilia sobre acceso a la justicia de las personas en condición de vulnerabilidad, 2008.

puede ser especialmente vulnerable y, además, refiere una serie de actuaciones para su protección. Entre éstas encontramos a las víctimas menores de edad (23.2.a.2 EVD), a las víctimas de delitos contra la libertad o indemnidad sexual (23.2.b.4) y a las víctimas de violencia de género, aunque el EVD emplea la palabra "sexo" en lugar de "género" (23.2.3 EVD). Esta idea tuitiva de protección de la víctima poco a poco va permeando nuestra legislación, nuestra jurisprudencia y nuestra realidad social.

En el caso de las víctimas de *deepfake* sexual que, además, son menores de edad, se dan los tres motivos de vulnerabilidad: el primero, que tienen per se por el hecho de su corta edad, el segundo por convertirse en víctimas de delitos contra la libertad o indemnidad sexual, y el tercero por ser víctimas de violencia sobre las mujeres. Considero que las menores de edad son víctimas especialmente vulnerables ante los desnudos por internet. Se enfrentan al escrutinio y a la vergüenza frente a sus compañeros de recreo y de pupitre. Y no disponen de los mismos mecanismos de defensa que tienen las mayores de edad. Además, en atención a su corta edad, resulta mucho más complicado diferenciar la verdad de la mentira. Su mundo es más pequeño que el de los mayores de edad y, consecuentemente, los parámetros de viralidad de una imagen también. El daño de saber que cuando entren al colegio o al instituto el resto de sus compañeros pueden haberlas visto "desnudas" requiere de respuestas por parte de la maquinaria procesal. Además, "las consecuencias del comportamiento delictivo pueden tener mayor trascendencia al territorial a1 desarrollarse en el ciberespacio, libre de todo límite".[50]

Por lo que respecta a las víctimas vulnerables *ad hoc,* todas podemos ser víctimas de *deepfakes* y así lo han referido famosas los últimos años. Laura Escanes, tras tener conocimiento de que había sido desnudada por medio de aplicaciones de IA, sentenciaba en su perfil de X en 2023 "Si me quiero desnudar, me desnudo yo. Como en estas fotos.[51] Pero no he dado consentimiento para que editen una foto mía".

[50] E. CERRATO GURI, *Ciberviolencia de género: influencia internacional y europea en la obtención y conservación de prueba electrónica*, en *Revista General de Derecho Europeo*, 2023, n. 61, p. 166.

[51] Compartía la *influencer* una serie de fotos donde se intuía desnuda, que ella mi-

Refiriendo que "el cuerpo de una mujer no se utiliza. Ni para el placer, ni para abusar ni para manipular" y finalizaba indicando "me repugna la persona que las haya creado, pero también los que están ahí y les parece divertido y callan".[52] Muestra así la *influencer* la realidad a la que muchas mujeres nos enfrentamos. Además, ella tiene el valor de señalar a los culpables refiriendo que no son solo los que crean las imágenes, también quién las reenvía o se entretiene con éstas. Esta actitud madura ante la victimización sufrida sabiendo que no tiene nada de lo que avergonzarse no puede pedirse a una víctima menor de edad, que no tiene los mismos mecanismos y recursos psicológicos para hacer frente a la agresión.

Además, en menores de edad es todavía más difícil diferenciar la verdad de la mentira al desconocer muchos de los receptores cómo es el cuerpo de una mujer desnuda. En el desnudo a una mujer mayor de edad, tanto ella como sus parejas o exparejas pueden saber que la imagen es falsa (tiene una cicatriz tras una cesárea, una marca de nacimiento en la nalga, estrías en la barriga tras un embarazo, un poco de celulitis, los pechos algo caídos…) Esta situación por supuesto que no reduce el desvalor de la acción, pero, al menos, en su reducto más privado de intimidad, puede contrarrestar con objetividad. De poco servirá pues en la era digital es más sencillo expandir un rumor que demostrar su falsedad y la sensación de vergüenza ante las risas de los compañeros se asemeja a la que sentiría si la imagen fuera real, porque el resto al concibe como real. Las menores de edad ni siquiera cuentan con este pequeño espacio de paz. Simplemente la imagen se tiene por verdadera y no tienen modo de demostrar su falsedad.

3.2. *El caso de las niñas de Almendralejo*

Este caso, conocido por la valiente actitud de Miriam Al Adib (@miriam_al_adib, madre de una de las menores afectadas, ginecóloga e *influencer),* trae causa en la difusión de imágenes manipuladas de menores desnudas *(deepfakes)* por parte de sus compañeros de institu-

sma subió a sus redes sociales tiempo atrás.

[52] https://www.elnacional.cat/enblau/es/famosos/fotos-ropa-laura-escanes-arrasan-red-no-autorizadas-estalla_1078164_102.html

to haciendo uso de aplicaciones de IA gratuitas. En el inicio del curso académico 2023-2024, estas aplicaciones ganaron popularidad entre los menores de edad, que las emplearon para desnudar a sus compañeras. Esta situación pasó en diversos puntos del país, pero fue el caso que aquí les refiero el que generó un punto de inflexión en la materia.

El caso llegó a la UE, que tuvo que pronunciarse respecto de los prestadores de servicios. Los menores condenados emplearon la aplicación "*Clothoff*", anunciada como aplicación de libre acceso para "desnudar a chicas gratis" con una fotografía. La aplicación no pide ni la edad del usuario ni la de la persona que ha sido fotografiada. Por medio de ésta, empleando IA generativa se desnudó "a una treintena de niñas, violando gravemente su derecho a la intimidad y al honor, con el agravante de ser menores de edad." Continúa la pregunta con solicitud de respuesta escrita a la Comisión del Parlamento Europeo[53] refiriendo que la aplicación no pregunta en ningún momento a su usuario si existe consentimiento para desnudar a la persona cuya imagen sube. Es más, la propia política de la aplicación deposita la responsabilidad en el uso de ésta en el usuario.[54] Llama la atención esta exoneración de responsabilidad pues es difícil imaginar un uso lícito de una aplicación cuyo fin es el de desnudar gratuitamente. Responde la Comisión Europea el 16-01-2024, respecto de la aplicación que "El intercambio de imágenes que representan abusos sexuales de menores es ilegal en la EU y el intercambio no consentido de imágenes íntimas es ilegal en diez Estados miembros". Además, "El reglamento de servicios digitales impone obligaciones de diligencia debida a los intermediarios en línea de la UE para contrarrestar la difusión de contenidos ilícitos." No obstante, considera la Comisión, que el reglamento de servicios digitales no es aplicable a la aplicación informática "*Chothoff*" pues sus servicios no se han designado como "plataformas en línea de muy gran tamaño" o "motores de búsqueda en línea de muy gran tamaño" y, además, el reglamento comenzará a aplicarse el 17-02-2024 (fecha posterior a la comisión del ilícito) y serán los Estados

[53] Pregunta con solicitud de respuesta escrita E-002788/2023 a la Comisión.

[54] Pregunta parlamentaria con solicitud de respuesta escrita presentada por J. CAÑAS (Renew), presentada a la Comisión el 22 de septiembre de 2023, E-002788/2023.

miembros los que se encargarán de supervisarlos y ejecutarlos, no siendo la Comisión la responsable de comunicarse con el representante de la plataforma.[55]

A la vista de la situación descrita, se informa a Fiscalía de menores para que investigue la causa. Considero esta situación procesalmente muy interesante por el reducido campo del objeto de estudio. Uno de los grandes problemas del *sexting* y de las *deepfakes* en mayores de edad es lo rápido que se propagan y la práctica imposibilidad de rehacer la cadena de reenvíos masivos en materia de prueba. Este caso sucedió en las aulas del instituto. Los menores de edad tienen un mundo muy reducido, siendo sus compañeros de colegio, sus iguales, y los de colegios vecinos con los que establecen relaciones. Informando a Fiscalía fue relativamente sencillo deshacer la cadena de reenvíos y llegar a los autores de los delitos. Se nos muestra aquí el escenario perfecto para que la maquinaria judicial investigue y castigue a los culpables de los hechos. Finalmente, el Juzgado de Menores de Badajoz consideró a 15 varones menores de edad responsables de 20 delitos de pornografía[56] y contra la integridad moral tras la manipulación de imágenes de, al menos, 20 chicas menores de edad residentes en Almendralejo así como su difusión por dos grupos de *whatsapp*. Esta sentencia se dictó de conformidad,[57] cuestión por la que más adelante trataremos la posibilidad de abrir la vía a una mediación penal. Vaya por delante toda mi sororidad y reconocimiento a la madre de una de las víctimas que decidió romper con el pacto de silencio y judicializar una situación que, de facto, es delictiva y debe ser castigada. Por su valentía denunciando, así como sosteniendo que estos actos no deben quedar impunes y que no son "cosas de niños". No obstante, considero que se podría haber explorado otra vía y otro modo de hacer las cosas por medio de la mediación penal, para empoderar a las víctimas y obtener un

[55] Respuesta del Sr. BRETON en nombre de la Comisión Europea, presentada el 16.1.2024 (E-002788/2023(ASW).

[56] El artículo 189.1 CP, respecto de la pornografía gráfica en menores de edad, incluye la representación virtual que, podría entenderse, entre otros, por imágenes realistas generadas por la tecnología *deepfake.*

[57] https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/Imponen-la-medida-de-libertad-vigilada-durante-un-ano-a-los-15-menores-acusados-de-manipular-y-difundir-imagenes-de-menores-desnudas-en-Badajoz

arrepentimiento sincero de los agresores, que comprenden el desvalor de su acción.

Una de las cuestiones que debiera sorprendernos es la corta edad de los menores en este caso, ya que cinco de ellos todavía no tenían ni 14 años y, consecuentemente, eran inimputables. Sin lugar a duda, hemos fallado como sociedad si niños de 13 y 14 años consideran gracioso desnudar a sus compañeras y reenviar sus imágenes al resto de compañeros del instituto. Al respecto, me gustaría indicar que la propia ley de responsabilidad penal del menor, en su artículo 3 de Régimen de los menores de catorce años, refiere lo siguiente: "Cuando el autor de los hechos mencionados en los artículos anteriores sea menor de catorce años, no se le exigirá responsabilidad con arreglo a la presente Ley, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el código civil y demás disposiciones vigentes. El Ministerio Fiscal deberá remitir a la entidad pública de protección de menores testimonio de los particulares que considere precisos respecto al menor, a fin de valorar su situación, y dicha entidad habrá de promover las medidas de protección adecuadas a las circunstancias de aquél conforme a lo dispuesto en la ley orgánica 1/1996, de 15 de enero." Consecuentemente, no es posible exigirles responsabilidades penales pero el Ministerio fiscal debe informar a la entidad pública de protección de menores para que valoren su situación.

Acudimos, por tanto, al art. 17 bis de la ley orgánica 1/1996[58], que en relación con las personas menores de catorce años en conflicto con la ley, dice así: "Las personas a las que se refiere el artículo 3 de la ley orgánica 5/2000, de 12 de enero, de responsabilidad penal de los menores serán incluidas en un plan de seguimiento que valore su situación socio-familiar diseñado y realizado por los servicios sociales competentes de cada comunidad autónoma. Si el acto violento pudiera ser constitutivo de un delito contra la libertad o indemnidad sexual o de violencia de género, el plan de seguimiento deberá incluir un módulo formativo en igualdad de género." Se desprende de su articulado que,

[58] Ley orgánica 1/1996, *de protección jurídica del menor*, de 15 de enero de 1996. Introducido por la ley orgánica 8/2021 *de protección integral a la infancia y la adolescencia frente a la violencia*, de 4 de junio de 2021.

ante tal situación, servicios sociales deben entrar a conocer qué sucede en el entorno del menor y, además, al tratarse de un delito contra la indemnidad sexual, que deberán cursar un módulo en igualdad de género.

El plan formativo llega bien y tarde. Es esta formación básica en materia de igualdad la que, considero, será capaz de modificar las conductas de los niños y adolescentes. Y esto no es labor del derecho penal, que debe seguir siendo la *última ratio* pues en caso contrario se estaría otorgando al derecho penal un papel de educación y concienciación social que, aunque debe ser tomado en consideración, también debe ser valorado con resistencias y no depositar en el derecho penal funciones que no le son las propias. Porque "no se trata tanto de transformar la legislación, sino de transformar la realidad". Las acciones llevadas a cabo dentro del sistema legal no pueden por sí mismas eliminar el patriarcado si no forman parte de cambios de carácter económico, cultural y social más amplios[59].

4. *Cuestiones procesales*

Nuestro proceso penal no es acorde a los avances tecnológicos ni consciente de la gran dependencia que nuestra vida *offline* tiene de nuestra vida *online*.[60] Y "tan real es este avance a dos tiempos que el proceso penal se ha visto obligado a su reforma en lo que a nuevos métodos de investigación penal se refiere, partiendo del entendimiento de Internet y las nuevas tecnologías de la sociedad de información como fuente de información sobre el delito, materializándose dicha reforma con la LO la ley orgánica 13/2015[61]. Medidas las cuales dotarán a los

[59] R. BERGALLI, E. BODELÓN GONZÁLEZ, *La cuestión de las mujeres y el derecho penal simbólico,* en *Anuario de Filosofía del Derecho,* 1992, n. 9, p. 47.

[60] Escribí hace unos años sobre la posibilidad de imprimir "pantallazos" y, además, mostrarlos para su cotejo ante el LAJ competente. Esta situación ya no resulta posible en las *stories* de Instagram, borrándose a las 24h y dificultando, aún más, la carga de la prueba: R. BORGES BLAZQUEZ, *La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea* en *Revista Boliviana de Derecho*, 2018, n. 5, p. 543.

[61] Ley orgánica 13/2015, *de modificación de la Ley de Enjuiciamiento Criminal pa-*

órganos judiciales de información suficiente para considerar unos hechos probados o no, por lo que, desde el punto de vista de la prueba, el resultado dichas investigaciones tendrá un importante valor probatorio, de ahí la doble naturaleza de dichas medidas, teniendo estas un claro objetivo probatorio"[62].

Como refiere Rivero Ortega respecto de la inclusión de la IA en nuestras vidas, "Los juristas analizamos estos fenómenos desde la perspectiva externa de quien no los ha generado. Así, el papel de la inteligencia artificial es resultado del protagonismo creciente de los informáticos, catalizadores también del problema de los sesgos de los algoritmos. Y han sido filósofos y sociólogos quienes han abierto el debate –y la confusión– entre sexos y géneros. En ambos casos se ven afectados derechos de personas, se suscitan potenciales conflictos de intereses y también se afecta a principios, valores y convicciones ideológicas muy asentadas en la mente de los grupos la extensión del acceso a medios que hace apenas unas décadas serían inasumibles para la inmensa mayoría de la población".[63] En este apartado, referiré someramente algunos de los problemas a los que se enfrenta el proceso en la persecución de este tipo de delitos. Expone muy acertadamente Llorente Sánchez-Arjona, que son tres los grandes problemas a los que nuestro sistema deberá dar respuesta. Nuestro primer problema es la dificultad de la prueba así como su posible manipulación.[64] Esta dificultad se une a un segundo problema que es la internacionalización del problema.[65] Nuestro tercer problema, es la falta de efectividad de las medidas cautelares[66] consecuencia tanto de la internacionalización

ra el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, de 5 de octubre de 2015.

[62] A. GÓMEZ CONESA, *El papel de whatsapp y redes sociales en el proceso penal del Siglo XXI*, en *Diario La Ley*, 2021, n. 9858, pp. 1-2.

[63] R. RIVERO ORTEGA, *Algoritmos, Sesgos, Sexos y Géneros: la sensatez del derecho,* en *Revista de la Facultad de Derecho de México,* 2023, n. 285, p. 15.

[64] M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia,* cit., pp. 418-426.

[65] M. LLORENTE SÁNCHEZ ARJONA, *Las víctimas en el espacio judicial europeo: estudio de la directiva 2011/29/UE, de 25 de octubre de 2012,* en *Revista de Estudios de la Justicia,* 2015, n. 22, p. 120.

[66] Escapa del objeto de estudio el uso de las nuevas tecnologías para quebrantar la prohibición de comunicación. Puede leerse: M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia,* cit., pp. 429-435.

como de las nuevas tecnologías. En el caso antes expuesto, la Agencia Española de Protección de datos inició de oficio actuaciones previas de investigación y contactó con el Ayuntamiento de Almendralejo y la Junta de Extremadura para que comunicasen de la posibilidad de retirar estas imágenes de internet por medio de un canal prioritario.[67] Por último, la mediación penal supone una alternativa que, en atención a la corta edad de las partes implicadas, puede suponer una serie de ventajas.

4.1. *Prueba y recursos: ¿qué es veraz y qué es falaz?*

Lo primero que debemos preguntarnos es si la vulnerabilidad puede afectar a la declaración de la víctima. Si respondemos que sí, surge una siguiente cuestión que es qué haremos para adaptar la declaración a esta víctima. Así, tratándose de un delito contra la indemnidad sexual y menores de 14 años, se tomará una única declaración de manera preconstituida y, a poder ser, haciendo uso de la cámara Gesell.[68]

Como indica Llorente Sánchez-Arjona, "Resulta cada vez más frecuente que las pruebas que se presentan ante los Tribunales partan de un soporte digital a través de sistemas de mensajería instantánea o de redes sociales, siendo de todo punto imprescindible demostrar en sede judicial la veracidad de las comunicaciones que se aportan por las partes".[69] Las conversaciones mantenidas por whatsapp, Instagram o cualquier otra red social pueden ser introducidas como documento electrónico[70] ya sea en soporte de documentos públicos (firmados electrónicamente por funcionarios que puedan dar fe, como el Letrado de la administración de justicia) o a través de acta notarial.[71] Pero ambos funcionarios públicos dan fe de la existencia del documento, no de su

[67] https://elpais.com/sociedad/2024-07-09/un-ano-de-libertad-vigilada-para-15-menores-de-almendralejo-por-manipular-imagenes-de-ninas.html

[68] Puede leerse: R. BORGES BLAZQUEZ, *Prueba preconstituida, derecho de defensa y vulnerabilidad,* Madrid, 2024.

[69] M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia,* cit., 419

[70] Definido en el artículo 3.5 Ley 59/2003, *de firma electrónica*, de 19 de diciembre de 2003.

[71] A. GÓMEZ CONESA, cit.

manipulación.[72] Este riesgo de manipulación de prueba fue tratado por el Tribunal Supremo en STS 300/2015, de 19 de mayo[73] y, tres años y dos meses después, tuvo que ser corregido en la STS 375/2018, de 19 de julio,[74] tras la eclosión de impugnaciones de "pantallazo" de

[72] *Ibid.*

[73] "Respecto a la queja sobre la falta de autenticidad del diálogo mantenido por Ana María con Constancio a través del Tuenti, la Sala quiere puntualizar una idea básica. Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido. Pues bien, en el presente caso, dos razones son las que excluyen cualquier duda. La primera, el hecho de que fuera la propia víctima la que pusiera a disposición del Juez de instrucción su contraseña de Tuenti con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial. La segunda, el hecho de que el interlocutor con el que se relacionaba Ana María fuera propuesto como testigo y acudiera al plenario" STS 300/2015, de 19 de mayo.

[74] "No es posible entender, como se deduce del recurso, que estas resoluciones establezcan una presunción iuris tantum de falsedad de estas modalidades de mensajería, que debe ser destruida mediante prueba pericial que ratifique su autenticidad y que se debe practicar en todo caso; sino que, en el caso de una impugnación (no meramente retórica y en términos generales) de su autenticidad -por la existencia de sospechas o indicios de manipulación- se debe realizar tal pericia acerca del verdadero emisor de los mensajes y su contenido. Ahora bien, tal pericia no será precisa cuando no exista duda al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba. En el presente caso, no hay razones para mantener una duda al respecto. En primer lugar, porque la propia víctima pone a disposición del Juez de Instrucción su teléfono móvil, del que directamente se consultan y transcriben los mensajes por el Letrado de la Administración de Justicia. Éste, como indica la sentencia recurrida, realiza una transcripción, que obra al folio 19 y siguientes del Tomo II de la causa en instrucción, y en ella se recoge íntegramente el contenido de los mensajes cruzados, el teléfono donde se encuentran y aquel del que proceden, que es número NUM000. Además, el uso de este número es atribuido a la acusa-

whatsapp, indicando nuestro TS que no debemos establecer una presunción *iuris tantum* de falsedad de la prueba aportada y que, en el caso de impugnación, debe haber sospechas o indicios de manipulación.[75]

La justicia se está enfrentando al riesgo de falsificación de pruebas producidas por inteligencia artificial, siendo que se pueden presentar contenidos audiovisuales engañosos e incluso falsos como si de pruebas legitimas se tratase.[76] Esta posible manipulación, en la obtención de prueba o, directamente, invención de una prueba trae consigo inseguridad jurídica "tanto por la complejidad técnica de este tipo de pruebas, como por la novedad y constante aparición de nuevas plataformas de comunicación que exigen la constante adaptación de nuestros jueces y tribunales al tener cada una de ellas peculiaridades propias"[77] La carga de la veracidad del medio de prueba será la parte interesada que lo introdujo.[78] Este paso por detrás de la sociedad hace que no exista doctrina consolidada en materia probatoria "pero debe pensarse, que lo que ha cambiado es el formato, la buena doctrina permanece en el tiempo".[79] Además, como alerta Llorente Sánchez-Arjona, aunque pueda parecer poco creíble, es más sencillo manipular

da. Con todo ello, se garantiza, en primer lugar, que si las conversaciones hubieran llegado a ser cuestionadas en cuanto a su origen y/o contenido se hubiera podido asegurar su autenticidad mediante el correspondiente informe pericial; y, en segundo lugar, la forma y modo en que los mensajes se obtuvieron despeja cualquier duda sobre tales extremos, que no surgen por el mero hecho de que el recurrente indique que pudieron haber sido objeto de manipulación o que existen serias dudas sobre la cadena de custodia de los mensajes, ya que se trata de argumentos puramente retóricos y no sustentados en un indicio mínimamente objetivo sobre que ello hubiera sucedido así." STS 375/2018, de 19 de julio.

[75] No puedo detenerme en esta cuestión por motivos de espacio, pero explica brillantemente la cuestión M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia,* cit., pp. 424-425.

[76] P. BELLO SAN JUAN, *La inteligencia,* cit., p. 236.

[77] M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia,* cit., 419.

[78] T. ARMENTA DEU, R*egulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre* en *Revista de Internet, Derecho y Política*, 2018, n. 27, pp. 67-79.

[79] S. CARRETERO SÁNCHEZ, *Las redes,* cit., p. 3.

un documento electrónico que físico.[80] Al respecto, tal vez la figura del testigo *online*[81] arroje un poco de luz entre tanta sombra. La propia página web del Instituto Nacional de Ciberseguridad (INCIBE) refiere que pueden ser útiles "para tener evidencias sobre un uso indebido de fotografías o vídeos publicados en una web o red social sin permiso, pero también para demostrar casos en los que el usuario recibe amenazas, injurias, calumnias o es víctima de una suplantación de identidad en una red social".

Como previamente se ha indicado, las *deepfakes* traen consigo una dificultad para el juzgador que debe diferenciar la verdad de la mentira. Para esto no solamente es necesaria formación en nuevas tecnologías, sino que muy probablemente será necesario que profesionales expertos en la materia puedan asesorarle así como acudir a peritos.[82] Como se ha indicado en el apartado anterior, la actualidad en los juzgados, con medios limitados, hace que nuestros magistrados acepten por ciertos documentos que no son discutidos por las partes, entre otros. Al respecto, el Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior que ha diseñado la Secretaría de Estado de Seguridad "pone el foco en la prevención; en la cooperación entre las diferentes Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y los operadores jurídicos; en la dotación de capacidades suficientes y adecuadas para articular respuestas adaptadas a las diferentes modalidades

[80] M. LLORENTE SÁNCHEZ ARJONA, *La ciberviolencia,* cit., 419.

[81] "Los testigos online permiten certificar evidencias digitales en una fecha y hora determinada, o lo que es lo mismo, el contenido de una web concreta en un momento determinado, o el envío de un correo electrónico a una persona específica. Para ello, este tipo de herramientas basan su funcionamiento en el uso de firmas digitales para acreditar de manera inequívoca una prueba. De esta forma, cualquier clase de prueba tomada permitirá acreditar su integridad, al contrario de lo que sucede con las capturas de pantalla o cualquier otro método similar en el que no interviene una entidad de confianza, y que no permiten demostrar su autenticidad, ya que han podido ser manipuladas." https://www.incibe.es/ciudadania/blog/testigos-online-y-obtencion-de-pruebas-te-explicamos-su-utilidad

[82] Escapa del objeto de la investigación: J. M. DE GREGORIO MELGAR, *Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea y su uso en el análisis forense de la aplicación Telegram Messenger en Android,* en *Ciencia Policial: Revista del Instituto de Estudios de Policía*, 2017, n. 145, pp. 123-148.

delictivas; en la colaboración con la industria y los operadores relevantes en materia de ciberseguridad en el sector público y privado; y en el respeto escrupuloso a la libertad, a la privacidad y demás derechos fundamentales".

De no estar conforme con la sentencia, se abrirá la posibilidad del recurso de apelación alegando un gravamen. El recurso de casación si, además del gravamen, cumple con unos requisitos tasados. Pero también el juicio de revisión como medio de impugnación de la cosa juzgada. En efecto, de acuerdo con el artículo 954.1 LECrim, "1. Se podrá solicitar la revisión de las sentencias firmes en los casos siguientes: a) Cuando haya sido condenada una persona en sentencia penal firme que haya valorado como prueba un documento o testimonio declarados después falsos (…)".[83]

4.2. *Perspectiva internacional y medidas cautelares en un mundo globalizado e interconectado*

Si bien es cierto que en la UE disponemos de normativa para la cooperación en materia probatoria, que fue transpuesta a nuestro ordenamiento interno por medio de la ley 23/2014[84],comparto con Cerrato Guri que "esta normativa no abarca la singularidad que emana de la obtención de la prueba electrónica, por lo que es necesaria su complementación".[85] La sociedad de la información, la inexistencia de fronteras y los envíos masivos de comunicaciones mediante dispositivos electrónicos desde cualquier punto del planeta, hace que los límites temporales y espaciales que han caracterizado al Derecho Penal sean puestos en entredicho. Para ello, deberemos acudir al Convenio sobre la Ciberdelincuencia de Budapest de 2001[86] y a diversas órdenes europeas como pueden serlo la Orden Europea de Entrega y Conser-

[83] Pueden leerse los capítulos explicativos de recursos e impugnación de la cosa juzgada en: S. BARONA VILAR, J. L. GÓMEZ COLOMER (a cura di), *Derecho Procesal III,* Valencia, 2024.

[84] Ley 23/2014, *de reconocimiento mutuo de resoluciones penales en la Unión europea*, de 20 de noviembre de 2014.

[85] E. CERRATO GURI, cit., 179.

[86] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

vación de Pruebas Electrónicas[87] o la Orden Europea de Investigación.[88] Como indica Cerrato Guri, "ninguno de estos textos internacionales ha hecho mención expresa a los delitos de violencia de género, creemos que la definitiva aprobación de esta iniciativa legislativa[89] puede favorecer la implementación del Segundo Protocolo Adicional al Convenio de Budapest por parte de los Estados miembros de la UE que lo han ratificado -la mayoría- en la lucha contra la ciberdelincuencia y, en concreto, en la persecución de los delitos de violencia de género, siendo necesario examinar su encaje específico en este contexto".[90]

Además, las plataformas que se emplean para la comisión de estos delitos tienen su sede fuera de España y, muchas veces, fuera de la Unión europea. Consecuentemente, no tienen por qué reconocer la autoridad jurisdiccional del juzgador nacional que les solicita los datos. En este sentido, Cerrato Guri "Más de veinte años de vigencia del Convenio de Budapest ponen de manifiesto la necesidad de reforzar la cooperación internacional en la obtención de prueba electrónica transfronteriza en un contexto donde la ciberdelincuencia es cada vez más latente". Ejemplo de ello es que "en muchas ocasiones, no se puede saber dónde están dichas evidencias porque su ubicación, particularmente si nos referimos a la 'nube', depende de la decisión de un tercero que interviene como intermediario en la comunicación o en el almacenamiento de los datos y que, incluso, pude ir cambiando su ubicación en atención a circunstancias completamente ajenas a la investigación criminal".[91]

[87] Reglamento 2023/1543/UE del Parlamento europeo y del Consejo, *sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales*, de 12 de julio de 2023, en DOUE 191 de 28 de julio de 2023.

[88] Directiva 2011/41/CE del Parlamento europeo y del Consejo, *relativa a la orden europea de investigación en materia penal*, de 3 de abril de 2014, en DOUE L 130 de 1 de mayo de 2014.

[89] En el momento de suscribir las líneas, se refiere la autora a la propuesta de reglamento del Parlamento Europeo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.

[90] E. CERRATO GURI, cit., p. 158.

[91] *Ibid*., p. 170.

En cuanto a medidas cautelares, si acudimos a la página de la Agencia Española de Protección de Datos (AEPD), ésta indica que "Si tiene conocimiento de que actualmente están colgadas en internet determinadas imágenes de contenido sexual o que muestran actos de agresión, cuya difusión sin el consentimiento de las personas afectadas está poniendo en alto riesgo sus derechos y libertades o su salud física y/o mental, y no ha logrado su retirada a través de los canales especialmente previstos por el prestador de servicios, puede presentar una reclamación por esta vía."[92] Tras esto, la Agencia puede adoptar medidas urgentes para limitar la continuidad del tratamiento de los datos personales. Esta medida cautelar no puede asegurarnos una efectividad real porque los contenidos que se han colgado en la red se han podido descargar en dispositivos electrónicos privados, siendo imposible con los medios actuales realizar tal rastreo. Queda, por tanto, plantearse cuál es la efectividad real de las medidas cautelares si no es posible eliminar las descargas.

4.3. *Mediación como ¿solución?*

La huida del proceso y el uso de medios alternativos de resolución de conflictos es un tema candente durante las últimas décadas que ha sido objeto de estudio por procesalistas, civilistas y penalistas. Sentencian Ríos Martín y Olalde Altarejos, "El proceso penal convencional no respeta convenientemente ni atiende a las necesidades efectivas de las personas que, tapadas bajo una maraña de formalidades, acaban por ocultar la naturaleza del problema subyacente en la infracción penal y por hacer imposible un abordaje razonable de sus soluciones".[93] Entre aquellos ámbitos que podrían optar por una forma de resolución de conflictos diferente a la procesal penal se encuentra la violencia interpersonal pues las partes implicadas probablemente sigan manteniendo algún tipo de relación a futuro. La justicia restaurativa va más

[92] Agencia Española de Protección de Datos, sede electrónica (https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/nuevaReclamacion.jsf?QID=Q600&ce=0)

[93] J. C. RÍOS MARTÍN, A. J. OLALDE ALTAREJOS, *Justicia restaurativa y mediación. Postulados para el abordaje de su concepto y finalidad*, en *Revista de Mediación*, 2011, n. 8, p. 11.

allá de la reparación del daño, busca también la prevención y la pacificación de los conflictos optando por el diálogo en lugar de la confrontación porque "parte de la víctima y de sus intereses, pero los hace confluir con los del infractor y con los de la comunidad; la paz y el diálogo social que el delito quebró serán así restablecidos y saldrá fortalecida la vigencia de la norma".[94] A este respecto, Barona Vilar, la mediación penal requiere de dos garantías para ser incorporada a nuestro sistema: el control judicial del acuerdo y que si no hay acuerdo se acudirá al proceso penal. "La mediación es el instrumento del instrumento -que es el proceso penal- de manera que sirve a este como instrumento de garantía que es de los ciudadanos y de la sociedad".[95]

Apostar por una mediación penal en caso de *deepfakes* sexuales por parte de menores de edad abre un abanico de preguntas a las que deberemos responder: ¿quién ejercerá de mediador?, ¿valoramos la mediación entre iguales?, ¿es una buena opción devolver el conflicto a su entorno y resolverlo en su ámbito natural?, ¿podríamos plantear una mediación, aunque los victimarios fueran inimputables? En el caso expuesto, los agresores tenían apenas 14 años, siendo plausible, en línea con lo planteado por Aranda Jurado, pensar en una mediación escolar donde los mediadores estén en los últimos años en el colegio o instituto (primero y segundo de bachiller) para que sean sus iguales los que les muestren el desvalor de sus acciones.[96] Porque "la mediación ofrece a la víctima del delito la oportunidad de participar directamente en la solución de la situación creada por la infracción penal y abordar sus consecuencias; de recibir respuestas a sus preguntas acerca de los hechos directamente de la persona ofensora, si así lo desea; de expresar el impacto sufrido a consecuencia de lo ocurrido; de obtener la restitución o reparación; de recibir disculpas; de restaurar, cuando sea necesario, la relación con la persona ofensora; de establecer reglas de conducta preventivas de cara al futuro; de elaborar eficazmente su par-

[94] *Ibid*., p. 14.

[95] S. BARONA VILAR, *Mediación penal. Fundamento, fines y régimen jurídico*, Valencia 2011, p. 245.

[96] Estos interrogantes en los que, por cuestiones de espacio, no me resulta posible detenerme, son estudiados en profundidad por la profesora M. M. ARANDA JURADO, *La mediación en el ámbito educativo español,* en S. BARONA VILAR, S. (a cura di), *Meditaciones sobre mediación (MED+),* Valencia, 2022, pp. 633-652.

ticular duelo y alcanzar su cierre. Por su parte, a la persona infractora se le brinda la oportunidad de reconocer la responsabilidad sobre lo ocurrido y conocer y comprender sus efectos en la(s) víctima(s); de expresar sus emociones (incluso el remordimiento) respecto de la ofensa; de recibir apoyo para reparar el daño causado a la víctima o a su familia; de compensar, restituir, reparar, disculparse; de restaurar, cuando sea necesario, la relación con la víctima, de alcanzar un cierre".[97] Al fin y al cabo, reconocer de manera voluntaria la autoría del ilícito deviene en punto de partida para resolver eficazmente un conflicto.[98]

5. *Breves reflexiones*

Comparto con Llorente Sánchez-Arjona, "Resulta paradójico que, a pesar de los avances experimentados por la sociedad actual, se sigan reproduciendo en estos espacios virtuales comportamientos sexistas o claramente atentatorios contra la igualdad de género en un escenario marcadamente tecnológico y vanguardista pero que continúa manteniendo la esencia de la cultura patriarcal imperante durante siglos".[99] Observamos como el machismo y la violencia se están integrando en la vía virtual. No puede negarse el componente del género al ser principal (y casi unánimemente) perjudicadas las mujeres por los *deepfakes* sexuales. Una vez más, deviene necesaria la aplicación de la perspectiva de género en los tribunales para entender y comprender a estas víctimas. En estos casos, es importante que los estereotipos y prejuicios de género queden fuera del sistema judicial porque, de acuerdo con la recomendación general núm. 33 (2015) sobre acceso de las mujeres a la justicia de Naciones Unidas, "distorsionan las percepciones y dan lugar a decisiones basadas en creencias preconcebidas y mitos, en lugar de hechos. Con frecuencia, los jueces adoptan normas rígidas sobre lo que consideran un comportamiento apropiado de la mujer y castigan a las que no se ajustan a esos estereotipos. El establecimiento

[97] J. C. Ríos Martín, A. J. Olalde Altarejos, cit., pp. 11-12.
[98] *Ibid*., p. 13.
[99] M. Llorente Sánchez Arjona, *La ciberviolencia,* cit., p. 3.

de estereotipos afecta también a la credibilidad de las declaraciones, los argumentos y los testimonios de las mujeres, como partes y como testigos. Esos estereotipos pueden hacer que los jueces interpreten erróneamente las leyes o las apliquen en forma defectuosa. Esto tiene consecuencias de gran alcance, por ejemplo, en el derecho penal, ya que dan por resultado que los perpetradores no sean considerados jurídicamente responsables de las violaciones de los derechos de la mujer, manteniendo de esta forma una cultura de impunidad".[100]

En la actualidad asistimos a una "reformulación de las conductas delictivas que en las que el *deepfake* interviene como medio comisivo, ya que si bien se trata de delitos tradicionales en los que esta tecnología es incorporada (p.ej. chantajes), adquieren una nueva dimensión por la difusión que pueden alcanzar y el daño que puede provocar a la dignidad de las personas afectadas".[101] El potencial lesivo de estas prácticas hace que sea necesario tipificar las conductas como de violencia de género pues humillan controlan e intimidan a las mujeres, especialmente por medio de la pornovenganza o la sextorsión.[102] No en vano, es éste el tercer tipo de violencia digital en víctimas atendidas por el Servicio de Violencia de Género Digital el año 2024, solo por detrás del acceso al *whatsapp* por parte de la pareja de la víctima y del ciberacoso.[103] Como refiere Carretero Sánchez, sabemos que podemos ejercer nuestro derecho cuando han atacado nuestra intimidad u honra, pero también sabemos que el derecho actúa tarde, que el mal está ya hecho y que una de las características de la red es la posibilidad de anonimato, de la sensación de que la conducta del infractor va a quedar impune, de que el elevado número de injurias y calumnias vertidas haciendo uso de las TICs colapsaría la justicia.[104] Y, como muchos in-

[100] Recomendación general núm. 33 del Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW/C/GC/33), *sobre el acceso de las mujeres a la justicia*, de 3 agosto 2015, p. 14.

[101] P. BELLO SAN JUAN, *Nuevas tecnologías,* cit., p. 2.

[102] P. BELLO SAN JUAN, *La inteligencia artificial al servicio del crimen,* cit., p. 241.

[103] Informe tercer trimestre 2024, Asociación Stop Violencia de Género Digital y Observatorio de violencia Digital, pp. 20-21.

[104] S. CARRETERO SÁNCHEZ, cit., p. 3.

dividuos saben, insultar o acosar las más de las veces no tendrá consecuencias jurídicas para el/la o los/las infractores/as.[105]

La importancia del caso de las niñas de Almendralejo como objeto de estudio se debe al pequeño entorno en el que sucedió. Las dificultades que trae consigo seguir el rastro del primer reenvío en casos de *sexting* o *deepfake*s con mayores de edad la mayoría de las veces devienen en absoluciones. Aquí, en cambio, al ser un instituto, un espacio acotado, ha sido posible identificar a los adolescentes que manejaron la aplicación. Salvada la dificultad probatoria en estos casos, fiscalía tuvo la posibilidad de marcar la hoja de ruta y dejar claro que esto no son asuntos menores o "cosas de niños" y que las mujeres se suicidan ante estas situaciones. Es éste un problema de prueba que solamente podemos comprender aplicando una doble perspectiva de vulnerabilidad (en la testifical de las víctimas) y transnacional (si el crimen no conoce fronteras tampoco debe conocerlas su investigación). La perspectiva europea e internacional que le da el hecho de que los prestadores de servicios estén fuera del estado español y la necesidad de hacer uso de instrumentos europeos como la orden europea de investigación o internacionales como el Convenio de Budapest. La lucha contra la ciberdelincuencia es global y hemos suscrito diversos convenios y tratados que han traído consigo modificaciones de calado de la LECrim. Pero no es suficiente con legislar, también debe aplicarse la legislación. Para esto son necesarios operadores jurídicos especializados que pierdan el miedo a la cooperación judicial y al uso de las nuevas tecnologías. No en vano, el informe sobre cibercriminalidad en España (2023) refiere entre los objetivos específicos del Plan Estratégico contra la Cibercriminalidad "Impulsar la formación y la especialización de los miembros de las FCSE en materia de ciberseguridad y cibercriminalidad" e "Impulsar la coordinación a nivel nacional e internacional y favorecer la colaboración entre el sector público y privado."[106] Al respecto, como indica Carretero Sánchez, tal vez deberíamos aplicar "una presunción *iuris tantum* de falsedad" de lo que observamos en inter-

[105] En el mismo sentido: *Ibid.*

[106] Informe sobre la cibercriminalidad en España, Secretaría de Estado de Seguridad, 2023, p. 6.

net,[107] en lugar de continuar asumiendo que lo que ven nuestros ojos es cierto, en una era en la que la Inteligencia Artificial (IA) ha avanzado más rápido que nuestras mentalidades y, por supuesto, que nuestro proceso.

Nos estamos enfrentando a un problema que trasciende las fronteras procesales. Intentamos solucionar las diferentes aristas que nos muestra la violencia de género desde el proceso penal pero el proceso penal no sabe dar respuesta a un problema social. Por ello, he querido emplear este trabajo para valorar la posibilidad de una mediación penal en menores. Si se explica el desvalor de la acción y se comprende puede ser mejor que la imposición coactiva de una pena. "A todo ello contribuye la Justicia Restaurativa y su instrumento privilegiado: la mediación."[108] No sabemos si la mediación penal funcionará, pero sí sabemos que el proceso penal no está dando a las víctimas la respuesta que necesitan, por la revictimización que trae consigo y por la dificultad de la prueba. Estamos tratando de dar solución a un problema desde la maquinaria procesal pero la tecnología avanza más rápido que el código penal.[109] Además, esta ley ha sufrido innumerables reformas los últimos años cuando debería ser más duradera y *última ratio*. El *sexting* y las *deepfakes* se están empleando para pornovenganzas y extorsiones a mujeres y niñas que, aunque no tienen una tipificación expresa en el código penal, se encuentran subsumidos en delitos tuitivos de la intimidad o libertad e indemnidad sexuales así como el honor[110] realizando el artículo 189 CP la correspondiente diferenciación entre víctima mayor de edad y víctima menor de edad.[111] En esta cuestión,

[107] S. CARRETERO SÁNCHEZ, cit., p. 2.

[108] J. C. RÍOS MARTÍN, A. J. OLALDE ALTAREJOS, cit., p. 15.

[109] Al respecto, el Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior refiere la necesidad de "Promover un marco legal e institucional que dé solución a los desafíos que surjan relacionados con la ciberseguridad y la cibercriminalidad." p. 6.

[110] N. SORIANO RUIZ, *Difusión ilícita del sexting y violencia de género. Tratamiento penal y procesal en España*, en *Revista Electrónica de Estudios Penales y de la Seguridad,* 2019, n. 4, pp. 1-21.

[111] "A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección: a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexual-

serán los penalistas sustantivos los que deberán indicarnos si es posible subsumir estos delitos en el tipo penal existente o si necesitamos regular los "nuevos" delitos que se están cometiendo utilizando la IA. Cierro el trabajo como lo inicié, reiterando que el proceso penal es un parche al doloroso presente que viven las víctimas de ciberviolencia de género y que solo por medio de la educación se podrá conseguir un cambio de mentalidades y actitudes en las actuales y futuras generaciones. De lo contrario, continuaremos repitiendo los mismos problemas que mutarán y se adaptarán a realidades actuales y futuras, pero no desaparecerán.

Abstract

En este artículo se estudia la ciberviolencia de género en menores de edad con el objetivo de mostrar los problemas procesales en la práctica de la prueba y la adopción de medidas cautelares en un mundo globalizado. Estas cuestiones deben ser estudiadas desde la perspectiva de vulnerabilidad que otorga el hecho de que las víctimas sean menores de 18 años. Además, se valora la posibilidad de hacer uso de la mediación penal como posible solución a un conflicto que desborda las fronteras procesales.

KEYWORDS: Género – menores de edad – prueba – Inteligencia Artificial – mediación penal

mente explícita, real o simulada. b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales. c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes. d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales".

VIOLENZA INFORMATICA DI GENERE CONTRO I MINORI: VULNERABILITÀ, ASPETTI PROBATORI, DIMENSIONI SOVRANAZIONALI E FUGA DALL'AZIONE PENALE

Il presente articolo analizza il fenomeno della violenza informatica di genere perpetrata ai danni di minori nel contesto globalizzato. Scopo della ricerca è evidenziare le criticità relative all'acquisizione di prove e all'adozione di misure cautelari in un contesto transnazionale, problematiche che devono essere necessariamente interpretate alla luce della vulnerabilità intrinseca delle vittime, in quanto minori di 18 anni. Un ulteriore aspetto affrontato nel presente contributo è il potenziale ricorso alla mediazione penale come strumento alternativo di risoluzione dei conflitti, capace di trascendere i limiti dei tradizionali confini procedurali.

KEYWORDS: Genere – minori – prove – Intelligenza Artificiale – mediazione penale

ELENCO AUTORI E AUTRICI – LISTA DE AUTORES

Rocco Alfano, Procuratore della Repubblica aggiunto presso il Tribunale di Salerno.
Elisabetta Bergamini, Professoressa ordinaria di Diritto dell'Unione europea, Università di Udine.
Raquel Borges Blázquez, Profesora permanente laboral de Derecho administrativo y procesal, Universidad de Valencia.
Giuseppina Cersosimo, Professoressa ordinaria di Istituzioni di sociologia e di Sociologia del web e degli impatti sociali, Università di Salerno.
Sara De Vido, Professoressa ordinaria di Diritto internazionale, Università Ca' Foscari di Venezia.
Angela Di Stasi, Professoressa ordinaria di Diritto internazionale e Diritto dell'Unione europea, Delegata d'Ateneo alle Pari opportunità, Università di Salerno.
Rosario Espinosa Calabuig, Catedrática de Derecho internacional privado, Universitat de València.
Angela Festa, Ricercatrice in Diritto dell'Unione europea, Università della Campania Luigi Vanvitelli.
Angela Maria Gallo, Dottoranda di ricerca in Ordine internazionale e diritti umani, Università di Roma "La Sapienza".
Noelia Igareda González, Profesora titular de Filosofía del derecho, Universidad Autónoma de Barcelona.
Anna Iermano, Professoressa associata di Diritto internazionale, Università di Salerno.
Ángeles Jareño Leal, Catedrática de Derecho penal, Universidad de Valencia.
Maria José Jordán Díaz-Roncero, PDI Ayudante Doctora, Universitat de València.
Luigi Kalb, Professore ordinario di Procedura penale, Università di Salerno.
Elio Lo Monte, Professore ordinario di Diritto penale, Università di Salerno.
Daniela Marrani, Professoressa associata di Diritto internazionale, Università di Salerno.
Elena Martínez García, Catedrática de Derecho procesal, Universitat de València.
Mónica Martínez López-Sáez, Profesora ayudante doctora en Derecho constitucional, Universidad de València.

Claudia Morini, Professoressa associata di Diritto dell'Unione europea, Università del Salento.
Gianpaolo Maria Ruotolo, Professore ordinario di Diritto internazionale, Università di Foggia.
Mariangela Telesca, Ricercatrice di Diritto penale, Università di Salerno.
Valeria Tevere, Dottoressa di ricerca in Scienze giuridiche (curriculum internazionalistico-europeo-comparato), Università di Salerno. Funzionario pubblico.
Sara Tonolo, Professoressa ordinaria di Diritto internazionale, Università di Padova.
Juan Carlos Vegas Aguilar, Profesor de Derecho y criminología, Universidad Católica de Valencia.

Collana

Freedom, Security & Justice: European Legal Studies

1. R. Palladino, *La detenzione dei migranti. Regime europeo, competenze statali, diritti umani*, 2018.
2. A. Di Stasi (a cura di), *Tutela dei diritti fondamentali e* spazio europeo di giustizia. *L'applicazione giurisprudenziale del Titolo VI della Carta*, 2019.
3. M. Capozzolo, *Introduzione alla* libera circolazione *delle decisioni in materia civile e commerciale nello spazio giudiziario europeo. Il regolamento (UE) n. 1215/2012 e gli altri regolamenti "settoriali"*, 2019.
4. A. Di Stasi, L.S. Rossi (a cura di), *Lo spazio di libertà, sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere*, 2020 (open access).
5. A. Festa, *Lo Stato di diritto nello spazio europeo. Il ruolo dell'Unione europea e delle altre organizzazioni internazionali*, 2021.
6. I. Caracciolo, G. Cellamare, A. Di Stasi, P. Gargiulo (a cura di), *Migrazioni internazionali questioni giuridiche* aperte, 2022 (open access).
7. A. Di Stasi, M.C. Baruffi, L. Panella (a cura di), *Cittadinanza europea e cittadinanza nazionale. Sviluppi normativi e approdi giurisprudenziali*, 2023 (open access).
8. A. Di Stasi, R. Cadin, A. Iermano (a cura di), *Donne migranti e violenza di genere nel contesto giuridico internazionale ed europeo/Migrant women and gender-based violence in the International and European legal framework*, 2023 (open access).
9. M. Panebianco, *Stato di diritto e democrazia euro-globale. La crisi dell'est-ovest*, 2023 (open access).
10. A. Di Stasi, R. Palladino, A. Festa (edited by), *Migrations, Rule of Law, and European Values*, 2023 (open access).
11. A. Di Stasi, A. Iermano, A. Lang, A. Oriolo, R. Palladino, Spazio europeo di giustizia *e applicazione giurisprudenziale del Titolo VI della Carta dei Diritti fondamentali dell'Unione europea*, 2024.
12. A. Oriolo, A. R. Castaldo, A. Di Stasi, M. Nino (a cura di), *Criminalità transnazionale e Unione europea*, 2024.
13. M. Panebianco, *I gruppi globali di Stati. Diritto euro-internazionale del G7. G20 - BRICS*, 2024.

14. Di Stasi, R. E. Calabuig (a cura di) *Cyberviolenza di genere e nuove "frontiere" normative e giurisprudenziali: la direttiva UE 2024/1385/ Ciberviolencia de género y nuevas "fronteras" normativas y jurisprudenciales la directiva UE 2024/1385*, 2025.

Finito di stampare nel mese di marzo 2025
Presso la *Grafica Elettronica* (Na)

Il presente volume costituisce il risultato del lavoro svolto da una rete di ricerca multidisciplinare a cui hanno partecipato accademici dell'Università di Salerno e dell'Università di Valencia e che è stata integrata da studiosi delle Università Autonoma di Barcellona, Ca' Foscari di Venezia, Campania "Luigi Vanvitelli", Foggia, Sapienza di Roma e Udine. Questo network, integrato da operatori del diritto, ha utilizzato la lente di lettura del Diritto Internazionale Pubblico, del Diritto Internazionale Privato e del Diritto dell'Unione Europea, senza escludere i profili di Diritto Costituzionale, Criminologia, Diritto Penale e Diritto Processuale Penale. Inoltre, è stata arricchita da una indispensabile lettura sociologica con la finalità di fornire una analisi esaustiva della direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica, da prospettive molto diverse, riservando un *focus* specifico alla cyberviolenza, sempre più spesso esercitata nei confronti delle donne.

El presente volumen es fruto del trabajo realizado por una red de investigación multidisciplinar en la que han participado académicas/os de la Universidad de Salerno y de la Universidad de Valencia, y que se ha completado con académicas/os de la Universidad Autónoma de Barcelona, Ca' Foscari de Venecia, Campania "Luigi Vanvitelli", Foggia, Sapienza de Roma y Udine. Esta red, integrada por operadores jurídicos, ha sido realizada desde la óptica del Derecho Internacional Público, el Derecho Internacional Privado y el Derecho de la Unión Europea (sin excluir los perfiles de Derecho Constitucional, Criminología, Derecho Penal y Procesal). Además, se ha visto enriquecida por una imprescindible lectura sociológica y por un análisis exhaustivo de la directiva (UE) 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica desde perspectivas muy diferentes, reservando un enfoque específico en la ciberviolencia que se ejerce cada vez más contra las mujeres.

ISBN 979-12-235-0233-4

euro 60,00