unimc
UNIVERSITÀ DI MACERATA
l'umanesimo che innova

Collana del Dipartimento di Giurisprudenza
dell'Università degli Studi di Macerata

CRISTINA GRIECO

Intelligenza Artificiale e tutela degli utenti nel diritto dell'Unione europea

Editoriale Scientifica

COLLANA DEL DIPARTIMENTO
DI GIURISPRUDENZA DELL'UNIVERSITÀ
DEGLI STUDI DI MACERATA

Cristina Grieco

INTELLIGENZA ARTIFICIALE E TUTELA DEGLI UTENTI NEL DIRITTO DELL'UNIONE EUROPEA

EDITORIALE SCIENTIFICA

Volume stampato con il contributo del Dipartimento di Giurisprudenza e della Commissione di certificazione dei contratti di lavoro dell'Università degli Studi di Macerata.

Il presente volume è stato sottoposto al referaggio da parte di due esperti anonimi, esterni al Dipartimento di Giurisprudenza, appartenenti al settore scientifico-disciplinare relativo alla materia, oggetto del lavoro monografico, o a settore scientifico-disciplinare affine, designati dal Direttore del Dipartimento secondo la procedura stabilita dal regolamento della Collana del Dipartimento di Giurisprudenza (*double blind peer review*). I revisori hanno formulato un giudizio positivo sulla pubblicazione.

via San Biagio dei Librai, 39 - 80138 Napoli
www.editorialescientifica.com info@editorialescientifica.com
ISBN 979-12-5976-642-7

INDICE

PARTE I
DEFINIZIONI E REGOLAMENTAZIONE

CAPITOLO PRIMO
LA GRADUALE AFFERMAZIONE DELL'INTELLIGENZA ARTIFICIALE COME DISCIPLINA AUTONOMA IN EUROPA

CAPITOLO SECONDO
L'ATTUALE QUADRO GIURIDICO EUROPEO IN TEMA DI INTELLIGENZA ARTIFICIALE

CAPITOLO TERZO

LA NUOVA PROPOSTA DI REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE E IL QUADRO GIURIDICO EUROPEO IN MATERIA DI DIRITTI FONDAMENTALI

PARTE II
I POSSIBILI IMPATTI NEGATIVI DEI SISTEMI DI INTELLIGENZA ARTIFICIALE SU PRIVACY E NON DISCRIMINAZIONE

CAPITOLO QUARTO
INTELLIGENZA ARTIFICIALE E PRIVACY

CAPITOLO QUINTO
INTELLIGENZA ARTIFICIALE E DIVIETO DI DISCRIMINAZIONE

CONCLUSIONI

PARTE I

DEFINIZIONI E REGOLAMENTAZIONE

CAPITOLO PRIMO

LA GRADUALE AFFERMAZIONE DELL'INTELLIGENZA ARTIFICIALE COME DISCIPLINA AUTONOMA IN EUROPA

SOMMARIO. 1. Introduzione. – 2. Lo sviluppo dell'intelligenza artificiale. – 3. I tentativi di definire l'intelligenza artificiale. – 4. *Machine learning* e *deep learning* cosa sono (e perché spaventano).

1. Introduzione

Superare la resistenza al cambiamento può rivelarsi una sfida difficile. In bilico tra criticità e opportunità, una spinta forte verso l'innovazione arriva proprio dallo sviluppo incredibilmente rapido che, negli ultimi anni, sta avendo il settore dell'intelligenza artificiale.

I sistemi che fanno ricorso a pratiche algoritmiche stanno progressivamente trovando impiego in molti ambiti della società, inclusi diritto e giustizia. Essi stanno modificando in maniera significativa il modo di concepire e gestire i rapporti tra istituzioni pubbliche ma anche tra soggetti privati.

Gli incredibili passi avanti che la tecnologia sta facendo nei settori dell'apprendimento automatico e della robotica stanno riscrivendo radicalmente il rapporto uomo-macchina. Lo sviluppo di sistemi sempre più capaci di rivaleggiare con l'intelligenza umana[1] – e, in certi casi, di superarla – sta facendo emergere nuovi profili di rischio meritevoli di approfondimento[2].

[1] L. ALEXANDRE, *La guerra delle intelligenze. Intelligenza artificiale «contro» intelligenza umana*, Torino, 2018, p. 29 ss.

[2] È stato, infatti, evidenziato che «while technology offers many potentially creative opportunities for innovation and for rethinking assessment purposes, there are also numerous risks and challenges. Ethical concerns over social exclusion and new forms of digital dividedness and the increasing risks associated with big data and the rise of learning analytics» v. S. TIMMIS, P. BROADFOOT, R. SUTH-

Questo stato di cose, che genera una duplice esigenza di sicurezza[3] ma anche di controllo su questi sistemi, passa necessariamente da una regolamentazione specifica in grado di governare il cambiamento. È necessario approntare un *set* di norme chiare che garantiscano il corretto sviluppo ed impiego di questi sistemi mantenendo – al contempo – un clima di certezza giuridica idoneo a favorire il progresso tecnologico.

In tal senso, il legislatore europeo si trova a dover affrontare un panorama profondamente trasformato e sempre più mutevole. I continui cambiamenti e la velocità con la quale questi si verificano rendono difficile il ricorso a categorie giuridiche classiche e l'applicazione dei consueti paradigmi normativi[4].

ERLAND, A. OLDFIELD, *Rethinking assessment in a digital age: opportunities, challenges and risks*, in *British Educational Research Journal*, 2016, p. 454, disponibile online.

[3] Che quello della sicurezza sia un tema particolarmente sentito, soprattutto nel settore informatico, lo dimostrano due recenti atti adottati dalle istituzioni europee. Ci si riferisce, in particolare al Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 c.d. Regolamento DORA (*Digital Operational Resilience Act* – DORA), che stabilisce requisiti uniformi per la sicurezza delle reti e dei sistemi informativi delle imprese e delle organizzazioni che operano nel settore finanziario e assicurativo, nonché delle terze parti critiche che forniscono loro servizi relativi alle tecnologie dell'informazione e della comunicazione (le c.d. tecnologie ICT), necessari a resistere e, soprattutto, reagire alle minacce connesse alla sicurezza informatica. L'altro atto è la Direttiva NIS 2 – che aggiorna la Direttiva (UE) 2016/1148 (Direttiva NIS 1), ossia il primo atto legislativo a livello europeo in materia di sicurezza informatica – che introduce importanti misure in ambito di gestione dei rischi legati al tema della *cybersecurity*, obblighi di segnalazione degli incidenti informatici "significativi" per i soggetti strategici operanti nei settori individuati, ampliando il numero e la tipologia di attori coinvolti. Non più solo le aziende operanti nei settori altamente critici individuati in principio dalla Direttiva NIS1 – tra i quali ad esempio trasporti, banche e infrastrutture del mercato finanziario – ma anche soggetti parimenti qualificati come critici ma operanti in ambiti differenti, quali ad esempio i fornitori digitali (mercati online, motori di ricerca online, piattaforme di servizi di *social networking*), i gestori di rifiuti, i servizi postali e le organizzazioni di ricerca.

[4] L'imporsi delle nuove tecnologie sfida i canoni ordinari che regolano la

Le nuove tecnologie, in costante evoluzione, danno vita a transazioni e rapporti sempre più smaterializzati e a-territoriali[5] in cui cambia il ruolo stesso della persona[6]. Gli individui diventano, per alcuni aspetti, sempre più protagonisti e interconnessi, pur nella loro dimensione individualistica e isolata[7], e, nello stesso tempo, sempre più bisognosi di tutela perché inseriti in dinamiche di mercato che, il più delle volte, sfuggono al loro controllo.

2. Lo sviluppo dell'intelligenza artificiale

Convenzionalmente la nascita ufficiale dell'intelligenza artificia-

formazione del diritto positivo. È stato osservato da G. BOMBELLI, *Tecnologia, diritto, antropologia: appunti sull'Information (Knowledge) Society*, in M. Megale (a cura di), *ICT e diritto nella società dell'informazione*, Torino, 2012, pp. 18-21, che l'evoluzione tecnologica ha portato il diritto a focalizzarsi sulla produzione di «regole» invece che di «norme». La differenza è sostanziale poiché mentre le prime presuppongono «una visione unitaria dei processi sociali e, quindi, dell'ordinamento giuridico», le seconde sono prive di una visione d'insieme e lavorano in una sorta di situazione emergenziale dando vita a «una serie di interventi contingenti finalizzati alla mera imposizione di 'limiti'». Questo anche perché la *tecnologia* «diviene sempre più difficilmente interpretabile a partire dalle categorie giuridiche tradizionali e, al contempo, tende quasi ad autoistituirsi, in via autonoma, in termini 'giuridici', fino ad allestire e legittimare modelli interpretativi riferibili all'intera società». In dottrina è stato osservato che il progresso tecnologico che spinge la digitalizzazione verso frontiere sconosciute porta con sé quelli che oggi vengono comunemente definiti «disruptive effects» C. TWIGG-FLESNER, *Disruptive Technology – Disruptive Law? How the Digital Revolution Affects (Contract) Law,* in A. De Franceschi (eds.), *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution, Cambridge-Antwerp-Portland, Intersentia*, 2016, pp. 21-48.

[5] La riflessione è di F. FERRI, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Trento, 2022, p. 25 ss.

[6] Di «questione eminentemente transnazionale, e come tale difficilmente ricomponibile ricorrendo alla tradizione giuridica singolo-nazionale», parla A. VENANZONI, *Intersezioni costituzionali – Internet e Intelligenze Artificiali tra ordine spontaneo, natura delle cose digitale e garanzia dei diritti fondamentali*, in *Forum di Quaderni Costituzionali*, 27 aprile 2018, p. 4.

[7] Floridi ha utilizzato l'espressione *onlife*, si veda L. FLORIDI, *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Berlino, 2015, p. 74 ss.

le come disciplina scientifica viene associata ad un importante seminario[8] tenutosi nel 1956 presso il Dartmouth College di Hanover nel New Hampshire e il padre fondatore viene identificato in John McCarthy[9]. In occasione di quell'incontro, McCarthy delimitò i confini dell'intelligenza artificiale usando le seguenti parole «for the present purpose the artificial intelligence problem is taken to be that of making a machine behave in ways that would be called intelligent if a human were so behaving»[10].

A partire da quel seminario, l'intelligenza artificiale, raccogliendo i contributi sviluppati negli anni precedenti ma con uno sguardo già orientato verso le future potenzialità del settore, iniziò ad essere considerata una disciplina scientifica a tutti gli effetti[11].

[8] Nell'estate di quell'anno un gruppo di studiosi si riunì al Dartmouth College con lo scopo di esaminare, come apparve nella proposta per il seminario redatta l'anno precedente, la congettura che ogni aspetto dell'intelligenza potesse essere, in linea di principio, descritto in modo tanto preciso da far sì che una macchina lo simuli. Il seminario aveva le caratteristiche del *brainstorming*, ossia di un dibattito aperto e poco strutturato dal quale emerse, attraverso le discussioni comuni, un nuovo approccio teoretico teso a definire la possibilità della riproduzione dell'intelligenza da parte di un elaboratore elettronico. Il seminario si proponeva inoltre di raccogliere e analizzare i programmi caratterizzati da prestazioni definibili come intelligenti – come il *Logic theorist* (LT) di Allen Newell, Bernard Shaw e Herbert A. Simon in grado di dimostrare teoremi della logica del primo ordine – e di proporre una serie di obiettivi ambiziosi che avrebbero dovuto essere verificati dieci anni dopo in un nuovo incontro.

[9] Il convegno fu organizzato proprio da John McCarthy, che ai tempi rivestiva il ruolo di assistente universitario di matematica presso il Dartmouth College, insieme a Marvin Minsky, ricercatore di matematica e neurologia ad Harvard, Nathaniel Rochester, direttore della ricerca sull'informazione in un centro ricerche dell'IBM, e Claude E. Shannon, il matematico già famoso per la teoria dell'informazione, che lavorava presso i *Bell telephone laboratories*.

[10] J. MCCARTHY, M. L. MINSKY, N. ROCHESTER, C. E. SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955, in *AI Magazine Volume 27 Number 4,* 2006, disponibile online.

[11] Sebbene il 1956 sia unanimemente riconosciuto dalla comunità scientifica come l'anno nel quale viene datata la nascita di questa disciplina, in realtà molto spesso, quando si parla di storia dell'intelligenza artificiale, si fa riferimento anche alla cibernetica e all'avvento dei primi calcolatori elettronici. Nell'operazione di ricostruzione storica, vengono di sovente ricordati anche i contributi di Charles Babbage con la sua macchina analitica, di Gottfried Wilhelm Leibniz con il suo

La riflessione muove dalla tradizione formalistica di indagine sulla mente e preconizza che la prestazione artificiale faccia parte della pratica umana, esattamente come quella naturale, ma orientata nella direzione di un continuo tentativo dell'uomo di imitare e di riprodurre sé stesso e la natura. A motivo di ciò, la ricerca in questo nuovo settore ha ereditato molte idee, punti di vista e tecniche da altre discipline: *in primis* la matematica ma, in maniera significativa, anche la psicologia[12] e la filosofia. Nondimeno, sono senza dubbio la cibernetica e l'informatica ad aver aperto la strada alla nascita ufficiale dell'intelligenza artificiale.

All'inizio degli anni quaranta del secolo scorso si cominciò a indicare con il termine cibernetica lo studio sistematico dei processi riguardanti la comunicazione e il controllo sia negli animali sia nelle macchine[13]. Tuttavia, nonostante taluni successi iniziali, il tempo di questa disciplina sembrò presto volgere al termine perché dopo pochi anni, ovvero intorno alla metà degli anni cinquanta del novecento, le risorse economiche furono quasi completamente convogliate verso il più moderno settore dell'intelligenza artificiale.

progetto di meccanizzazione della ragione, ma anche di Raimondo Lullo con la macchina logica, fino ad arrivare persino agli automi semoventi di Erone di Alessandria v. F. AMIGONI, V. SCHIAFFONATI, M. SOMALVICO, voce *Storia dell'Intelligenza artificiale* in Enciclopedia della Scienza e della Tecnica (2008), Treccani online.

[12] In particolare, si devono alla filosofia, gli esiti del dibattito sulla natura dell'intelligenza e della razionalità; alla psicologia, l'analisi delle relazioni fra conoscenza e azione e, alla matematica, l'approccio formale basato sulla logica.

[13] Nel 1949, Donald O. Hebb dimostrò come una semplice regola di aggiornamento utilizzabile per modificare le forze di connessione fra i neuroni potesse dare luogo a processi di apprendimento. Warren S. McCulloch e Walter Pitts proposero, nel 1943, il primo modello di neuroni artificiali, attingendo alla conoscenza della fisiologia e delle funzioni di base dei neuroni, alla logica proposizionale e alla teoria della computabilità di Alan M. Turing. L'idea alla base del progetto cibernetico era di studiare i meccanismi dell'autoregolazione e del controllo presenti sia negli organismi viventi sia nelle macchine con retroazione, in grado cioè di rispondere in modo adattativo alle sollecitazioni dell'ambiente modificando il proprio comportamento. Uno dei risultati più significativi consentì di mostrare come ogni funzione calcolabile potesse essere elaborata da una qualche rete di neuroni connessi.

Lo sviluppo di tale settore richiedeva però un sistema nel quale riprodurre, emulandoli, i fenomeni di funzionamento tipici dell'intelligenza umana.

Con l'avvento dei primi elaboratori elettronici, negli anni segnati dalla seconda guerra mondiale[14], l'interesse verso il settore dell'intelligenza artificiale aumentò e si arrivò alla definizione del programma di ricerca poi presentato nel ricordato incontro di Dartmouth. Gli anni successivi al seminario furono caratterizzati da grandi aspettative, alimentate anche dai successi dovuti ai rapidissimi miglioramenti tecnologici dei supporti informatici utilizzati[15].

Ben presto, tuttavia, i ricercatori cominciarono a incontrare le prime difficoltà: metodi adatti ad essere applicati a casi semplici si rivelarono totalmente inadeguati in contesti più complessi e ampi. Le grandi aspettative iniziali dovettero fare i conti con il fallimento

[14] Alla base del meccanismo di funzionamento vi è proprio il concetto di macchina di Turing, un sistema teorico in grado di trovarsi in un numero finito di stati diversi e di eseguire un numero limitato di azioni al fine di poter esprimere qualsiasi tipo di procedura definita. La macchina di Turing è composta da un nastro di lunghezza infinita (suddiviso in celle lette da una testina, che può spostarsi di una cella avanti o indietro) e da un organo di controllo capace di leggere il simbolo che si trova nella cella sotto la testina. A un dato istante, l'azione che la macchina intraprende è determinata dal simbolo letto e dalla configurazione in cui la macchina si trova in quel momento. Dopo aver letto il simbolo stampato sulla cella, la testina può compiere due operazioni alternative (prima di spostarsi su un simbolo adiacente): lasciare il simbolo così com'è oppure cancellarlo e stamparne un altro. Il concetto di algoritmo può essere ricondotto proprio alla sequenza di operazioni svolte dalla macchina di Turing. Sempre ad A. M. TURING, *Computing Machinery and Intelligence*, *Oxford*, 1950, pp. 433-460, si deve l'ideazione del famoso *test* che porta il suo nome per verificare la presenza o meno di intelligenza in una macchina.

[15] Indicativamente possono essere rilevate due tendenze: da una parte il gruppo guidato da Newell, Shaw e Simon interessato alla simulazione dei processi cognitivi umani per mezzo dell'elaboratore, che con il GPS (*General problem solver*) del 1958 intendeva estendere l'ambito delle applicazioni del LT al di là di quelle puramente logiche (paradigma della simulazione); dall'altra quanti dedicavano le loro forze al raggiungimento della migliore prestazione possibile per i programmi, indipendentemente dal fatto che questa potesse essere realizzata adottando procedure più o meno imitative dei procedimenti seguiti dall'uomo (paradigma della prestazione o dell'emulazione).

dei progetti di traduzione automatica tra linguaggi naturali. A tutto ciò si aggiunse l'incapacità di trattare l'esplosione combinatoria. Ci si rese conto, ben presto, che l'estensione a problemi più ampi non si poteva affrontare semplicemente mediante l'impiego di *hardware* più veloci e memorie più estese, poiché esistevano insormontabili limitazioni innate alla loro stessa natura intrinseca.

Queste difficoltà condussero a concentrarsi su aree più ristrette di competenza.

Paradossalmente, fu proprio a partire da questo ridimensionamento delle aspettative che nacque l'intelligenza artificiale come settore industriale. Nel 1982 venne progettato il primo sistema commercializzabile finalizzato a supportare le configurazioni di ordini per nuovi sistemi di elaborazione.

L'intelligenza artificiale entrò così a far parte di un ampio programma che includeva la progettazione di *chip* e la ricerca relativa alle interfacce uomo-macchina. Parallelamente, si assistette al ritorno dell'approccio basato sulle reti neurali[16].

Intorno al 1985, quattro differenti gruppi di ricerca rielaborarono un algoritmo di apprendimento, scoperto anni prima, basato sulla retro propagazione dell'errore e lo applicarono con successo a molti problemi di apprendimento nei settori dell'informatica e dell'ingegneria.

Il ritorno a questo approccio fu promosso anche dalla nascita di una nuova disciplina: le scienze cognitive. Si tratta di un connubio particolarmente interessante che ha raccolto molte delle ambizioni di una parte della psicologia e di quel settore dell'intelligenza artificiale, più teorico e meno ingegneristico, che considerava la macchina uno strumento privilegiato per lo studio della mente.

Negli ultimi anni, l'intelligenza artificiale è stata caratterizzata

[16] Nel campo dell'apprendimento automatico, una rete neurale artificiale è un modello computazionale composto da "neuroni" artificiali, ispirato vagamente dalla semplificazione di una rete neurale biologica dove i neuroni sono organizzati in una serie di livelli e sono collegati solo con quelli dei livelli immediatamente inferiori e superiori. All'intera struttura viene indicato un obiettivo, come ad esempio riconoscere un volto, e riceve una serie di *input* che salgono verso l'alto ed il basso secondo una gerarchia per poi "accordarsi" e raggiungere l'obiettivo richiesto.

da numerosi cambiamenti sia a livello metodologico sia a livello contenutistico. L'attenzione è stata rivolta a problemi reali e molto più delimitati. Ciò che resta della caratterizzazione dell'intelligenza artificiale delle origini è la pluralità di approcci.

Accanto al tradizionale metodo logico della rappresentazione della conoscenza, infatti, ha acquistato peso crescente l'approccio sub simbolico, concepito per dotare i sistemi di intelligenza artificiale di prestazioni intelligenti anche senza una rappresentazione dettagliata della conoscenza. I confini della disciplina si sono estesi nella direzione di una visione dell'intelligenza non limitata al solo pensiero logico bensì sempre più orientata verso l'agire razionale[17].

Quello dell'intelligenza artificiale resta ancora oggi un settore sperimentale, scientifico ed ingegneristico[18]. Al momento presente l'obiettivo di questa disciplina non è la simulazione dell'intelligenza umana bensì la sua emulazione. Tramite le prestazioni intelligenti che vengono ottenute dalle macchine mediante l'impiego di meccanismi propri, non necessariamente uguali a quelli utilizzati dall'uomo, si punta a dare vita a prestazioni che sono qualitativamente equivalenti e quantitativamente superiori a quelle che potrebbe fornire un essere umano.

Paradossalmente oggi, dopo tutti gli sforzi compiuti per raggiungere tale obiettivo, è proprio questo aspetto a destare maggiore preoccupazione.

3. I tentativi di definire l'intelligenza artificiale

L'evoluzione storica dell'intelligenza artificiale ha consentito al-

[17] Cfr. F. AMIGONI, V. SCHIAFFONATI, M. SOMALVICO, *Voce Intelligenza artificiale*, in *Enciclopedia della Scienza e della Tecnica*, 2008, disponibile online.

[18] Somalvico, pioniere dell'intelligenza artificiale in Italia, sostiene che l'intelligenza artificiale sia «quella disciplina, appartenente all'informatica, che studia i fondamenti teorici, le metodologie e le tecniche che consentono di progettare sistemi *hardware* e sistemi di programmi *software* capaci di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana», M. SOMALVICO, *Intelligenza artificiale*, *Scienza&Vita*, n. 8, Milano, 1987, p. 20 ss.

la disciplina di mutare e di evolversi sino ad arrivare ad oggi circondata da un alone di diffidenza e di curiosità.

L'interesse intorno a questo settore è tale che di sovente *robot* e intelligenza artificiale sono divenuti una proficua fonte d'ispirazione per scrittori e produttori di ogni genere. Spesso, infatti, nella filmografia e nella letteratura moderne, questi diventano i protagonisti di un futuro distopico in cui all'umanità viene riservato un ruolo sempre più marginale e i sistemi di intelligenza artificiale, divenuti ormai più intelligenti e capaci dell'uomo, prendono il sopravvento.

È pur vero che lo scrittore russo Isaac Asimov aveva già aveva già ipotizzato siffatta evoluzione quando, all'interno dei suoi libri all'inizio degli anni quaranta, teorizzava le tre leggi della robotica[19].

Dalla fantascienza alla realtà il passo è più breve di quanto si pensi. Al giorno d'oggi, infatti, parole come metaverso, algoritmo, *blockchain*, *machine learning*, *deep learning* e intelligenza artificiale sono entrate prepotentemente nella quotidianità.

Eppure fornire una definizione univoca di intelligenza artificiale è tutt'altro che un compito semplice e, ancora oggi, non può dirsi che ne esista una generalmente riconosciuta. A tale proposito è stato osservato come persino Wikipedia, l'enciclopedia libera più vasta al mondo, si sia accontentata di una definizione tautologica che poco valore aggiunto apporta alla discussione sul tema[20].

[19] Secondo le quali: 1. un *robot* non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno; 2. un *robot* deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla prima legge; 3. un *robot* deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la prima o con la seconda legge, I. ASIMOV, *Robot Visions*, Londra, 1990 (ristampa). Oggi queste leggi sono applicate nell'*Algorithmic Society* cfr. J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data,* in *Faculty Scholarship Series,* 2017, p. 1219, definita come «a society organized around social and economic decision-making by algorithms, robots, and Al agents, who not only make the decisions but also, in some cases, carry them out».

[20] Di fronte alla sfida definitoria per eccellenza Wikipedia si limita ad una tautologia «Artificial intelligence (AI) is intelligence demonstrated by machines, as opposed to natural intelligence displayed by animals including humans». L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano,

Anche alcune istituzioni, operanti all'interno di sistemi normativi diversi, si sono cimentate nel compito di fornire una definizione di intelligenza artificiale[21].

Tuttavia, a prescindere dalle definizioni, su cui comunque ci si soffermerà più avanti nel presente scritto, è indubbio che lo sviluppo incredibilmente rapido che sta avendo l'intelligenza artificiale stia generando nuove opportunità e, al contempo, rischi inediti in tutti gli ambiti della società, non ultimi diritto e giustizia[22].

Il binomio diritto e intelligenza artificiale presenta, infatti, delle criticità[23] e restituisce problematiche e interrogativi del tutto nuovi destinati ad incidere sugli effetti che la rivoluzione digitale in atto avrà sulla tutela dei diritti dei singoli e sullo sviluppo del ragionamento giuridico[24], particolarmente in vista del così detto *Web 5.0* o

2022, p. 40 e ss. L'A. osserva come questa definizione, certamente vera, risulti anche del tutto inutile.

[21] In questo senso si possono menzionare gli sforzi operati dalla Commissione europea che ha definito l'intelligenza artificiale come quei «sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia per raggiungere specifici obiettivi» *Comunicazione l'intelligenza artificiale per l'Europa*, 25 aprile 2018, COM (2018) 237 def.). Anche il Consiglio d'Europa che ha istituito una *Inter-disciplinary Commitee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence* (MSI-AUT), in uno studio pubblicato nel settembre 2019, DGI(2019)05, disponibile online, si è impegnato per tentare di fornire una definizione di intelligenza artificiale e si è espresso nei seguenti termini «a set of advanced general-purpose technologies which use techniques from statistics, computer science and cognitive psichology to enable machines to do highly complex tasks efficiently».

[22] Per alcune interessanti riflessioni sulla prevenzione della criminalità utilizzando la tecnologia si vedano le riflessioni di J.T. KRAFT, *Big Data Analytics, Rising Crime, and Fourth Amendment*, *Universit of Illinois Journal of Law, Technology & Policy*, 2017, pp. 249-271.

[23] Non è casuale che sistemi algoritmici abbiano trovato veloce impiego in servizi quali *l'Information Retrieval*, che si occupa della rappresentazione, memorizzazione e organizzazione delle informazioni di testo al fine di renderne più agevole la ricerca da parte dell'utente interessato, e il *Legal Reasoning,* ovvero il ragionamento giuridico che viene utilizzato per sostenere una determinata posizione in giudizio o che conduce ad assumere dei provvedimenti.

[24] Per esempio la decisione di un giudice automatico potrebbe essere influen-

Emotional Web[25]. Al contempo, nonostante i timori legati alle capacità di auto apprendimento di questi sistemi, la cui evoluzione risulta non sempre prevedibile, è innegabile che l'intelligenza artificiale stia assumendo un ruolo sempre più cruciale nel percorso di trasformazione digitale della società e stia modificando il modo di approcciare alcune delle sfide decisive e urgenti dei tempi moderni, come i cambiamenti climatici[26], la sanità, la digitalizzazione della pubblica amministrazione e la tutela dell'ambiente.

Tali timori risultano accresciuti anche da un quadro giuridico frammentario e lacunoso che non consente agli utenti e agli operatori di fare affidamento su norme certe[27].

Dal punto di vista della riflessione giuridica, la prepotente e rapidissima diffusione di questi sistemi pone inoltre delle questioni del tutto nuove che investono soprattutto gli ambiti della protezione dei dati personali e della non discriminazione.

zata anche dagli aspetti emotivi, così come accade oggi nell'interazione tra gli umani. Si vedano in dottrina le riflessioni di E. CALZOLAIO, *Intelligenza artificiale ed autonomia della decisione: problemi e sfide*, in E. Calzolaio (a cura di) *La decisione nel prisma dell'intelligenza artificiale*, Padova, 2020, p. 1 e ss. In questo scenario in che modo un avvocato umano sarà in grado di persuadere un giudice automatico? Cfr. E. FRANCESCONI, *Intelligenza artificiale e diritto: tra scienza e fantascienza*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 11.

[25] È lo stadio in cui le machine arriveranno a tenere conto anche delle emozioni. Cfr. K. PATEL, *Incremental journey for world wide web: Introduced with web 1.0 to recent web 5.0 – a survey paper*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013, 3, 10, p. 410; R. PENROSE, *La mente nuova dell'imperatore*, Milano, 1992. L'A. evidenzia che "la mente umana non è algoritmica" ovvero non è una macchina di Turing. Per alcune riflessioni interessanti sul rapporto uomo-macchina v. P. STANZIONE, *La democrazia alla sfida degli algoritmi*, in Repubblica, 18 aprile 2021, disponibile online.

[26] *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - The European Green Deal* COM/2019/640*final*. Si tratta di quella strategia multisettoriale che punta, da una parte, a trasformare la sfida legata alla sostenibilità in opportunità e, dall'altra, a rendere l'Europa il primo continente ad impatto zero.

[27] V. *infra* cap. II.

In un simile scenario, è stato puntualmente osservato che «the real challenge is no longer digital innovation, but the governance of the digital»[28].

Per ciò che riguarda specificamente l'Unione europea, si percepisce l'urgenza nei tentativi di governare la rivoluzione tecnologica in atto per cercare di trarne il massimo vantaggio economico assicurando, al contempo, un'adeguata salvaguardia dei diritti e dei principi posti alla base dell'ordinamento sovranazionale[29].

4. *Machine learning* e *deep learning:* cosa sono (e perché spaventano)

Gran parte dei sistemi di intelligenza artificiale più recenti funzionano con il *machine learning* (*ML*), ovvero applicando meccanismi di apprendimento automatico[30]. Per dirla in parole semplici,

[28] L. FLORIDI, *Soft Ethics and the Governance of the Digital* and the General Data Protection Regulation, in *Philos Trans A Math Phys Eng Sci*., 2018, disponibile online.

[29] Si è già assistito a situazioni in cui l'utilizzo di algoritmi ha dato vita a dinamiche pregiudizievoli e a disparità di trattamento. Per alcune riflessioni si veda E. CIRONE, *Big Data e tutela dei diritti fondamentali*, in S. Dorigo (a cura di) *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., p. 143 e ss. Ha fatto molto discutere il licenziamento di Timnit Gebru, che si occupava di etica dell'intelligenza artificiale in Google. In un duro articolo pubblicato su Fast Company, e disponibile online, il vice direttore della sezione dedicata alla tecnologia, Katharine Schwab, sostiene che il licenziamento della Gebru, una delle poche donne nere assunte nell'azienda di *Mountain View*, sia stato un modo per silenziare la sua voce critica circa un utilizzo delle tecnologie di intelligenza artificiale da parte di Google non etico.

[30] Ad utilizzare per primo questa terminologia fu Arthur Samuel nel 1959 che definì il *machine learning* come quel «campo di studio che dà ai *computer* la possibilità di apprendere senza essere programmato esplicitamente». Aurélien Géron ha definito il *machine learning* «the science (and art) of programming computers so they can learn from data», A. GÉRON, *Hands-On Machine Learning with Scikit-Learn, Keras, and Tensorflow: Concepts, Tools, and Techniques to Build Intelligent Systems,* Sebastopol, 2019, p. 4. Ad oggi però, la definizione più accreditata dalla comunità scientifica è quella fornita da Tom Mitchell secondo cui «A computer program is said to learn from experience E with respect to some class of tasks T

con il termine *machine learning* si identifica quel settore che si concentra su come far svolgere ai computer specifici compiti senza la necessità di essere specificamente programmati.

In effetti, il concetto basilare che si cela dietro al *machine learning* è che sia possibile creare algoritmi che siano in grado di fare previsioni apprendendo dai dati. Questa modalità consente ai sistemi di eseguire dei comandi sfruttando l'apprendimento derivante dall'esperienza[31]. Tali algoritmi "adattivi" dovrebbero essere in

and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E», T. MITCHELL*, Machine Learning,* New York, 1997, p. 20.

[31] Gli algoritmi di *machine learning* rientrano generalmente in cinque categorie, a seconda della quantità e tipo di supervisione umana che ricevono durante la fase di *training*. In base al tipo di funzionamento vengono individuati i seguenti sottoinsiemi che consentono di operare una classificazione più dettagliata:

Supervised learning – apprendimento supervisionato: al sistema (che può essere un algoritmo, un *computer*, un *software*) vengono forniti sia dei dati di input sia le informazioni relative ai risultati. Sarà il sistema ad identificare una regola che colleghi i dati in ingresso con quelli in uscita, in modo da poter poi riutilizzare tale regola per altri compiti simili. Un esempio è la classificazione dei tumori sulla base delle loro caratteristiche.

Unsupervised learning – apprendimento non supervisionato: I dati di input non sono etichettati e il sistema apprende autonomamente la struttura logica partendo dai dati forniti. Un esempio di apprendimento non supervisionato è il rivelamento di anomalie nelle transazioni con carte di credito.

Semi-supervised learning – apprendimento semi-supervisionato: è una combinazione dei due approcci precedenti. Al sistema vengono forniti dati etichettati e non. Il riconoscimento facciale tramite foto di *Facebook* e *Google*, sono applicazioni che utilizzano questo approccio.

Reinforcement learning – Apprendimento per rinforzo: è principalmente un'area di ricerca. L'apprendimento per rinforzo si verifica quando un sistema riceve dati in un ambiente specifico e poi impara a massimizzare i risultati. Il computer *DeepMind AlphaGo* di Google, che ha imparato con successo a padroneggiare il gioco Go, è un recente esempio di questa tecnica.

Transfer learning – apprendimento trasferito: Si tratta di riutilizzare un modello precedentemente addestrato per la risoluzione di un problema diverso ma strettamente correlato. Lukas Biewald descrive un esempio di apprendimento trasferito in cui un modello di *deep learning* è stato addestrato su milioni di immagini di gatti e poi 'perfezionato' per rilevare alcuni melanomi in campo medico.

grado di ottimizzare e migliorare i risultati restituiti all'aumentare delle informazioni e delle esperienze acquisite[32].

In questa direzione, la tecnologia, negli ultimi anni, ha compiuto grandi passi avanti, anche grazie all'enorme disponibilità di dati[33] e a reti neurali sempre più estese. Per questo le prestazioni e i risultati offerti da questi sistemi risultano sempre più efficienti ed accurati.

Il *deep learning* (*DL*) rappresenta una sottocategoria del *machine learning* e si riferisce a quel settore che utilizza algoritmi modellati sul funzionamento e sulla struttura del cervello umano e che, per questo, vengono definiti reti neurali artificiali[34]. In altre parole, il *deep learning*, utilizzando sistemi artificiali, simula i processi di apprendimento tipici del cervello umano con il fine ultimo di insegnare alle macchine non solo ad apprendere autonomamente a partire da determinati *set* di dati – come avviene nel *machine learning* –

[32] Esempi di *machine learning* sono: i sistemi di raccomandazione che imparano dal comportamento e dalle preferenze degli utenti per suggerire prodotti a gruppi di utenti, usato per esempio da *Netfix, Amazon* o *Spotify*; le auto a guida autonoma che con il *machine learning* imparano a riconoscere l'ambiente e determinare un comportamento; la ricerca scientifica in campo medico che permette di fare previsioni su epidemie, diagnosi di tumori. Altri esempi sono i filtri *antispam* dell'*email* o l'auto compilatore di Google.

[33] Definiti in modo significativo e per nulla esagerato il "nuovo petrolio" dall'*Economist*, visto e considerato che costituiscono la principale risorsa dell'economia digitale (si veda *The world's most valuable resource is no longer oil, but data*, pubblicato il 6 maggio 2017). Sul tema si vedano i contributi di: S. TOMMASI, *Algoritmi e nuove forme di discriminazione: Uno sguardo al diritto europeo*, in *Revista de Direito Brasileira*, v. 27, n. 10, 2020, p.112-129; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. Inf.,* 2018, 4-5, pp. 689-726; G. FINOCCHIARO, *Considerazioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo (a cura di), *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, Torino, 2021, p. 332 e ss.

[34] Cfr. I. GOODFELLOW, Y. BENGIO, A. COURVILLE, *Deep Learning*, Cambridge, 2016, p. 164 ss. Algoritmi di questo tipo sono ad esempio utilizzati nel riconoscimento automatico della lingua parlata e dei volti, nella *computer vision* e nella bioinformatica, ovvero per descrivere dal punto di vista numerico e statistico determinati fenomeni biologici.

ma a farlo in maniera più profonda, per creare, come *output,* un maggior numero di livelli di astrazione[35].

La caratteristica peculiare del *deep learning*, che lo differenzia dal *machine learning,* è quindi la scalabilità: i sistemi di apprendimento profondo, infatti, sono in grado di migliorare le proprie prestazioni all'aumentare dei dati in loro possesso, mentre i sistemi di apprendimento propri del *machine learning* lavorano per obiettivi e si fermano una volta raggiunti i livelli di *performance* attesi. La differenza è da rinvenire anche nel fatto che nei sistemi di *machine learning,* le caratteristiche di un determinato oggetto vengono estratte e selezionate manualmente con lo scopo di creare un modello che sia in grado di categorizzare gli oggetti sulla base del riconoscimento e della classificazione di quelle caratteristiche, nei sistemi di *deep learning* la rete neurale apprende in modo autonomo come analizzare dati grezzi per svolgere in maniera efficiente un determinato compito.

Nondimeno, essendo i dati la base imprescindibile per il funzionamento di entrambe le tipologie di sistemi, è fondamentale che quelli utilizzati per addestrare gli algoritmi siano quanto più possibile scevri da errori oltre che sufficientemente ampi e diversificati. In caso contrario, sarà molto più difficile per il sistema trovare modelli che possano funzionare correttamente e si rischia di cadere nella trappola dell'*overfitting*, cioè di modelli che elaborano correttamente i dati di addestramento ma restituiscono risultati poco accurati.

È proprio quest'ultimo aspetto a preoccupare. Ciò su cui si fa affidamento quando si pensa al *machine learning* e al *deep learning* è la capacità dell'algoritmo, partendo da *set* di dati immessi, di apprendere autonomamente. Erroneamente, tuttavia, si dà altresì per certo che tali sistemi siano anche in grado di migliorarsi e di "imparare dai propri errori". Sovente si parte dell'assunto che, in quanto "macchine", gli algoritmi che consentono alle tecnologie di intelli-

[35] Si veda H. SHIN, H. R. ROTH, M. GAO, L. LU, Z. XU, I. NOGUES, J. YAO, D. MOLLURA, R. M. SUMMERS, *Deep Convolutional Neural Networks for Computer-Aided Detection: CNN Architectures, Dataset Characteristics and Transfer Learning*, 2016, disponibile online.

genza artificiale di funzionare siano caratterizzati da neutralità e obiettività: ovvero, che non siano passibili di errore.

Spesso si sottovaluta che tali tecnologie sono sempre progettate da esseri umani e si nutrono dei dati che gli stessi sviluppatori immettono nel sistema. Per questo non è raro che le stesse riflettano distorsioni e discriminazioni sociali e culturali, siano esse volontarie o meno[36].

Gli algoritmi lavorano partendo da *set* di dati storici, collegandoli in modo statistico[37]. Ne consegue che la decisione finale assunta, seppur elaborata da un sistema algoritmico correttamente funzionante, potrebbe comunque risultare incorretta. Ciò è vero soprattutto in relazione a casi singoli, visto che la scienza statistica è maggiormente idonea ad indagare fenomeni collettivi e a restituire risultati quantitativi e qualitativi meno accurati e attendibili laddove la si applichi a singoli casi[38].

Per garantire un impiego quanto più possibile equo ed efficiente di tali nuovi tecnologie dunque, la selezione accurata dei dati da immettere nel sistema risulta essere un passaggio assolutamente

[36] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997, p. 28. L'A. ha osservato che la tesi della neutralità della tecnologia, sicuramente importante per sottolineare la responsabilità di chi la adopera, trascura il fatto che il concreto ruolo di una tecnologia deriva anzitutto dalla sua forma e dalle sue specifiche modalità d'uso, che contribuiscono a definirne senso e portata sociale. Vi sono effetti che si producono per il solo fatto che si sceglie di ricorrervi.

[37] G. SARTOR, *Artificial Intelligence: Challenges For Eu Citizens And Consumers*, gennaio 2019, in *Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies,* disponibile online, l'A. evidenzia che «this reliance on past practices or assessments may be based on exclusion and prejudice and lead to unfair discrimination».

[38] «Il calcolo delle probabilità, e la statistica a mezzo del calcolo delle probabilità, anche se applicati a masse di casi, non possono mai portare a conclusioni sicure, ma solo a conclusioni probabili. Possono legittimare dei dubbi più o meno forti - e questa è certamente una funzione utile - ma non possono mai scioglierli in modo definitivo. Possono fornire non «testi di significatività», ma «elementi di sospetto» C. GINI, *I pericoli della Statistica*, Relazione inaugurale della prima riunione scientifica della Società Italiana di Statistica, Pisa, 9 ottobre 1939, disponibile online.

cruciale. I *set* di dati devono essere di altissima qualità, sufficientemente rappresentativi in modo da (tentare) di non riflettere preesistenti aspettative sociali e culturali[39], non perpetrare distorsioni strutturali e non restituire decisioni, anche solo potenzialmente, discriminatorie[40].

Peraltro è già stato osservato che, al momento attuale, le voci più forti che discutono dei potenziali pericoli dell'intelligenza artificiale sono quelle di uomini bianchi e mediamente benestanti, per i quali l'unico rischio che potrebbe configurarsi è l'ascesa futura di un "nuovo predatore" più intelligente. Mentre per coloro che quotidianamente lottano contro emarginazione e pregiudizi, i possibili rischi connessi allo sviluppo di tali tecnologie sono già oggi una conseguenza potenziale dell'impiego di sistemi di intelligenza artificiale[41].

Come si avrà modo di approfondire nel corso del presente lavoro, è già nelle prime fasi della programmazione e dello sviluppo dell'algoritmo, infatti, che possono porsi le basi per il verificarsi di discriminazioni, dirette o indirette, ad esempio qualora venga ordinato al sistema di includere nel *set* di dati che conducono alla decisione alcune caratteristiche legate tradizionalmente a scelte discriminatorie.

Alla luce delle criticità che potrebbero emergere e visto l'impiego crescente di tali tecnologie in molti e diversificati ambiti, appare dunque cruciale che lo sviluppo di tali sistemi, destinati a diventare un volano fondamentale per l'economia moderna, sia sostenuto e accompagnato da un processo di adeguamento organizzativo e normativo a tutto campo.

[39] Si rimanda a *infra* cap. V.

[40] Si veda *infra* cap. IV e S. TOMMASI, *Algoritmi e nuove forme di discriminazione: Uno sguardo al diritto europeo*, cit., p. 114.

[41] K. CRAWFORD, *Artificial Intelligence's White Guy Problem,* 25 giugno 2016*,* in *New York Times,* disponibile online, «Currently the loudest voices debating the potential dangers of superintelligence are affluent white men, and, perhaps for them, the biggest threat is the rise of an artificially intelligent apex predator. But for those who already face marginalization or bias, the threats are here».

CAPITOLO SECONDO

L'ATTUALE QUADRO GIURIDICO EUROPEO IN TEMA DI INTELLIGENZA ARTIFICIALE

SOMMARIO. 1. Introduzione. – 2. La CEDU e le linee guida del Consiglio d'Europa in tema di intelligenza artificiale. – 3. La posizione del Parlamento europeo. La Carta sulla Robotica e la Risoluzione sulle implicazioni dei *Big Data* per i diritti fondamentali. – 4. Le linee guida, il libro bianco e la dichiarazione europea sui diritti e i principi digitali per il decennio digitale della Commissione europea.

1. Introduzione

Ravvisando nelle tecnologie di intelligenza artificiale una grande opportunità ma, allo stesso tempo, dei potenziali rischi, l'Unione europea, negli ultimi anni, ha iniziato ad interessarsi in modo crescente del tema.

Si sono già registrate molte ed eterogenee iniziative a diversi livelli, anche se, all'inizio, queste[1] risultavano caratterizzate da un approccio perlopiù settoriale[2], orientato soprattutto a supportare la ricerca scientifica[3]. Recentemente le istituzioni sono però intervenute per correggere il tiro, sottolineando che l'obiettivo finale a cui si deve puntare è proprio l'uniformità normativa.

[1] V. *infra* par. 2, 3 e 4.

[2] La Commissione europea ha già finanziato alcuni progetti che pongono al centro l'utilizzo dell'intelligenza artificiale: MURAB – *AI for health - MRI and Ultrasound Robotic Assisted Biopsy;* AEROARMS – *AI for Industries AErial RObotics System integrating multiple ARMS and advanced manipulation capabilities for inspection and maintenance;* BRIDGET – *AI for Culture Billions of images and videos are created every day but people lack sophisticated recognition tools to quickly find the information they need.*

[3] A. ADINOLFI, *L'unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., p. 14.

Effettivamente, in una prospettiva *de iure condendo*, le nuove iniziative intraprese evidenziano un deciso cambio rotta, poiché adottano un approccio di più ampio respiro e si muovono nella direzione di approntare il primo insieme di norme destinato a gestire, a tutto campo, le opportunità e i rischi insiti nelle nuove tecnologie[4].

V'è da dire che l'intelligenza artificiale è considerata, a ragion veduta, la tecnologia più importante del ventunesimo secolo. Una di quelle tecnologie c.d. *disruptive*[5] destinate, cioè, a modificare per sempre la fisionomia stessa della società e che permetterà, se correttamente utilizzata, di affrontare in modo più efficiente ed efficace alcune delle sfide decisive dei tempi moderni[6].

Nondimeno, da un punto di vista giuridico, il prepotente e rapidissimo sviluppo di questi sistemi pone delle questioni del tutto nuove che investono, tra le altre, la tutela dei diritti fondamentali e, in particolare, la protezione dei dati personali e il divieto di discriminazione[7].

[4] Il Parlamento ha costituito una Commissione speciale sull'intelligenza artificiale in un'era digitale (AIDA) per analizzare l'impatto dell'IA sull'economia dell'Unione europea. Inoltre, il 20 ottobre 2020 ha presentato tre iniziative legislative, tutte finalizzate a chiarire come l'UE possa regolamentare l'intelligenza artificiale più efficacemente per dare una spinta positiva all'innovazione, agli *standard* etici e alla fiducia nella tecnologia. Le proposte sono rispettivamente orientate a ricercare un equilibrio tra tutela dei cittadini e promozione dello sviluppo tecnologico (25 febbraio 2021 2020/2216(INI)); creare un sistema di responsabilità civile orientato al futuro in grado di proteggere privati e imprese (12 febbraio 2021 (2020/2129(INL)); dare vita ad un sistema efficace di proprietà intellettuale e salvaguardie per gli sviluppatori 25 febbraio 2021 (2020/2129(INL)).

[5] Cfr. J. BOWER, CLAYTON M. CHRISTENSEN, *Disruptive Technologies: Catching the Wave*, 1995, in *Harvard Business Review*, 73, no. 1, January–February 1995, pp. 43–53.

[6] Non a caso l'uso dell'intelligenza artificiale è uno dei punti nevralgici del ricordato *Green Deal* europeo.

[7] Il Parlamento europeo ha adottato la Risoluzione del 14 marzo 2017 sulle implicazioni dei *Big Data* per i diritti fondamentali: protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI)), all'interno della quale, dopo aver preso atto dell'utilizzo massivo dei *Big Data,* anche e, soprattutto, in processi automatizzati, sottolinea che devono essere garantite misure tecniche e operative che ne «assicurino la trasparenza, la non discriminazione del pro-

In un simile scenario, le istituzioni sovranazionali e, in particolare, la Commissione europea, sono chiamate al difficile compito che impone, da un lato, di gestire correttamente la rivoluzione tecnologica in atto e, dall'altro, di ricercare un adeguato bilanciamento, non sempre facile, tra gli ingenti interessi economici collegati all'impiego delle nuove tecnologie di intelligenza artificiale e il sistema di tutele e di valori propri dell'ordinamento sovranazionale.

A preoccupare sono soprattutto i rischi connessi a meccanismi decisionali opachi e la mancanza di trasparenza nell'utilizzo degli algoritmi.

Il dibattito sulle sorti dell'intelligenza artificiale in Europa, e non solo, resta dunque più che mai aperto e molteplici sono le iniziative di *soft law* promosse sul tema a più livelli e all'interno di sistemi giuridici diversi. Come già evidenziato, ad una generalizzata consapevolezza circa le enormi opportunità connesse all'utilizzo di tali sistemi, si accompagna spesso una diffusa percezione dei rischi legati ad uno sviluppo non rispettoso dei diritti fondamentali e delle libertà individuali.

Un ulteriore elemento che si evidenzia, in questi primi sforzi di inquadramento normativo, soprattutto con riferimento ai diritti fondamentali, concerne l'interrogativo se sia o meno necessario, anche alla luce dell'importante ruolo attribuito ai poteri privati nel settore delle nuove tecnologie, procedere alla codificazione di nuovi diritti digitali[8].

cesso decisionale automatizzato e il calcolo delle probabilità del singolo comportamento; che la trasparenza dovrebbe offrire alle persone informazioni significative sulla logica utilizzata, l'importanza e le conseguenze previste; che ciò dovrebbe includere informazioni sui dati utilizzati per formare l'analisi dei *big data* e permettere alle persone di comprendere e monitorare le decisioni che le riguardano».

[8] Si rimanda per approfondimenti nel presente scritto alle considerazioni conclusive. La questione si era posta in termini analoghi nel caso del GDPR nell'ambito della decisione algoritmica automatizzata. Si vedano, in proposito, S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 76 ss. e, più in generale, F. PIZZETTI, (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 37 ss.; G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale la protezione dei dati personali,* in G. Caggiano, G. Contaldi, P. Manzini (a cura

Al fine di fornire un quadro giuridico quanto più possibile completo, di seguito si esamineranno i principali atti di *soft law* adottati dal Consiglio d'Europa e dalle istituzioni europee in materia di intelligenza artificiale.

2. La CEDU e le linee guida del Consiglio d'Europa in tema di intelligenza artificiale

Lo sviluppo incredibilmente rapido dei sistemi di intelligenza artificiale e i possibili profili di interferenza "in negativo" con la protezione dei diritti fondamentali, molti dei quali oggetto di tutela da parte della stessa CEDU, non poteva non sollecitare un intervento da parte del Consiglio d'Europa.

Tra le molte iniziative intraprese, lo studio *Algorithms and Human Righs*[9]*,* redatto nel 2017 dal Comitato di esperti sull'intelligenza artificiale, risulta particolarmente rilevante. All'interno del documento, il Comitato solleva una serie di preoccupazioni per i diritti umani innescate dal crescente ruolo degli algoritmi nel processo decisionale. Affronta, in particolare, i temi della responsabilità e della differenza tra decisione automatizzata e decisione umana, evidenziando che società e governi hanno ormai acquisito una notevole esperienza nella comprensione del processo decisionale umano e dei suoi fallimenti mentre hanno appena iniziato a misurarsi con i limiti e i confini del processo decisionale algoritmico.

A differenza delle posizioni assunte dalle istituzioni europee, che si esamineranno nei paragrafi a seguire, il Comitato pone dubbi circa la possibilità – ma anche l'opportunità – di elaborare un disegno normativo unitario volto a disciplinare l'utilizzo degli algoritmi

di), *Verso una legislazione europea sui mercati e i servizi digitali*, Bari, 2021, p. 216 ss. e P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?,* in *Osservatorio Il Diritto dell'Unione europea*, 2022, disponibile online.

[9] COMMITTEE OF EXPERT OF INTERNET INTERMEDIARIES, ALGORITHMS AND HUMAN RIGHTS*, Study on the Human Rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications,* Council of Europe, 2017, disponibile online.

e delle tecniche di elaborazione automatica, considerato che molte di queste tecnologie si trovano, ad oggi, nelle loro prime fasi di sviluppo ed è necessaria una maggiore comprensione delle loro implicazioni sociali.

Lo studio conclude sottolineando la necessità di uno sforzo comune che coinvolga più *stakeholders* e pone un'enfasi particolare sull'importanza del sostegno alla ricerca transdisciplinare, orientata ai problemi e basata sulle prove e sullo scambio di buone pratiche.

Da ultimo, il Comitato auspica che il Consiglio d'Europa, in quanto principale organizzazione per i diritti umani operante sul continente, acquisisca il ruolo di autorità guida e sede di elezione dove esplorare ulteriormente gli impatti dei sistemi di intelligenza artificiale sull'effettivo esercizio dei diritti umani nella sfera pubblica e privata.

Sempre in seno al Consiglio d'Europa, un altro contributo significativo sul tema è quello offerto dalla Commissione europea per l'efficacia della giustizia (CEPEJ)[10] che ha elaborato la *Carta etica europea sull'impiego dell'intelligenza artificiale nei sistemi giudiziari e in ambiti connessi*[11].

[10] Commissione istituita nel 2002 con l'obiettivo di monitorare e misurare la qualità dei sistemi giudiziari dei Paesi membri. Da alcuni anni la CEPEJ ha iniziato ad occuparsi del fenomeno della diffusione delle nuove tecnologie dell'informazione e della comunicazione nel diritto, redigendo nel biennio 2014-2016 un rapporto dettagliato sull'impiego delle tecnologie dell'informazione nei tribunali in Europa (CEPEJ, Study n. 24. *Thematic report: Use of information technology in European Courts*, 2016, disponibile online e nel 2017 delle linee sulla cybergiustizia, CEPEJ, *Guidelines on how to drive change towards cyberjustice*, 7 dicembre 2016, disponibile online, all'interno delle quali ha esaminato i possibili benefici legati ad un uso virtuoso degli strumenti di IA in ambito giudiziario, i rilievi di F. CERESA GASTALDO, *Lo statuto della giustizia digitale nella Carta etica della CEPEJ*, in *Iusitinere*, 2 aprile 2021, aggiornamento 6 giugno 2022, disponibile online.

[11] CEPEJ, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment adopted by the CEPEJ during its 31st Plenary meeting*, Strasburgo, 3-4 dicembre 2018, disponibile online. Per un commento cfr. C. BARBARO, *CEPEJ, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in *Questione Giustizia*, 7 dicembre 2018, disponibile online e S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra*

Si tratta anche in questo caso di uno strumento di *soft law*[12] che contiene un elenco di principi sostanziali e metodologici da applicare ai sistemi di intelligenza artificiale che vengono impiegati nei contesti giudiziari[13]. Il documento è indirizzato ad una platea di destinatari molto ampia. Quindi non soltanto ai legislatori dei singoli Stati, chiamati al difficile compito di adottare un'adeguata cornice normativa in materia di intelligenza artificiale, ma anche agli operatori del settore impegnati nello sviluppo di sistemi algoritmici[14].

La Carta etica, elaborata in seno alla CEPEJ, non si pone l'obiettivo di proibire o disincentivare l'introduzione dell'intelligenza artificiale nei sistemi giudiziari ma, al contrario, di incoraggiarne le applicazioni che possono apportare un miglioramento in

scienze penali e informatiche, in *Legislazione Penale*, 18 dicembre 2018. Sul tema dei rischi nascenti dall'utilizzo di sistemi di intelligenza artificiale in ambito giudiziario si vedano anche, *ex multis*, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Diritto Penale Contemporaneo*, 2019, p. 12 ss. e anche R.C.A GUIMARÃES, *A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal,* in *Revista Brasileira de Direito Processual Penal*, vol. 5, 2019, pp. 1555-1588; A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento tra scienza, etica e diritto*, in *Analisi Giuridica dell'Economia*, 2019, pp. 47-60; M. DYMITRUK, *Ethical artificial intelligence in judiciary*, in *Jusletter.it*, 2019, disponibile online.

[12] Si tratta di uno strumento di *soft law*, i cui principi «necessitano di un sistema affidabile di *enforcement*» cfr. A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *AI: profili giuridici – Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *Rivista di Biodiritto*, vol. 3, 2019, p. 210 ss.

[13] Rispetto dei diritti fondamentali, non discriminazione, qualità, sicurezza, trasparenza, imparzialità, equità e controllo dell'utente. A questo elenco si accompagnano quattro appendici: ovvero uno studio approfondito relativo all'utilizzo dell'intelligenza artificiale nei sistemi giudiziari, alcune raccomandazioni sull'uso degli strumenti di intelligenza artificiale, un glossario e, come proposto anche dalla stessa Commissione europea, una *checklist* di autovalutazione per verificare il rispetto dei diritti sanciti dalla CEDU.

[14] Cfr. *Directorate of Human Rights, Secretariat of the European Commission for the Efficiency of Justice, The CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. Presentation note*, 4 dicembre 2018, disponibile online.

termini di efficienza e qualità della giustizia e che, al contempo, offrano adeguate garanzie di un impiego responsabile e rispettoso dei diritti fondamentali enunciati dalla CEDU.

In definitiva la CEPEJ, mutuando un concetto già sviluppato con successo dal diritto dell'Unione europea[15], auspica che i sistemi di intelligenza artificiale vengano sviluppati adottando un'ottica *"ethical-by-design"* o *"human-rights-by-design"*[16]*,* e dunque un approccio volto a garantire la tutela dei diritti umani fin dalla progettazione di tali servizi.

Nei due studi allegati alla Carta, inoltre, la CEPEJ identifica i potenziali aspetti problematici con riguardo alle diverse applicazioni di intelligenza artificiale e i rischi per la tutela dei diritti umani. Nel secondo, in particolare, i possibili impieghi dell'intelligenza artificiale nei sistemi giudiziari vengono graduati sulla base di un'analisi del rischio e catalogati all'interno di quattro categorie, in base al loro livello di compatibilità con i cinque principi contenuti nella Carta etica: quelli il cui uso è da incoraggiare, quelli da considerare ma con l'adozione di adeguate precauzioni metodologiche, quelli in relazione ai quali sarebbero necessari ulteriori approfon-

[15] Ci si riferisce al principio di *privacy by design* e *privacy by default* elaborato in seno al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 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) (più comunemente conosciuto con l'acronimo GDPR).

[16] Cfr. CEPEJ, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment,* cit.*,* p.8. Il Comitato (cd. T-PD) della Convenzione 108, ha avuto modo di chiarire che «[i]n tutte le fasi del trattamento, compresa la raccolta dei dati, gli sviluppatori, i produttori e i fornitori di servizi di IA dovrebbero adottare un approccio volto a tutelare i diritti umani fin dalla progettazione di tali servizi *("human rights by design*") ed evitare qualsiasi potenziale pregiudizio (*bias*), anche involontario o occulto, il rischio di discriminazione o altri effetti negativi sui diritti umani e le libertà fondamentali degli interessati. Gli sviluppatori di IA dovrebbero vagliare accuratamente la qualità, la natura, l'origine e la quantità di dati personali utilizzati, riducendo i dati inutili, ridondanti o marginali durante lo sviluppo e le fasi di addestramento e poi monitorando l'accuratezza del modello man mano che viene alimentato con nuovi dati».

dimenti scientifici e, infine, quelli su cui invece la CEPEJ esprime le più "estreme riserve".

Sempre in seno al Consiglio d'Europa, un ulteriore contributo allo studio e all'approfondimento dei possibili profili di interferenza tra i sistemi di intelligenza artificiale e la tutela dei diritti umani arriva anche dal CAHAI (*Ad Hoc Committee on Artificiale Intelligence*)[17]. Il Comitato, che non a caso riassume così il proprio scopo «towards an application of AI based on human rights, the rule of law and democracy», evidenzia come risulti strettamente necessario fissare dei requisiti minimi *standard* che i sistemi di intelligenza artificiale devono rispettare in modo da poter garantire la trasparenza, la qualità dei dati elaborati, la salvaguardia dell'autonomia decisionale umana oltre ad idonei e sufficienti strumenti di reclamo avverso decisioni considerate scorrette o inique.

In particolare, secondo il Comitato, andrebbe incoraggiato lo sviluppo e l'impiego di tutti quei sistemi virtuosi che promuovono, rafforzano e accrescono la protezione dei diritti umani, la tutela della democrazia e dello stato di diritto.

3. La posizione del Parlamento europeo. La Carta sulla Robotica e la Risoluzione sulle implicazioni dei *Big Data* per i diritti fondamentali

Per ciò che riguarda specificamente il sistema europeo, il senso di urgenza nel gestire i sistemi di intelligenza artificiale con modalità che risultino pienamente rispettose dei diritti fondamentali, si avverte innanzitutto nelle posizioni espresse dal Parlamento, che è stata una delle prime istituzioni a presentare delle raccomandazioni in materia, ritenendo l'intelligenza artificiale determinante per il futuro digitale dell'Unione europea ma, allo stesso tempo, considerando assolutamente cruciale che il suo sviluppo avvenga in modo sicuro e nel rispetto dei diritti fondamentali[18].

[17] I lavori del Comitato sono disponibili online.

[18] Nell'intervista, disponibile online, rilasciata da Axel Voss (EPP, Germania), l'eurodeputato, incaricato della relazione sull'intelligenza artificiale, ha sotto-

Riconoscendo che l'intelligenza artificiale può fare una grande differenza, in positivo o in negativo, il Parlamento europeo ha istituito una commissione dedicata – *Artificial Intelligence in a Digital Age* (AIDA)[19]. L'AIDA è stata incaricata di esaminare l'impatto delle nuove tecnologie sugli aspetti ritenuti più rilevanti: ovvero la ricerca di un equilibrio tra diritti degli individui e la promozione dello sviluppo tecnologico, un sistema di responsabilità civile orientato al futuro per proteggere privati e imprese unitamente ad un sistema efficace di proprietà intellettuale che garantisca adeguata tutela agli sviluppatori[20].

Da un punto di vista strettamente giuridico, il Parlamento auspica che l'Unione europea arrivi a dotarsi di un sistema normativo unitario volto a ridisegnare compiutamente l'insieme delle norme destinate a regolare il settore dell'intelligenza artificiale[21]. Un siste-

lineato che l'UE potrebbe fissare degli *standard* globali sull'intelligenza artificiale, ma per trarne beneficio la normativa dovrà arrivare in fretta ed essere flessibile.

[19] Decisione del Parlamento europeo del 18 giugno 2020 sulla costituzione, le attribuzioni, la composizione numerica e la durata del mandato della commissione speciale sull'intelligenza artificiale in un'era digitale (2020/2684(RSO).

[20] Si veda in materia il contributo di G. MORGESE, *La tutela del software in Europa tra normativa internazionale e comunitaria*, in *Sud in Europa*, 2009, disponibile online.

[21] Cfr. in particolare la Risoluzione del 15 gennaio 2019 sulla guida autonoma nei trasporti europei, dove si evidenzia, al par. 20, che le norme in vigore in tema di responsabilità come ad esempio la direttiva 85/374/CEE sulla responsabilità per danno da prodotti difettosi e la direttiva 2009/103/CE sull'assicurazione degli autoveicoli "non sono state concepite per far fronte alle sfide poste dall'utilizzo di veicoli autonomi" ed evidenzia che "l'attuale quadro normativo, in particolare in tema di responsabilità, assicurazione, registrazione e protezione dei dati personali, non sarà più sufficiente o adeguato a fronte dei nuovi rischi derivanti dall'aumento dell'automazione, della connettività e della complessità dei veicoli". In dottrina, A. ADINOLFI, *L'unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., p. 21 in nota 24; G.M. RUOTOLO, *La disciplina europea della responsabilità dei fornitori dei servizi online tra regime pregresso, proposte di riforma e un rischio di* bis in idem, in G. Caggiano, G. Contaldi, P. Manzini, *Verso una legislazione europea sui mercati e i servizi digitali*, cit., p. 59 e ss.

ma di norme incentrato sulla persona, in modo da offrire garanzia di sicurezza, trasparenza e presa di responsabilità e che sia in grado di assicurare il rispetto dei diritti fondamentali, scongiurare la creazione di pregiudizi e discriminazioni e stimolare la responsabilità sociale e ambientale.

Secondo il Parlamento europeo, un sottoutilizzo dell'intelligenza artificiale potrebbe generare una inefficiente attuazione di programmi importanti, come il ricordato *Green Deal* europeo, e causare una perdita di vantaggio competitivo, stagnazione economica e meno opportunità di crescita. Di contro, un utilizzo non correttamente regolamentato rappresenterebbe una seria minaccia, particolarmente per la tutela dei diritti fondamentali.

Nella consapevolezza dei potenziali rischi che si corrono nel "maneggiare" in modo scorretto questi sistemi, il Parlamento europeo è intervenuto mettendo in campo diverse iniziative[22]. Tra queste, le più significative sono certamente la Carta sulla robotica[23] e la Risoluzione sull'impatto dei *Big Data*[24].

Con il primo intervento, il Parlamento ha indirizzato alla Commissione delle raccomandazioni concernenti le norme di diritto ci-

[22] Ad esempio si vedano le proposte linee guida per l'uso dell'intelligenza artificiale in campo militare e civile *2020/2013(INI) Artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice,* la *Relazione sull'uso dell'IA nell'istruzione, nella cultura e nel settore audiovisivo* del 19 maggio 2021.

[23] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

[24] Risoluzione del Parlamento europeo C 263/82, *Implicazioni dei Big Data in termini di diritti fondamentali Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto* (2016/2225(INI)). Pur non essendoci una definizione specifica, con l'espressione *Big Data* si fa generalmente riferimento «alla raccolta, all'analisi e all'accumulo di ingenti quantità di dati, tra i quali possono essere ricompresi dati di natura personale […] in ipotesi anche provenienti da fonti diverse» AGCM – AGCOM – GARANTE PER LA PRIVACY, *Indagine conoscitiva sui Big Data, 10 febbraio 2020 (disponibile all'interno dei siti delle tre Autorità*), p. 7.

vile che dovrebbero regolare il settore della robotica[25]. All'interno del documento il Parlamento fornisce un ventaglio di possibili proposte in materia di responsabilità per danno causato da un *robot* come l'applicazione degli istituti della responsabilità oggettiva, la gestione dei rischi, l'istituzione di un regime di assicurazione obbligatorio nonché l'istituzione di uno *status* giuridico *ad hoc* consistente in una personalità elettronica, che permetta di ritenere i *robot* più sofisticati responsabili delle proprie azioni dannose[26]. L'autonomia dei *robot* solleva infatti, tra le altre, una problematica connessa alle possibilità di inquadramento in categorie giuridiche esistenti. Ci si interroga, in particolare, se gli stessi debbano essere considerati alla stregua di soggetti o oggetti del diritto e se, in quanto dotati di un'evoluta intelligenza artificiale, dovrebbero assumere dei livelli di responsabilità più elevati[27].

La seconda iniziativa, di più ampio respiro, valuta le implicazioni dei *Big Data*[28] sui diritti fondamentali[29]. In particolare,

[25] A dimostrazione di quanto suggestivo risulti ancora il tema, la risoluzione apre con citazioni letterarie che passano da Frankenstein a Pigmalione, dal Golem di Praga fino a Karel Čapek, lo scrittore ceco a cui si deve l'introduzione della parola *robot*.

[26] V. A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F. P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *AI: profili giuridici Intelligenza artificiale: criticità emergenti e sfide per il giurista*, cit., p. 210 ss.

[27] B. ANDREA, *Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies*, in *Europa e diritto privato*, 2022, n. 2, p. 369. L'. A. osserva come la dicotomia tra soggetti giuridici e oggetti non sia superabile, *tertium non datur*, e l'unica classificazione ammissibile, di tutte le tecnologie avanzate esistenti e ragionevolmente prevedibili, è quella di cose, oggetti e artefatti, prodotti dell'intelletto umano e che così concepite rientrano chiaramente nella nozione di prodotto.

[28] Sulla complessità del concetto di *Big data*, v. M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo,* Bologna, 2019, p. 26; D. LANEY, *3D data management: controlling data volume, velocity, and variety*, in *Technical report*, META Group, 2001, disponibile online; M.C. CARROZZA ET AL., *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, in *BioLaw Journal*, 3, 2019, p. 241, che parlano di variabilità, secondo cui il contenuto dei dati muta di significato a seconda dell'analisi a cui è sottoposto.

[29] A dimostrazione di quanto il tema sia sentito si veda l'opera-denuncia di C.

all'interno della Risoluzione trasmessa a Consiglio e Commissione, richiamando gli articoli 1, 7, 8, 11, 14, 21, 47 e 52 della Carta di Nizza e il GDPR, il Parlamento europeo, nella parte dei considerando, evidenzia che la proliferazione dei trattamenti e dell'analisi dei dati, l'elevato numero di soggetti coinvolti nella raccolta, nella conservazione, nel trattamento e nella condivisione e la combinazione di grandi insiemi di informazioni contenenti dati personali e non personali provenienti da una serie di fonti diverse, pur generando opportunità significative, hanno creato una grande incertezza sia per i cittadini sia per il settore pubblico e privato relativamente ai requisiti specifici per la conformità alla vigente legislazione dell'UE in materia.

Il Parlamento chiarisce, inoltre, che per trarre pieno beneficio dalle prospettive e dalle opportunità offerte dai *Big Data*, è necessario che la fiducia pubblica in tali tecnologie sia garantita da un rigoroso rispetto dei diritti fondamentali, dalla conformità alla vigente legislazione in materia di protezione dei dati nonché dalla certezza giuridica per tutti i soggetti coinvolti.

4. Le linee guida, il libro bianco e la dichiarazione europea sui diritti e principi digitali per il decennio digitale della Commissione europea

Anche la Commissione europea, sollecitata ad occuparsi del tema, è intervenuta lanciando nel 2018 la *Strategia sull'Intelligenza artificiale*[30] e

O'NEIL, *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia,* Milano, 2017, p. 49 ss., e specialmente p. 261 ss. Sul punto anche M. PALMIRANI, *Big Data e conoscenza*, in *Riv. fil. dir.*, n. 1/2020, p. 73 ss. e spec. p 87. L'A. sottolinea la necessità di «introdurre accanto al diritto alla spiegabilità dell'algoritmo e della decisione automatica finale (ossia dell'esito) anche il principio della conoscibilità dei dati non tanto e non solo quelli che sono stati contribuiti o osservati dall'utente, ma anche quelli che hanno contribuito al processo quindi quelli inseriti, derivati, collettivi, statistici, anche se anonimi».

[30] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni –

nominando un gruppo di esperti per facilitarne l'implementazione (AI HLEG)[31].

All'interno del documento, che delinea un piano di misure politiche e di investimenti per promuovere l'economia agile dei dati per i prossimi cinque anni, si introduce l'idea di un'intelligenza artificiale[32] *made in Europe* etica, sicura e all'avanguardia, che poggia essenzialmente su tre pilastri: incoraggiare l'utilizzo dell'intelligenza artificiale nei settori pubblico e privato; prepararsi ai cambiamenti socioeconomici provocati dall'intelligenza artificiale; assicurare un quadro giuridico ed etico compiuto e coerente.

In un'ottica inclusiva e propositiva, tutti – cittadini, esperti e *stakeholders* – sono stati chiamati a dare un contributo diretto alla politica europea sull'intelligenza artificiale, attraverso consultazioni mirate e discussioni online nell'ambito dell'*Alleanza europea sull'IA*[33]. Il Centro comune di ricerca della Commissione lavora per garantire un monitoraggio costante sia delle capacità industriali, tecnologiche e di ricerca sia delle tecnologie di intelligenza artificiale adottate in tutta Europa. I risultati sono raccolti e regolarmente

L'intelligenza artificiale per l'Europa, 25 aprile 2018, COM(2018) 237 *final*.

[31] Il gruppo *High-Level Expert Group on Artificial Intelligence* (AI HLEG), istituito nel 2008, è composto da 52 esperti indipendenti scelti tra soggetti provenienti dal mondo accademico, dalla società civile e dall'industria, con il compito di sostenere lo sviluppo dell'agenda europea sull'intelligenza artificiale e con quello, ancora più specifico, di elaborare due documenti: gli orientamenti etici per l'intelligenza artificiale e le raccomandazioni sugli investimenti e la politica.

[32] In base alla definizione fornita dal AI HLEG, «l'Intelligenza artificiale (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (ad esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)». La definizione elaborata all'interno del documento "Una definizione di IA: principali capacità e discipline scientifiche" è disponibile online. Si veda, in particolare, sul tema dell'utilizzo dei droni e sulle problematiche connesse F. BORGIA, *L'uso militare dei droni, Profili di diritto internazionale*, Napoli, 2018, p. 38 ss.

[33] *Alleanza europea sull'IA,* disponibile online.

aggiornati all'interno di un portale dedicato denominato *AI Watch*[34].

In tutti i documenti adottati dalla Commissione, emerge in modo inequivocabile l'urgenza di colmare l'importante *gap* tecnologico che divide l'Europa da Cina e Stati Uniti in questo settore, al fine di non perdere ulteriore terreno e mantenere alta la competitività[35].

La Commissione, che si propone come coordinatrice degli sforzi europei e nazionali in materia, ha varato, insieme agli Stati membri e a Norvegia e Svizzera[36], il *Piano Coordinato sull'intelligenza artificiale*[37].

In una visione molto ambiziosa, si mira a gettare le basi per

[34] *AI Watch,* disponibile online.

[35] Sempre all'interno della Comunicazione, *L'Intelligenza artificiale per l'Europa*, cit., la Commissione auspica che venga adottato «un approccio coordinato per sfruttare al massimo le opportunità offerte dalla IA». In tale documento la Commissione evidenzia altresì come l'Europa si collochi molto dietro a Stati Uniti e Cina quanto ad investimenti nel settore – nel 2016 circa 2 miliardi dell'Unione contro i 12 miliardi in USA e i 7 miliardi in Cina e nell'area asiatica. N. BOLDRINI, *Intelligenza Artificiale: Europa "terza incomoda" tra Cina e USA?*, in *AI4Business*, 26 febbraio 2019, disponibile online; P. POCCIANTI, *Le potenze investono sull'intelligenza artificiale: il ruolo dell'Europa tra Usa e Cina*, Agenda Digitale, 22 febbraio 2019, disponibile online.

[36] In Italia, nel luglio del 2020, il MISE ha pubblicato il documento definitivo contenente le proposte per la *Strategia italiana per l'Intelligenza Artificiale.* Altri cinque Stati membri (Francia, Finlandia, Svezia, Regno Unito e Germania) hanno già adottato strategie mirate per l'intelligenza artificiale. Danimarca, Lussemburgo, Paesi Bassi, Irlanda e Norvegia hanno incluso le azioni relative all'intelligenza artificiale nelle loro più ampie strategie di digitalizzazione. Austria, Belgio, Danimarca, Estonia, Italia, Lettonia, Polonia, Portogallo, Repubblica ceca, Slovacchia, Slovenia e Spagna stanno elaborando le loro strategie.

[37] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni, *Piano coordinato sull'intelligenza artificiale*, 7 dicembre 2018, COM(2018) 795 *final*. La proposta di un piano coordinato basato sulla dichiarazione di cooperazione sull'IA, avviata nell'aprile 2018 in occasione della Giornata digitale, è stata firmata da tutti gli Stati membri e dalla Norvegia e approvata dal Consiglio europeo nel giugno 2018. L'obiettivo è promuovere la cooperazione transfrontaliera e mobilitare tutti gli attori per aumentare gli investimenti pubblici e privati ad almeno 20 miliardi di euro l'anno nei prossimi dieci anni.

un'Unione Europea che sia in grado di imporsi sulla scena mondiale come *leader* industriale, ma anche normativo, nel settore dell'intelligenza artificiale[38]. Un obiettivo che tuttavia si accompagna ad un altro, ugualmente fondamentale, imperativo, ovvero garantire un utilizzo delle tecnologie di intelligenza artificiale etico e sicuro[39]. Si intende promuovere un approccio che ponga sempre al centro l'uomo, si parla a questo proposito di *IA antropocentrica*. Un concetto questo che non verrà più abbandonato nei successivi atti adottati[40].

Nel piano si legge che l'Unione mira allo sviluppo di un'intelligenza artificiale affidabile, ispirandosi ai valori etici e sociali inclusi nella Carta dei diritti fondamentali. L'idea è quella di dare vita in Europa ad un ecosistema favorevole all'innovazione per l'intelligenza artificiale: un ambiente dove gli operatori economici possano trovare infrastrutture, norme, strutture di ricerca nonché adeguati livelli di competenza, al fine di poter attrarre preziosi investimenti. Tuttavia, per poter dare vita ad un simile scenario, non si può prescindere da un quadro giuridico chiaro, che affronti in ma-

[38] Si tratta del c.d. "Effetto Bruxelles", l'espressione è notoriamente di A. BRADFORD, *Effetto Bruxelles. Come l'Unione europea regola il mondo*, Milano, 2021, p. 220.

[39] Che sia un tema particolarmente sentito lo dimostra il fatto che il 28 febbraio 2020 a Roma, la Pontificia Accademia per la Vita, Microsoft, IBM, FAO e il Ministero Italiano per l'Innovazione hanno firmato l'appello *Call for AI Ethics*. Con questo documento, indicando una nuova algoretica, i firmatari si sono impegnati a richiedere lo sviluppo di un'IA che serva ogni persona e l'umanità nel suo complesso; che rispetti la dignità della persona umana, in modo che ogni individuo possa beneficiare dei progressi della tecnologia; che non abbia come unico obiettivo un maggiore profitto o la graduale sostituzione delle persone sul posto di lavoro. Include 3 aree di impatto (etica, educazione e diritti) e 6 principi (trasparenza, inclusione, responsabilità, imparzialità, affidabilità, sicurezza e privacy). Il documento è disponibile sul portale dedicato.

[40] V. A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione, in Sezione "Atti convegni AISDUE"*, n. 15, 14 marzo 2023, *Quaderni AISDUE*, p. 322. Secondo L'A. i diritti fondamentali costituiscono il limite alle possibili applicazioni tecnologiche.

niera appropriata le nuove sfide tecnologiche e che garantisca la certezza del diritto.

Su questi presupposti, e dopo aver avviato una consultazione pubblica attraverso la quale sono state raccolte oltre cinquecento opinioni, il AI HLEG ha pubblicato gli *Orientamenti etici per un'IA affidabile*[41], su cui ci si soffermerà tra breve, che la Commissione, con la comunicazione *Creare fiducia nell'intelligenza artificiale antropocentrica*[42] ha sostenuto, utilizzandoli come linee guida per i futuri atti adottati.

Nel documento si promuove l'idea di un'intelligenza artificiale affidabile basata su tre componenti essenziali ovvero legalità, eticità e robustezza. L'utilizzo dell'intelligenza artificiale deve avvenire in ottemperanza a tutte le leggi e ai regolamenti applicabili, deve essere assicurata l'adesione a principi e valori etici, ma anche il rispetto dei diritti fondamentali e l'affidabilità dei sistemi in modo da scongiurare, nella massima estensione possibile, che si possano causare danni, anche non intenzionali.

Tutti gli obiettivi devono necessariamente coesistere in quanto interdipendenti. Ciascuna componente, isolatamente considerata, seppur necessaria, non risulta sufficiente per dare vita ad un'intelligenza artificiale affidabile. Idealmente poi, le tre parti operano armonicamente e si sovrappongono e, nel caso di tensioni tra le stesse, le norme dovrebbero essere congeniate in modo da poter agilmente risolvere eventuali conflitti. Viene riproposta l'idea di sistemi di intelligenza artificiale antropocentrici, che siano messi al servizio dell'umanità e del bene comune, con l'obiettivo ultimo di migliorare il benessere complessivo della società.

Si pone l'accento sul fatto che questo preciso momento storico rappresenti un'importante occasione per plasmare quella che sarà la percezione futura da parte degli individui dell'intelligenza artifi-

[41] Gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG), *Orientamenti etici per un'IA affidabile*, 8 aprile 2019, disponibile online.

[42] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*, Creare fiducia nell'intelligenza artificiale antropocentrica*, Bruxelles, 8.4.2019 COM(2019) 168*final* testo disponibile online.

ciale e dare vita ad un sistema equo che garantisca ai produttori un vantaggio competitivo e ai cittadini un impiego delle tecnologie di intelligenza artificiale etico e affidabile che rispetti i valori fondanti dell'Unione europea (diritti fondamentali individuali ma anche democrazia e Stato di diritto).

L'imperativo è, dunque, massimizzare i benefici minimizzando i rischi[43]. Nei documenti delle istituzioni, l'etica diventa il pilastro fondamentale e, allo stesso tempo, la netta linea di demarcazione che consente di dar vita e calibrare un'intelligenza artificiale affidabile. Si sottolinea, tuttavia, che l'etica non è sufficiente[44], è necessario un approccio sistemico, che coinvolga tutti i soggetti e i processi durante l'intero ciclo di vita della tecnologia[45].

Rispetto alle tre componenti necessarie (ovvero legalità-eticità-robustezza), gli orientamenti si soffermano sulle ultime due, rimandando ad altra sede e ad azioni future le valutazioni sul rispetto della legalità da parte dei sistemi di intelligenza artificiale. Sul punto, il Comitato (AI HLEG) si limita ad osservare che, pur essendo la regolamentazione un presupposto necessario, non è anche sufficiente ad ottenere un'intelligenza artificiale affidabile, poiché spesso il diritto non riesce a stare al passo con gli sviluppi tecnologici o con le

[43] *Orientamenti etici per un'IA affidabile*, cit., par. 10.

[44] Di etica in questo settore parla B. WAGNER, *Ethics As An Escape From Regulation. From "Ethics-Washing" To Ethics-Shopping?*, in *Being Profiled: Cogitas Ergo Sum*, Amsterdam, 2018, parte IV, disponibile online. L'A. sottolinea in modo condivisibile che: «A strange confusion among technology policy makers can be witnessed at present. While almost all are able to agree on the common chorus of voices chanting 'something must be done,' it is very difficult to identify what exactly must be done and how. In this confused environment it is perhaps unsurprising that the idea of 'ethics' is presented as a concrete policy option. Striving for ethics and ethical decision-making, it is argued, will make technologies better. While this may be true in many cases, much of the debate about ethics seems to provide an easy alternative to government regulation. Unable or unwilling to properly provide regulatory solutions, ethics is seen as the 'easy' or 'soft' option which can help structure and give meaning to existing self-regulatory initiatives. In this world, 'ethics' is the new 'industry self-regulation».

[45] *Orientamenti etici per un'IA affidabile*, cit., par. 13, 14.

norme etiche oppure, semplicemente, non è adatto ad affrontare determinate questioni[46].

Il Rapporto evidenzia che non tutte le situazioni presentano gli stessi livelli di rischio e, di conseguenza, le medesime esigenze di tutela. I sistemi di intelligenza artificiale che offrono consigli musicali, necessariamente, non suscitano le stesse preoccupazioni etiche dei sistemi di intelligenza artificiale che propongono terapie mediche salvavita. Allo stesso modo, sono differenti le opportunità e i rischi associati a sistemi di intelligenza artificiale utilizzati nel contesto di relazioni diverse (es. impresa e consumatore, impresa e impresa, datore di lavoro e lavoratore, settore pubblico e cittadini) perché diverse sono le posizioni di partenza, in termini di dinamiche di forza e di potere contrattuale. A motivo di ciò, si prospetta l'opportunità che gli Orientamenti, pensati per essere un documento generale, vengano integrati, all'occorrenza, con approfondimenti settoriali.

Oltre a fornire un elenco di principi etici, gli Orientamenti includono indicazioni su come tali principi possano essere resi effettivamente operativi con gradualità crescente. Si introducono i concetti di competitività e innovazione "responsabili" e di "globalità" negli approcci e nelle soluzioni proposte[47].

Si parte quindi da un metodo basato sui diritti fondamentali, ma è evidente che la riflessione dovrebbe spingersi oltre e aiutare a comprendere, in maniera più dettagliata, ciò che si deve fare e non solo ciò che (attualmente) è possibile fare con la tecnologia.

Il documento si divide in tre capitoli. Nel primo sono elencati i principi etici che devono osservati al fine di garantire l'eticità e la robustezza dei sistemi di intelligenza artificiale. Nel secondo vengono elencati i sette requisiti che i sistemi dovrebbero soddisfare durante il loro intero ciclo di vita. All'interno del terzo ed ultimo capitolo viene fornita una vera e propria lista di controllo, seppur non esaustiva, per la valutazione dell'affidabilità dei sistemi di intelligenza artificiale.

[46] Si rimanda per alcune riflessioni su questo punto alle conclusioni del presente lavoro.

[47] *Orientamenti etici per un'IA affidabile*, cit., par. 17, 18.

Sono quattro i principi elencati, definiti come imperativi etici, a cui si deve aderire per garantire che siano sviluppati, distribuiti e utilizzati in modo affidabile, ovvero: rispetto dell'autonomia privata; prevenzione dei danni; equità ed esplicabilità[48].

Secondo il primo dei principi, ovvero il rispetto dell'autonomia privata, i sistemi di intelligenza artificiale non devono subordinare, costringere, ingannare, manipolare, condizionare o aggregare in modo ingiustificato gli esseri umani[49]. Al contrario, devono essere progettati per aumentare, integrare e potenziare le abilità cognitive, sociali e culturali. La distribuzione delle funzioni tra esseri umani e sistemi di intelligenza artificiale dovrebbe seguire i principi di progettazione antropocentrica e lasciare ampie opportunità di scelta all'essere umano. Per fare questo deve essere sempre garantita la sorveglianza e il controllo dei processi operativi nei sistemi di intelligenza artificiale.

[48] L'esplicabilità, come si avrà modo di approfondire, è un requisito fondamentale quando si parla di intelligenza artificiale. Si vedano in dottrina le riflessioni di E. CALZOLAIO, *Intelligenza artificiale ed autonomia della decisione: problemi e sfide*, cit., p. 3 ss.; L. FLORIDI, F. CABITZA, *Intelligenza Artificiale – L'uso Delle Nuove Macchine*, Milano, 2021, p. 22 ss.; F. PELAGALLI, *IA, cinque principi per un modello di sviluppo etico*, in *Il Sole 24 Ore*, 15 luglio 2018, disponibile online; A. LONGO, G. SCORZA, *Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà*, Milano, 2020, p. 26 ss.; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 2019, p. 63 ss. È stato osservato che non sempre è possibile spiegare perché un modello ha generato un particolare risultato o una determinata decisione. Ciò in quanto, per la gran parte, gli algoritmi, sono da considerarsi sistemi imperscrutabili, una sorta di "*black box*". La definizione è di F. PASQUALE, *The Black Box society. The Secret Algorithms Money and Information*, Cambridge, 2016, p. 141. È stato evidenziato che: «Gli algoritmi ci hanno liberati dai viaggi di gruppo, dai punti di vista obbligati e dalle soste obbligatorie davanti ai panorami da *souvenir*. Essi nascono da un desiderio di autonomia e libertà. Tuttavia contribuiscono anche ad assoggettare l'internauta a quella strada calcolata, efficace, automatica, che si adatta ai nostri desideri regolandosi, in segreto, sul traffico altrui» ma, aggiunge anche, «insieme alla carta, ci siamo persi il paesaggio», D. CARDON, *Che cosa sognano gli algoritmi, Le nostre vite al tempo dei Big Data*, Milano, 2016, p. 90.

[49] *Orientamenti etici per un'IA affidabile*, cit., par. 50. In pratica, una fedele riproduzione delle ricordate tre leggi della robotica di Asimov; I. ASIMOV, *Robot Visions*, cit., p. 10 ss. si veda *supra* nota 19.

Per ciò che riguarda il secondo dei principi, ovvero la prevenzione, viene chiarito che queste tecnologie non devono causare danni né aggravarli e neppure influenzare negativamente gli esseri umani, dei quali devono sempre essere tutelate la dignità e l'integrità fisico-psichica. I sistemi di intelligenza artificiale e gli ambienti in cui operano devono essere sicuri e protetti, tecnicamente robusti e deve essere garantito che non siano esposti ad usi malevoli. Un'attenzione particolare deve inoltre essere dedicata ai soggetti vulnerabili.

Da ultimo, vengono illustrati i contenuti dei principi di equità e di esplicabilità[50]. In particolare, di equità si parla sotto due punti di vista, sostanziale e procedurale[51]. La dimensione sostanziale implica un impegno a garantire una distribuzione giusta ed equa di costi e benefici, a garantire agli individui la libertà di scelta e tenerli indenni da distorsioni inique, discriminazioni e stigmatizzazioni, promuovendo le pari opportunità in termini di accesso all'istruzione, ai beni, ai servizi e alla tecnologia. Inoltre, l'equità sostanziale implica che gli operatori del settore dell'intelligenza artificiale rispettino il principio di proporzionalità tra mezzi e fini e valutino attentamente come bilanciare interessi e obiettivi concorrenti. La dimensione procedurale dell'equità attiene invece alla garanzia del diritto ad un ricorso effettivo, che implica che l'organismo responsabile della decisione sia agevolmente identificabile.

Per ciò che concerne il concetto di esplicabilità[52], si richiede che i processi siano trasparenti, che le capacità e lo scopo dei sistemi di intelligenza artificiale utilizzati siano comunicati apertamente e che le decisioni, per quanto possibile, siano spiegabili a coloro che ne sono direttamente o indirettamente coinvolti.

Per la risoluzione di eventuali conflitti tra tali principi, in assenza di soluzioni predefinite, il AI HLEG auspica che vengano definiti metodi di discussione responsabile, coerenti con l'impegno fondamentale dell'Unione europea a favore della partecipazione de-

[50] *Orientamenti etici per un'IA affidabile*, cit., par. 51.
[51] *Ibidem*, par. 52.
[52] *Ibidem*, par. 53.

mocratica, del processo equo e di una comunicazione politica aperta.

All'interno del secondo capitolo, i principi descritti vengono tradotti in requisiti concreti che i sistemi di intelligenza artificiale devono soddisfare. Nella specie, ne vengono individuati sette, da verificare e monitorare costantemente durante l'intero ciclo di vita della tecnologia:

- *Intervento e sorveglianza umani*. All'interno dei sistemi di intelligenza artificiale devono essere previsti meccanismi di *governance* che garantiscano l'adozione di un approccio con intervento umano – *"human-in-the-loop*", con supervisione umana – *"human-on-the-loop"* – o con controllo umano – *"human-in-command"* [53].

- *Robustezza tecnica e sicurezza*. Affinché possa parlarsi di un'intelligenza artificiale affidabile è necessario che vengano sviluppati algoritmi sicuri, affidabili e sufficientemente robusti in grado di far fronte a errori o incongruenze e capaci di gestire eventuali risultati sbagliati.

- *Riservatezza e governance dei dati*. Durante l'intero ciclo di vita del sistema di intelligenza artificiale, devono essere garantite la tutela della riservatezza e la protezione dei dati. Poiché la profilazione del comportamento umano può consentire ai sistemi di dedurre anche dati particolari, occorre garantire che le persone ripongano fiducia nella tecnologia e che gli venga sempre assicurato il pieno controllo sui propri dati.

- *Trasparenza*. I *set* di dati e i processi che determinano la decisione del sistema di intelligenza artificiale devono essere al contempo tracciabili, spiegabili e comunicabili. Deve essere rispettato il diritto degli utenti ad essere informati del fatto che si trovino ad interagire con un sistema di intelligenza artificiale e deve essere assicurata la possibilità di preferire l'interazione umana.

[53] Analoga questione si era posta nell'ambito del GDPR che conferisce ai singoli il diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato quando questa produca effetti giuridici che li riguardano o incida in modo analogo significativamente sulla loro persona (articolo 22). V. *infra* cap. IV.

- *Diversità, non discriminazione ed equità*. Le parole d'ordine, per ottenere un'intelligenza artificiale affidabile, sono inclusione e diversità. Durante l'intero ciclo di vita del sistema tutti i portatori di interessi influenzati dall'intelligenza artificiale devono essere presi in considerazione e coinvolti nel processo.

- *Benessere sociale e ambientale*. In linea con i principi di equità e di prevenzione dei danni, si dovrebbe anche tenere conto dell'impatto che queste tecnologie hanno sull'ambiente e sugli altri esseri senzienti, in particolare gli animali.

- *Accountability*. Questo requisito impone che vengano previsti meccanismi in grado di garantire la verificabilità degli algoritmi, la riduzione al minimo degli effetti negativi e la possibilità di segnalarli nel caso si verifichino. Si prevede che l'implementazione pratica di tali principi avvenga mediante il ricorso a metodi tecnici e non tecnici[54].

Una delle novità più interessanti del documento è il tentativo di contribuire a facilitare il compito per gli operatori del settore di verificare la conformità dei propri sistemi con i ricordati requisiti attraverso la pubblicazione di un elenco di valutazione dettagliato, una sorta di *assessment*, che è stato poi trasformato in uno strumento interattivo *web-based*[55]. Nel terzo e ultimo capitolo, infatti, viene fornita, unitamente ad una raccomandazione generale sulle modalità di attuazione, una lista di controllo per la valutazione dell'affidabilità dell'intelligenza artificiale, rilasciata in versione "beta"[56], e destinata a sviluppatori e distributori di tali sistemi[57].

[54] Sulla scia già tracciata con successo in ambito *privacy*, viene richiamato anche in questo caso il concetto di *"by design"* a significare che il rispetto dei diritti e dei principi etici deve essere garantito sin dalla progettazione del sistema. Tra i metodi tecnici vengono inoltre annoverati: l'esplicabilità di un dato comportamento, l'esigenza di poter sempre spiegare il motivo per cui un sistema si è comportato in un determinato modo, le esigenze di prova e convalida e, infine, gli indicatori di qualità del servizio. Tra i metodi non tecnici vengono inclusi, oltre a regolamentazioni, codici di condotta, certificazioni e *governance* anche l'istruzione e la formazione, l'inclusione, il dialogo sociale e il necessario coinvolgimento dei portatori di interessi durante l'intero ciclo di vita del sistema di intelligenza artificiale.

[55] Oltre 350 imprese hanno risposto all'invito e hanno fornito un loro *feedback* sul documento.

[56] *Orientamenti etici per un'IA affidabile*, cit., p. 30.

[57] Il Comitato (AI HLEG) raccomanda di rendere obbligatoria la valutazione di

Gli orientamenti esaminati sono stati accolti con favore dagli Stati membri e dalla Commissione che, come già ricordato, in risposta, ha indirizzato alle altre istituzioni coinvolte nella discussione sul tema, una comunicazione[58] all'interno della quale ha confermato di appoggiare i requisiti fondamentali per un'intelligenza artificiale affidabile elaborati dal AI HLEG e ha incoraggiato i portatori di interessi ad applicarli, testare la lista di controllo e proporre eventuali integrazioni[59].

Nel mese di febbraio 2020, la Commissione è intervenuta con un pacchetto di atti che riassumono la visione programmatica dell'Europa sull'intelligenza artificiale per il prossimo futuro che si compone di un documento principale, ovvero il *Libro bianco sul-l'intelligenza artificiale*[60], una relazione esplicativa[61] e due comunicazioni[62].

"affidabilità dell'Intelligenza Artificiale" per tutti i sistemi impiegati nel settore privato che hanno il potenziale per avere un impatto significativo sulla vita umana. l'integrazione della lista sulla base delle specificità applicative dei singoli sistemi di IA, in modo da adattarla ai casi d'uso e ai contesti specifici in cui operano i sistemi.

[58] Comunicazione, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit.

[59] Sempre all'interno della Comunicazione, *L'Intelligenza artificiale per l'Europa*, cit., la Commissione auspica che venga adottato «un approccio coordinato per sfruttare al massimo le opportunità offerte dalla IA». In tale documento la Commissione evidenzia altresì come l'Europa si collochi molto dietro a Stati Uniti e Cina quanto ad investimenti nel settore – nel 2016 circa 2 miliardi dell'Unione contro i 12 miliardi in USA e i 7 miliardi in Cina e nell'area asiatica. N. BOLDRINI, *Intelligenza Artificiale: Europa "terza incomoda" tra Cina e Usa?*, cit., disponibile online; P. POCCIANTI, *Le potenze investono sull'intelligenza artificiale: il ruolo dell'Europa tra Usa e Cina*, in Agenda Digitale, 22 febbraio 2019, disponibile online.

[60] Libro Bianco sull'intelligenza artificiale, *Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020, COM(2020) 65*final*.

[61] La Commissione rileva che anche in tema di responsabilità, le dimensioni e l'effetto combinato delle sfide poste dall'IA potrebbero rendere il quadro normativo non idoneo a proteggere le vittime e avanza l'ipotesi di prendere in considerazione alcuni adeguamenti della direttiva sulla responsabilità per danno da prodotti difettosi e dei regimi nazionali in materia di responsabilità attraverso iniziative unitarie europee che adottino un approccio mirato e basato sul rischio. Si vedano in tema di responsabilità per i servizi online le riflessioni di G.M. RUOTOLO, *La disciplina europea della responsabilità dei fornitori dei servizi online tra regime pregresso, proposte di riforma e un rischio di* bis in idem, *cit.*, p. 59 ss.

[62] Nella prima delle due, Comunicazione della commissione al parlamento eu-

All'interno del Libro Bianco sono compendiate buona parte delle problematiche (e delle soluzioni) affrontate, più o meno compiutamente, nelle precedenti iniziative intraprese dalle istituzioni europee[63].

Dalla lettura del documento emerge piuttosto chiaramente l'idea di un'Europa che non vuole perdere la sfida né in termini umani né in termini di competitività e che non vuole mancare l'appuntamento con il futuro pur rimanendo fedele alle proprie conquiste in tema di diritti fondamentali e di libertà. Quella che viene delineata è una strategia *win-win* che si traduce in due macro concetti: "ecosistema di eccellenza" ed "ecosistema di fiducia"[64]. L'intero documento è permeato da una visione propositiva e perva-

ropeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni, *Plasmare il futuro digitale dell'europa, Bruxelles*, 19.2.2020 com(2020) 67*final*, la Commissione fissa i tre principali obiettivi dell'azione europea in tema di tecnologie emergenti: dar vita ad una tecnologia al servizio delle persone; sviluppare un'economia equa e competitiva; costruire una società aperta, democratica e sostenibile fondata sul valore del rispetto dei diritti fondamentali. Nella seconda, *Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'internet delle cose e della robotica in materia di sicurezza e di responsabilità*, Bruxelles, 19.2.2020 com(2020) 64*final*, disponibile online, la Commissione evidenzia che devono essere assicurate la sicurezza, l'affidabilità e la costanza nel funzionamento delle tecnologie digitali emergenti e che devono essere previsti meccanismi solidi per rimediare agli eventuali danni verificatisi – ossia deve essere introdotto un solido quadro delle responsabilità – che sia in grado di assicurare una tutela effettiva.

[63] Sia consentito rinviare per alcune riflessioni sul documento a C. GRIECO, *Le linee guida della commissione europea e il libro bianco sull'intelligenza artificiale*, in R. Giordano, A. panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale, Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, pp. 475-492.

[64] È stato opportunamente osservato che i termini utilizzati non sono affatto casuali. Il termine "ecosistema", mutuato dalla biologia, restituisce perfettamente un'immagine di equilibrio dinamico che deve crearsi tra le diverse componenti di un sistema affinché questo possa operare con successo. M. ZANICHELLI, *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in A. D'ALOIA (a cura di) *Intelligenza artificiale e diritto, come regolare un mondo nuovo*, Milano 2021, p. 56 e ss.

siva di intelligenza artificiale che deve però realizzarsi nel pieno rispetto dei diritti individuali e collettivi[65].

Proprio con riferimento alla tutela dei diritti fondamentali, la Commissione evidenzia che per raggiungere il secondo obiettivo, ovvero creare un "ecosistema di fiducia", il ruolo centrale deve essere svolto dalle istituzioni europee chiamate a implementare un quadro normativo chiaro, coerente e puntuale che miri innanzitutto a garantire la certezza del diritto, assicurando la sicurezza degli individui nell'utilizzo delle tecnologie di intelligenza artificiale ma anche dettando regole certe per gli operatori del settore[66].

Cionondimeno, non si può sottacere la difficoltà intrinseca nell'elaborazione di un quadro normativo esauriente a causa della rapidissima evoluzione della tecnologia. Quello del digitale infatti, è uno di quei settori in cui il diritto, più che accompagnare una trasformazione gentile della società, si trova a rincorrere una realtà in continuo cambiamento quasi impossibile, o addirittura controproducente, da cristallizzare in una norma. Ciò che correttamente la Commissione auspica è di poter dar vita ad un quadro normativo coerente ma "aperto" ai nuovi futuri sviluppi, che si limiti a fornire risposte adeguate a problematiche chiaramente individuabili per le quali esistono già soluzioni praticabili[67].

[65] Viene evidenziato che le aree di intervento stabilite all'interno del Libro bianco devono essere lette, in quanto complementari, unitamente a quelle del piano presentato in parallelo nella strategia europea per i dati. I dati devono essere conformi ai principi FAIR, *Findable, Accessible, Interoperable and Reusable*, cioè dati reperibili, accessibili, interoperabili e riutilizzabili, v. *Piano d'azione del gruppo di esperti della Commissione sui dati FAIR,* 2018, disponibile online.

[66] Viene posto l'accento sul fatto che, unitamente alla mancanza di investimenti e di competenze, la mancanza di fiducia è uno dei fattori principali che pone un freno alla diffusione dell'intelligenza artificiale.

[67] Rilevando l'assenza di un quadro giuridico uniforme alcuni Stati membri hanno iniziato a muoversi in autonomia. La Commissione tedesca per l'etica dei dati ha predisposto un sistema normativo su cinque livelli basato sul rischio che spazi dall'assenza di regolamentazione per i sistemi di IA più innocui ad un divieto totale per i più pericolosi. La Danimarca ha recentemente avviato il prototipo di un "marchio per l'etica dei dati". Malta ha introdotto un sistema di certificazione volontaria per l'intelligenza artificiale. In tema di prospettive e criticità dei meccanismi di certificazione cfr. A. HENRIKSEN, *Certification Standards and Ex-*

Secondo la Commissione, la normativa di settore, adottando un approccio basato sul rischio, deve includere una definizione di intelligenza artificiale abbastanza flessibile da accogliere il progresso tecnico ma anche sufficientemente precisa da garantire la necessaria certezza del diritto[68]. In questo modo, diventa possibile costruire un sistema basato sulla gradualità e la proporzionalità degli interventi. Le prescrizioni obbligatorie e bloccanti si dovrebbero applicare solo ai sistemi di intelligenza artificiale classificati come ad "alto rischio"[69], ovvero quelli che sulla base di criteri certi e predeterminati, implicano rischi significativi e inaccettabili per i diritti fondamentali, la sicurezza e i diritti dei consumatori.

Nel corso del 2022, quindi all'incirca un anno dopo la presentazione della proposta di Regolamento sull'intelligenza artificiale[70], a dimostrazione di quanto il tema dell'innovazione tecnologica sia in cima all'agenda delle istituzioni europee, la Commissione ha sotto-

planation Methods in Applied IA, in AIES 21, Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics and Society, 2021, p. 574. Per un approfondimento sulle regole etiche si veda altresì il contributo di P. CIHON, M. KLEINALTENKAMP, J. SCHUETT, S. D. BAUM, *AI Certification: Advancing Ethical Practice by Reducing Information Asymmetries*, in *IEEE Transactions on Technology and Society*, 2021, p. 200 ss.

[68] L'approccio non è unanime sul punto. Una coalizione di 14 Stati (Danimarca, Belgio, Repubblica Ceca, Finlandia, Francia, Estonia, Irlanda, Lettonia, Lussemburgo, Olanda, Polonia, Portogallo, Spagna e Svezia) ha firmato un *position paper* intitolato "*Innovative and trustworthy AI: two sides of the same coin*". La proposta è di continuare ad adottare atti di *soft law* per la regolamentazione dell'intelligenza artificiale ad alto rischio più che un vero e proprio documento normativo. L'obiettivo è evitare la messa a punto di barriere legali e requisiti onerosi, difficili da rispettare e, quindi, di ostacolo all'innovazione e al progresso scientifico del settore. L'adozione di meccanismi volontari, favorirebbe la collaborazione dei vari soggetti coinvolti nella progettazione, diffusione e utilizzo dell'IA, creando appunto quel clima di fiducia auspicato dalla Commissione.

[69] Viene chiarito che affinché un'applicazione di intelligenza artificiale possa essere considerata ad "alto rischio" devono ricorrere due criteri tra loro cumulativi: in primo luogo l'intelligenza artificiale deve essere utilizzata in un settore intrinsecamente considerato ad alto rischio; in secondo luogo le modalità applicative devono essere tali da poter generare rischi significativi.

[70] Su cui *infra* cap. III.

posto a Parlamento e Consiglio la *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*[71].

Il documento non contiene nuovi diritti specificamente dedicati al settore del digitale[72]. A tale conclusione si può pervenire anche leggendo il preambolo del documento secondo cui la Dichiarazione «si basa segnatamente sul diritto primario dell'UE» e allo scopo vengono richiamati i Trattati, la Carta di Nizza ma anche la giurisprudenza della Corte di giustizia, il diritto derivato, le dichiarazioni degli Stati membri e le risoluzioni del Parlamento europeo. Viene, infatti, esplicitamente evidenziato che l'Unione europea è «un'unione di valori», sancita dall'articolo 2 del trattato sull'Unione europea e che, secondo la Carta di Nizza, si fonda sui valori indivisibili e universali della dignità umana, della libertà, dell'uguaglianza e della solidarietà. Ma soprattutto, viene evidenziato che «con l'accelerazione della trasformazione digitale è giunto il momento che l'UE specifichi come si dovrebbero applicare nell'ambiente digitale i suoi valori e diritti fondamentali applicabili *offline*. La trasformazione digitale non dovrebbe comportare una regressione dei diritti per cui ciò che è illegale *offline* è illegale *online*.

La Dichiarazione, pur non essendo unicamente incentrata sul tema dell'intelligenza artificiale, merita comunque un approfondimento in questa sede poiché contribuisce a chiarire la visione comune perseguita dalle istituzioni europee, che si pone nell'ottica di affrontare, a tutto tondo, il tema dell'evoluzione tecnologica.

[71] La Dichiarazione è stata firmata il 15 dicembre 2022 sulla base di una proposta della Commissione (COM (2022) 28*final*), del 22 gennaio 2022. Si vedano per alcune considerazioni sulla Dichiarazione E. QUINN, *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in *verfassungsblog.de*, 22 December 2022, disponibile online; L. CIANCI, *Dichiarazione europea sui diritti e principi digitali: quid pluris?*, in *Diritto pubblico comparato ed europeo*, 2022, p. 381 ss.; P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?,* cit., disponibile online.

[72] COM (2022) 28*final*, cit., punti 3 e 10. In dottrina è stato osservato da A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali,* cit., p. 330, che: «la Dichiarazione sembra, tuttavia, accogliere non tanto un approccio di tipo integrativo delle fonti vigenti quanto, piuttosto, si propone di far sì che i diritti già garantiti nel mondo reale lo siano anche in quello virtuale, seguendo la linea guida che sollecita a parificare la tutela dei diritti *online* a quella garantita *offline*».

L'atto in questione, peraltro, si pone in continuità con altre iniziative precedenti quali la "Dichiarazione di Tallinn sull'*e-government*"[73], la "Dichiarazione di Berlino sulla società digitale su un governo digitale fondato sui valori"[74] e la "Dichiarazione di Lisbona – Democrazia digitale con uno scopo"[75].

All'interno del preambolo della Dichiarazione è contenuto un nuovo monito affinché si adotti un modello di trasformazione digitale che rafforzi la dimensione umana della tecnologia nel contesto del mercato unico, che risulti anche funzionale alla lotta ai cambiamenti climatici e alla protezione dell'ambiente. Inoltre, nel ricordare i diritti più pertinenti nel contesto della trasformazione digitale, la Commissione auspica che il documento diventi un punto di riferimento per imprese e quanti sono impegnati nello sviluppo e nella diffusione di nuove tecnologie e, allo stesso tempo, e sia utile ad orientare la visione dei responsabili politici verso una trasformazione digitale "umanocentrica" basata sulla solidarietà e sulla sostenibilità e finalizzata a promuovere l'inclusione, la libertà di scelta, la partecipazione, la sicurezza, la protezione, il conferimento di maggiore autonomia e la responsabilità.

D'altra parte, la Dichiarazione si inserisce nel contesto dell'altra comunicazione della Commissione denominata *Bussola per il digitale 2030: il modello europeo per il decennio digitale*[76], all'interno della

[73] Il 6 ottobre 2017 a Tallinn i rappresentanti di trentadue Paesi UE ed EFTA (tra i quali l'Italia con il Commissario Straordinario per l'attuazione dell'Agenda digitale, Diego Piacentini) hanno firmato la Dichiarazione che definisce le linee d'azione in materia di *eGovernment* per i prossimi cinque anni.

[74] Dichiarazione di Berlino sulla società digitale e il governo digitale basato sul valore firmata l'8 dicembre 2020 dai ministri responsabili di tutti gli Stati membri dell'UE.

[75] Si tratta di un'iniziativa della Presidenza portoghese del Consiglio dell'Unione europea che ha inteso definire un nuovo paradigma di transizione digitale. È stata lanciata durante l'evento *Leading the Digital Decade* il 1° giugno 2021 ed è stata istituita per rafforzare il "modo europeo di fare affari" come una proposta di valore riconosciuto a livello mondiale e un vantaggio competitivo unico che si propone di elevare gli *standard*, bilanciando lo sviluppo tecnologico con il rispetto dei principi etici e la promozione dei diritti umani.

[76] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the*

quale si auspica che, in linea con i valori sovranazionali, la trasformazione digitale si realizzi in un mondo aperto e interconnesso in cui imprese innovative, cittadini e autorità coesistano, dando vita ad una società digitale antropocentrica, inclusiva, fiorente e sostenibile[77].

La Dichiarazione contiene, altresì, riferimenti espliciti alla sovranità digitale, al rispetto dei diritti fondamentali, allo Stato di diritto e alla democrazia, all'inclusione, all'accessibilità, all'uguaglianza, alla sostenibilità, alla resilienza, alla sicurezza, al miglioramento della qualità della vita, alla disponibilità di servizi e al rispetto dei diritti e delle aspirazioni di ciascuno[78].

Le istituzioni, ed in particolare la Commissione, auspicano che il documento contribuisca a guidare i responsabili politici nella riflessione sulla loro visione della trasformazione digitale che metta al centro le persone, sostenga la solidarietà e l'inclusione, tramite la connettività, l'istruzione, la formazione e le competenze digitali,

regions 2030 Digital Compass: the European way for the Digital Decade, Brussels, 9 marzo 2021, COM(2021) 118*final* testo reperibile online. Per tradurre le ambizioni digitali dell'UE per il 2030 in termini concreti, la Commissione il 9 marzo 2021 ha presentato una bussola per il digitale concepita attorno a quattro punti cardinali: 1) cittadini dotati di competenze digitali e professionisti altamente qualificati nel settore digitale; 2) infrastrutture digitali sostenibili, sicure e performanti; 3) trasformazione digitale delle imprese; 4) digitalizzazione dei servizi pubblici. Si vedano in dottrina le considerazioni di A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali,* cit., p. 322. L'A. evidenzia come «la finalità dell'Unione è, in sintesi, quella di promuovere l'evoluzione tecnologica e, più in particolare, il processo di digitalizzazione, massimizzando i benefici che ne derivano sia nel settore pubblico (soprattutto riguardo ai servizi), sia nell'attività delle imprese, nonché nello sviluppo di infrastrutture di ricerca e nella formazione»

[77] Peraltro, lo stesso Consiglio europeo, all'interno delle conclusioni del 25 marzo 2021, aveva già avuto modo di sottolineare il ruolo fondamentale svolto dalla trasformazione digitale per la crescita, la prosperità, la sicurezza e la competitività dell'Unione europea, come anche per il benessere della società e aveva invitato la Commissione a fare ricorso "a tutti gli strumenti disponibili", nell'ambito delle politiche industriale, commerciale e della concorrenza.

[78] In dottrina A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali*, cit., p. 322, dove si legge che «il richiamo ai principi e diritti fondamentali esplica, anzitutto, la funzione di limite alle applicazioni tecnologiche».

condizioni di lavoro giuste ed eque nonché l'accesso a servizi digitali online.

Per ciò che riguarda strettamente il tema dell'intelligenza artificiale, la Dichiarazione affronta le questioni della libertà di scelta e dell'interazione con i sistemi algoritmici. Anche in questo caso, è presente un continuo ammonimento a tutelare e rispettare i diritti fondamentali e i valori europei. Si richiede infatti, che vengano adottate tutte le misure che possano garantire il rispetto dei diritti degli individui. In particolare, viene evidenziato che ogni persona dovrebbe essere messa nelle condizioni di godere dei benefici offerti dall'intelligenza artificiale pur mantenendo la propria libertà di effettuare scelte informate, anche nell'ambiente digitale, e rimanendo sempre protetta dai rischi e dai danni alla salute[79], alla sicurezza e vedendo tutelati i propri diritti individuali.

Peraltro la Commissione, consapevole della dimensione sovraterritoriale del digitale e, ancora di più, delle tecnologie di intelligenza artificiale, ha contribuito a porre in risalto la portata globale dei principi sanciti all'interno della Dichiarazione, inserendo – all'interno del preambolo[80] – un riferimento ai diritti umani universali, con l'ambiziosa intenzione di "ispirare" gli altri attori internazionali, chiamati anche loro, in particolare oltreoceano, a governare lo sviluppo straordinariamente rapido che sta avendo il fenomeno dell'intelligenza artificiale.

[79] Si veda per tutti sul tema delle competenze e dei valori dell'Unione declinati proprio con riferimento al tema del diritto alla salute G. DI FEDERICO, S. NEGRI, *Unione Europea e salute. Principi, azioni, diritti e sicurezza*, Padova, 2020 e anche A. NATO*, Il diritto alla salute dei cittadini dell'Unione e l'assistenza sanitaria transfrontaliera: recenti sviluppi,* in *Studi sull'integrazione europea,* 2-3/2016, pp. 573-590. Inoltre, con particolare riferimento al rapporto tra diritto alla salute, sovranità nazionale e pratiche discriminatorie si vedano, nello specifico, i seguenti contributi di G. DI FEDERICO, *Access to Healthcare in the European Union: Are EU Patients (Effectively) Protected Against Discriminatory Practices?*, in L.S. Rossi, F. Casolari, *The Principle of Equality in EU Law*, Cham, 2017, pp. 229-253; ID., *Protezione della salute,* in S. Di Allegrezza, R. Mastroianni, F. Pappalardo, O. Pollicino, O. Razzolini, (a cura di), *Carta dei diritti fondamentali dell'Unione europea,* Milano, *2017,* pp. 664-679 e ID., *L'accesso alle cure mediche nell'Unione europea tra diritti fondamentali e sovranità nazionali*, in *Quaderni Costituzionali*, 2013, pp. 679-688.

[80] COM (2022) 28*final*, cit., par. 6.

CAPITOLO TERZO

LA NUOVA PROPOSTA DI REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE E IL QUADRO GIURIDICO EUROPEO IN TEMA DI DIRITTI FONDAMENTALI

SOMMARIO. 1. Inquadramento dell'iniziativa. – 2. Struttura e campo di applicazione della proposta di regolamento sull'intelligenza artificiale. – 2.1. La definizione di "sistema di intelligenza artificiale". – 3. L'approccio basato sul rischio. – 3.1. Le pratiche vietate. – 3.1.1. La manipolazione. – 3.1.2. Lo Sfruttamento di gruppi vulnerabili. – 3.1.3. Il *social scoring* pubblico. – 3.1.4. L'Identificazione biometrica a distanza in tempo reale. – 3.2. I sistemi "ad alto rischio" e i requisiti da soddisfare. – 3.3. I sistemi c.d. "a medio rischio" e gli obblighi di trasparenza. – 4. Regime sanzionatorio e *governance* europea. – 5. La tutela dei diritti fondamentali nell'ordinamento dell'Unione europea. – 5.1. I diritti fondamentali in Europa: prima e dopo Lisbona. – 5.2. Il rilievo della Convenzione europea per la salvaguardia dei diritti dell'uomo nell'ordinamento dell'Unione europea. 6. Piano della successiva indagine.

1. Inquadramento dell'iniziativa

La proposta di regolamento sull'intelligenza artificiale[1] rappresenta ad oggi il testo più importante in materia. A motivo di ciò si considera opportuna, nella dinamica del presente lavoro, una sua trattazione separata.

L'iniziativa da parte della Commissione è giunta in risposta alle richieste esplicite delle altre istituzioni europee[2], che avevano ripe-

[1] Proposta di regolamento del Parlamento europeo e del Consiglio del 21 aprile 2021 COM(2021) 206*final*, 2021/0106 (COD), che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione.

[2] Secondo il Consiglio europeo la proposta dovrebbe «salvaguardare i nostri

tutamente sollecitato un intervento normativo volto ad assicurare il buon funzionamento del mercato interno per i sistemi di intelligenza artificiale nel contesto del quale affrontare, a livello sovranazionale, i rischi emergenti legati a queste nuove tecnologie[3].

La Commissione, nel rispetto degli impegni assunti, nel mese di aprile 2021 ha presentato il testo finale di una bozza di regolamento[4].

Nel solco già delineato dai precedenti atti di *soft law* esaminati nei paragrafi precedenti ed emanati dalle istituzioni europee ma anche dallo stesso Consiglio d'Europa, la Commissione, nell'ambito

valori nonché i nostri diritti fondamentali ed essere socialmente equilibrata. Tale approccio aumenterà l'attrattività del modello europeo». Riunione straordinaria del Consiglio europeo dell'1 e 2 ottobre 2020, Conclusioni, EUCO 13/20, 2020, punto 7.

[3] Quello sull'intelligenza artificiale è solo uno degli atti normativi che si va ad inserire all'interno di una strategia più ampia adottata dalle istituzioni europee sulla *governance* del digitale. In particolare, già a partire dal 2017, sono state intraprese diverse iniziative legislative nel contesto di un più generale programma che coinvolge la regolazione della gestione dei dati, dei servizi del mercato digitale e della robotica. Di recente adozione sono, in particolare, il Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 Settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (*Digital Markets Act*); Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (*Digital Services Act*) Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (*Data Governance Act*).

[4] Come si legge nella Relazione di accompagnamento alla proposta di regolamento, l'Unione prende atto che «l'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale, nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea. Tale azione è particolarmente necessaria in settori ad alto impatto, tra i quali figurano quelli dei cambiamenti climatici, dell'ambiente e della sanità, il settore pubblico, la finanza, la mobilità, gli affari interni e l'agricoltura. Tuttavia gli stessi elementi e le stesse tecniche che alimentano i benefici socio-economici dell'IA possono altresì comportare nuovi rischi o conseguenze negative per le persone fisiche o la società».

di tale proposta, ribadisce la necessità che lo sviluppo e l'impiego dei sistemi di intelligenza artificiale avvenga nel pieno rispetto dei diritti fondamentali, non come mera condizione fine a sé stessa, ma come parametro fondamentale per consentire l'affermazione di un modello europeo nel mondo[5].

Il documento, che propone "un approccio normativo orizzontale all'IA equilibrato e proporzionato"[6], introduce tre categorie: i sistemi incompatibili con i principi del diritto europeo, il cui uso è espressamente vietato; i sistemi considerati ad "alto rischio" il cui utilizzo è sottoposto a stringenti adempimenti e altre forme di intelligenza artificiale destinate a interagire con gli esseri umani[7].

La Commissione ha riconfermato l'approccio basato sul rischio[8], dimostrando di non ritenere accettabile il superamento dei presidi fondamentali posti a tutela della persona, neppure se in gioco ci sono competitività e investimenti. La "terza via" proposta è ancora una volta "umanocentrica" e prevede un utilizzo virtuoso dell'intelligenza artificiale che deve diventare un motore per l'economia europea ma che deve altresì consentire di preservare il nucleo irrinunciabile dei diritti fondamentali e delle libertà. L'obiettivo è dunque quello di gestire l'innovazione e non di subirla.

Gli obiettivi che emergono dalla proposta di regolamento sono molto puntuali e possono così riassumersi: assicurare che i sistemi di intelligenza artificiale immessi ed utilizzati sul mercato europeo siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione; assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nel settore; migliorare la *governance* e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e i requisiti di sicurezza applicabili ai sistemi algoritmici, al fine di facilitare lo sviluppo di un mercato unico di tutte quelle tecnologie che si dimostrino lecite, sicure e affidabili e, infine, prevenire la frammentazione del mercato.

[5] Cfr. A. BRADFORD, *Effetto Bruxelles. Come l'Unione europea regola il mondo*, cit., p. 220 ss.

[6] Proposta di regolamento, *cit.*, p. 3.

[7] V. *infra* paragrafi 3.1.1, 3.1.2, 3.1.3.

[8] V. *infra* paragrafo 3.2.

2. Struttura e ambito di applicazione della proposta di regolamento sull'intelligenza artificiale

La proposta di regolamento, piuttosto articolata, si compone di dodici titoli, che ricomprendono ottantacinque articoli, preceduti da ben ottantanove considerando. Il testo è inoltre corredato da nove allegati tecnici[9].

All'interno della prima parte della proposta, ovvero nel titolo I, vengono definiti l'oggetto e il campo di applicazione del regolamento che, in linea con l'approccio seguito da altre normative di derivazione europea, quali ad esempio il GDPR, risulta essere piuttosto ampio.

In particolare, l'ambito di applicazione *ratione materiae* e *ratione personae* delle nuove regole è puntualmente delineato all'interno dell'articolo 2, dove viene evidenziato che il regolamento si applicherà unicamente agli impieghi di intelligenza artificiale destinati al settore civile con esclusione, quindi, di tutti quei sistemi utilizzati esclusivamente per scopi militari. Sembrerebbero invece ricompresi i materiali *dual use*[10]. Inoltre, viene chiarito che le nuove regole si applicheranno: ai fornitori che immettono sul mercato o mettono in servizio sistemi di intelligenza artificiale all'interno dell'Unione europea, indipendentemente dal fatto che siano stabiliti in un Paese membro o terzo; agli utenti dei sistemi di intelligenza artificiale situati nell'Unione e, infine, ai fornitori e agli utenti di sistemi di intelligenza artificiale situati in un paese terzo, laddove l'*output* prodotto dal sistema sia destinato ad essere utilizzato nell'Unione europea. Le nuove regole, chiaramente, non potranno trovare appli-

[9] Per una disamina generale della proposta si veda il contributo di G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il Regolamento Europeo Sull'intelligenza Artificiale, Analisi informatico-giuridica*, in *i-lex*, 2021, disponibile online.

[10] I beni *'dual use'*, o 'a duplice uso', sono quei prodotti, inclusi i *software* e le tecnologie, che possono avere un utilizzo sia civile sia militare. Essi comprendono tutti i beni che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari. La circolazione di tali beni è disciplinata dal Regolamento europeo 821/2021 e l'*export* è subordinato a specifiche autorizzazioni rilasciate dalle autorità nazionali competenti.

cazione nei confronti delle autorità pubbliche di un paese terzo né delle organizzazioni internazionali, laddove utilizzino i sistemi di intelligenza artificiale nel quadro di accordi internazionali, potranno invece applicarsi nel caso in cui tali sistemi siano impiegati nell'ambito di programmi di cooperazione giudiziaria o investigativa condotti con l'Unione europea o con uno Stato membro.

A motivo del fatto che l'ambito di applicazione previsto nella proposta di regolamento è così ampio ed include anche prodotti forniti da aziende situate in Paesi terzi, qualora siano destinati ad essere utilizzati o trovino comunque applicazione all'interno dei confini dell'Unione, nel corso della presente analisi si è scelto di analizzare anche quei casi di applicazioni di tecnologie algoritmiche avvenute, o comunque testate, al di fuori dei confini europei. Ciò in quanto, verosimilmente, quegli stessi sistemi saranno destinati ad essere commercializzati in Europa o, comunque, ad essere utilizzati da cittadini europei.

L'articolo 3 contiene le definizioni dei termini utilizzati all'interno del documento. Di primaria importanza è certamente la definizione di "sistema di intelligenza artificiale", su cui però ci si soffermerà nel paragrafo successivo[11].

La seconda parte della proposta, che ricomprende i titoli da II a IV, contiene la disciplina delle diverse categorie di sistemi di intelligenza artificiale individuate dal legislatore europeo.

Come si avrà modo di approfondire nei paragrafi a seguire, la Commissione riconferma una classificazione che segue un approccio c.d. *risk-based*, parametrato appunto sui rischi che le caratteristiche intrinseche o l'utilizzo dei vari sistemi di intelligenza artificiale generano. Vengono individuate tre categorie: ovvero i sistemi che comportano (i) un rischio inaccettabile, (ii) un rischio alto, e (iii) un rischio medio o basso.

Il titolo II, che include unicamente l'articolo 5, elenca le "pratiche" – ossia gli utilizzi o gli effetti prodotti dall'intelligenza artificiale – qualificate come proibite dall'ordinamento europeo, in ragione del loro contrasto con i valori o i diritti fondamentali tutelati dall'Unione.

[11] V. *infra* paragrafo 3.2.

Il divieto riguarda quattro categorie: i sistemi che utilizzano tecniche subliminali per distorcere il comportamento delle persone in un modo che provochi o possa provocare a tale persona o ad un'altra un danno fisico o psicologico; le pratiche cd. di manipolazione, che sfruttano le vulnerabilità di determinati gruppi di persone al fine di distorcerne il comportamento in modo potenzialmente dannoso; i sistemi cd. di *social scoring* utilizzati dalle autorità pubbliche allo scopo di valutare o classificare l'affidabilità delle persone in determinati contesti sociali e, infine, l'uso di sistemi di identificazione biometrica a distanza, che include il riconoscimento facciale e vocale in tempo reale in spazi pubblicamente accessibili e per fini di *law enforcement*.

A seguire, il titolo III contiene la regolamentazione dei sistemi di intelligenza artificiale che creano un rischio elevato per la salute e la sicurezza o i diritti fondamentali delle persone fisiche. I sistemi c.d. ad alto rischio sono classificati tenendo in considerazione due diversi parametri: la destinazione d'uso come componenti di sicurezza di determinate categorie di prodotti e la presenza di funzionalità o l'appartenenza a determinati settori socioeconomici che incidono sui diritti fondamentali.

Vengono elencati i requisiti obbligatori che questi sistemi devono soddisfare, con particolare riferimento alla gestione dei dati, agli obblighi di trasparenza e spiegabilità[12] del sistema, alla sicurezza e robustezza tecnica, alla supervisione umana e vengono altresì imposti una serie di obblighi ai fornitori, agli utenti[13] e agli altri soggetti coinvolti nel ciclo di vita delle tecnologie. È previsto che tali sistemi, essendo il loro impiego particolarmente critico e rischioso, pur essendo ammessi, debbano soddisfare dei requisiti più stringenti e debbano essere sottoposti obbligatoriamente ad una valutazione

[12] Si vedano le riflessioni di C. MORELLI, *Intelligenza artificiale e la partita della Explainable AI*, in *Altalex*, 14 giugno 2021, disponibile online.

[13] Secondo la definizione contenuta all'interno della proposta con il termine "utente" ci si riferisce a "qualsiasi persona fisica o giuridica […] che utilizza un sistema di IA sotto la sua autorità": la nozione differisce dunque da quella comune di "utilizzatore finale" del sistema.

preliminare di conformità prima di poter essere commercializzati o, comunque, prima di poter essere utilizzati.

La proposta di regolamento disciplina anche le procedure relative alla valutazione di conformità *ex ante* a cui questi sistemi sono soggetti e gli organismi deputati al controllo.

All'interno del titolo IV vengono elencati ulteriori obblighi di trasparenza – diversi o, comunque, aggiuntivi rispetto a quelli previsti per i sistemi ad alto rischio – a cui sono soggetti determinati sistemi di intelligenza artificiale che presentano rischi specifici per le persone fisiche.

Si tratta, in particolare, di quei sistemi che: (i) interagiscono con gli esseri umani; oppure (ii) sono utilizzati per rilevare le emozioni o determinare l'associazione con determinate categorie (sociali) sulla base di dati biometrici; o, ancora, che (iii) generano o manipolano contenuti audiovisivi (*deepfake*[14]). In tutti questi casi è previsto un particolare obbligo di trasparenza che impone ai produttori di informare l'utilizzatore del fatto che si trova ad interagire con un algoritmo e, dunque, con un sistema di intelligenza artificiale.

Infine, la terza e ultima parte della proposta, che comprende i titoli da V a XII, contiene la normativa sulla *governance* e sul controllo dei sistemi di intelligenza artificiale, insieme alle regole sull'esecuzione del regolamento.

In particolare, il titolo V si pone l'obiettivo di creare un quadro giuridico favorevole all'innovazione tecnologica e sociale. A tale fine, si promuove la creazione di "ambienti normativi controllati" (*normative sandboxes*) per la sperimentazione tecnologica, fornendone una regolamentazione essenziale[15]. Il titolo VI disciplina gli

[14] Il *deepfake*, termine divenuto di uso comune nel 2017, è una tecnica per la sintesi dell'immagine umana basata sull'intelligenza artificiale, usata per combinare e sovrapporre immagini e video esistenti con video o immagini originali, utilizzando una specifica tecnica di apprendimento automatico, conosciuta come rete antagonista generativa. Questa tecnica viene usata per creare falsi video ma anche *fake news*, truffe in rete, per compiere atti di *cyberbullismo* o altri crimini informatici.

[15] Si rimanda a *infra* cap. IV par. 5 per capire come questi spazi di sperimentazione possano essere utilizzati, ad esempio, al fine di favorire il coordinamento tra la proposta di regolamento sull'intelligenza artificiale e l'attuale regolamenta-

organismi di governo del sistema-mercato di intelligenza artificiale a livello dell'Unione e degli Stati membri. Il titolo VII mira ad agevolare le funzioni di *governance* attraverso la creazione di una banca dati europea per i sistemi di intelligenza artificiale ad alto rischio. Il titolo VIII fornisce la regolamentazione del monitoraggio successivo all'immissione sul mercato dei sistemi di intelligenza artificiale, degli obblighi informativi e della vigilanza del mercato. Nel titolo IX si elenca una serie di norme relative alla creazione di codici di condotta per i fornitori di sistemi di intelligenza artificiale non ad alto rischio, che mirano a incoraggiare l'adozione volontaria, anche da parte di questi ultimi, dei requisiti obbligatori per i sistemi ad alto rischio. Gli ultimi titoli contengono norme di carattere generale relative all'esecuzione del futuro regolamento quali, ad esempio, l'obbligo di riservatezza nella gestione delle informazioni, disposto in capo alle autorità pubbliche (titolo X); le norme relative al potere di adottare atti delegati (titolo XI); gli obblighi per la Commissione di valutare regolarmente la necessità di aggiornamenti e di preparare relazioni periodiche sulla valutazione e la revisione del regolamento (titolo XII)[16].

2.1. *La definizione di "sistema di intelligenza artificiale"*

Trovandosi nella necessità di delimitare il campo di applicazione delle nuove regole, la Commissione nell'elaborazione del testo, si è presto trovata dinanzi ad una prima sfida sostanziale, quella di fornire una definizione di "sistemi di intelligenza artificiale"[17].

zione europea in tema di tutela dei dati.

[16] Si veda G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il Regolamento Europeo Sull'intelligenza Artificiale, Analisi informatico-giuridica,* cit., p. 8.

[17] In Italia, in assenza di una compiuta definizione normativa, la qualificazione giuridica dell'IA è stata offerta dal Consiglio di Stato (sezione III) che, con la sentenza del 25 novembre 2021, n. 7891 ha affrontato, per la prima volta, la distinzione tra il concetto di algoritmo e di meccanismi di IA, chiarendo che l'IA costituisce un'evoluzione degli algoritmi e si configura quando «l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole *software* e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza

All'interno dell'articolo 3 è riportata una definizione funzionale e, giocoforza, molto ampia, di sistema di intelligenza artificiale definito come: «qualsiasi *software* sviluppato con una o più delle tecniche e approcci elencati nell'Allegato I al Regolamento che può, per un dato insieme di obiettivi definiti dall'uomo, generare risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono»[18].

Come indicato nel testo, la definizione viene dettagliata all'interno dell'allegato I dove viene riportato un elenco di tecniche e approcci che definiscono il perimetro dei sistemi di intelligenza artificiale.

In particolare, i metodi a cui fa riferimento l'articolo 3, e che sono elencati all'interno dell'allegato I, sono: «gli approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra metodi di ricerca e ottimizzazione». In altre parole, vengono richiamati i tre modelli generali dell'apprendimento automatico, degli approcci basati sulla logica e di quelli statistici.

La definizione fornita dalla Commissione presenta però delle criticità[19].

Sebbene, infatti, all'interno dell'articolo 4 della proposta si preveda il ricorso ad atti delegati per modificare l'elenco delle tecniche

tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico».

[18] Articolo 3 della proposta di regolamento. All'interno dell'articolo 4 viene altresì specificato che il contenuto dell'Allegato I è soggetto a revisione periodica al fine di adeguarne il contenuto agli sviluppi tecnologici che dovessero esserci nel tempo.

[19] È stato osservato che l'approccio *cherry-picking,* utilizzato nel definire l'IA, porterebbe ad escludere dall'ambito di applicazione della proposta alcuni sistemi che presentano un elevato livello di rischio, comparabili con quelli dei sistemi inclusi e, d'altra parte, ad includerne altri che, sebbene facciano ricorso alle tecniche elencate, non necessariamente presentano profili di rischio e che tutto ciò sembra contrastare con l'obiettivo, dichiarato dal legislatore europeo, di voler utilizzare un approccio basato sul rischio e tecnologicamente neutrale V. G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il Regolamento Europeo Sull'intelligenza Artificiale, Analisi informatico-giuridica,* cit., p. 10.

e degli approcci definiti nell'allegato I, al fine di mantenere l'elenco aggiornato agli sviluppi futuri del mercato e delle tecnologie, la definizione fornita e l'elenco rischiano di risultare troppo restrittivi per alcuni aspetti e, al contempo, troppo ampi per altri.

La definizione contenuta nell'articolo 3, infatti, mette in luce la volontà della Commissione di fornire una cornice di riferimento ampia che risulti, per quanto possibile, priva di tecnicismi, ma piuttosto focalizzata sulle modalità con cui i sistemi di intelligenza artificiale interagiscono con il mondo esterno, in linea con il modello *risk-based* scelto per la proposta. Diversamente, l'elenco contenuto nell'allegato I presenta, già ad una prima lettura, un linguaggio molto più tecnico, essendo chiaramente rivolto agli operatori del settore che, come tali, sono in grado di comprendere anche una terminologia più dettagliata.

Nondimeno, è proprio sulla scelta di includere un elenco che potrebbero profilarsi alcune criticità[20].

A ben vedere, infatti, il richiamo esplicito ai tre approcci contenuto all'interno dell'allegato I potrebbe portare ad includere anche sistemi che, normalmente, non sono considerati di intelligenza arti-

[20] La Risoluzione del Parlamento europeo su un regime di responsabilità civile per l'Intelligenza artificiale 2020/2014(INL) adotta una definizione molto più generica e astratta, ovvero un sistema che è basato su *software* o incorporato in dispositivi *hardware*, e che mostra un comportamento che simula l'intelligenza, tra l'altro, raccogliendo ed elaborando dati, analizzando e interpretando il suo ambiente, e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici". Questa definizione, che appare anche più simile a quella proposta originariamente dal Gruppo di esperti di alto livello, appare più neutrale dal punto di vista tecnologico e maggiormente in linea con una valutazione dell'IA basata sul rischio. È stato osservato che non si vede il motivo per la Commissione di definire specifici modelli di IA, ben potendo la proposta limitarsi a disciplinare l'IA e le decisioni algoritmiche in senso lato, ed è stato evidenziato che questa scelta potrebbe addirittura accrescere l'incertezza giuridica, anche tra gli operatori del settore, poiché il confine fra le varie tecniche elencate non è sempre chiaro (ad esempio tra calcoli complessi e approcci statistici, o ancora tra approcci logici e procedurali) e non risulta sempre agevole determinare se un certo sistema di IA adotti o meno le tecniche definite V. G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il Regolamento Europeo Sull'intelligenza Artificiale,* cit., p. 8.

ficiale, particolarmente laddove si consideri anche l'inclusione di modelli logici e statistici, che in pratica ricomprendono la grande maggioranza dei sistemi che si basano su decisioni algoritmiche[21]. Al contrario, se la definizione di intelligenza artificiale e l'elenco fornito dovessero essere interpretati in maniera troppo restrittiva, potrebbero risultarne escluse alcune applicazioni generate con sistemi algoritmici che, sebbene sviluppate attraverso metodi tradizionali, presentano comunque un alto grado di rischio, specialmente quando non sottoposte al controllo umano[22].

3. L'approccio basato sul rischio

Come più volte ricordato, la proposta di regolamento, nel dettare regole uniformi per lo sviluppo e l'impiego di sistemi di intelligenza artificiale, è concepita secondo un approccio *risk-based*. La nuova disciplina infatti, è stata elaborata per tentare di ridurre al minimo i rischi per la sicurezza e i diritti degli utilizzatori che potrebbero derivare dall'impiego di sistemi di intelligenza artificiale e, allo scopo, è stata predisposta una disciplina che prevede l'adeguamento di tali sistemi a *standard* qualitativi elevati sin dalle primissime fasi di progettazione e sviluppo.

Nondimeno, nel corso di lavori preparatori, anche grazie agli studi settoriali affidati a comitati di esperti e alle estese consultazioni pubbliche avviate, che hanno consentito la partecipazione attiva al processo decisionale e un confronto aperto tra istituzioni e cittadini, ci si è resi conto dell'esistenza di una serie di pratiche generali e di impieghi specifici di intelligenza artificiale che generano dei rischi talmente elevati per i diritti degli utilizzatori da dover introdurre, in alcuni casi espliciti, divieti o in altri, quantomeno, delle adeguate e severe misure di attenuazione e di controllo.

[21] Si veda V. DIGNUM, *Responsible artificial intelligence: how to develop and use AI in a responsible way*, Cham, 2019, p. 9 ss.

[22] A. BIBAL, M. LOGNOUL, A. DE STREEL, B. FRÉNAY, *Legal Requirements on Explainability in Machine Learning*, in *Artificial Intelligence and Law*, 2021, pp. 149–169.

3.1. *Le pratiche vietate*

Come ricordato, l'elenco dei sistemi di intelligenza artificiale caratterizzati dal livello di rischio più elevato è contenuto all'interno del titolo II della proposta che include il solo articolo 5[23].

In questo caso, la Commissione non definisce i sistemi vietati

[23] L'articolo 5 elenca le pratiche di intelligenza artificiale delle quali è vietata nell'Unione l'immissione in commercio, in servizio o in uso, ovvero:

a) un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

b) un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

c) sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari:

i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;

d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;

ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;

iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro.

bensì identifica alcune pratiche poste in essere mediante l'utilizzo di sistemi algoritmici che generano, o che potrebbero generare, effetti considerati inaccettabili poiché in contrasto con i valori e i diritti fondamentali dell'Unione. Per queste pratiche, il legislatore europeo pone un divieto generalizzato, salvo ammettere limitate eccezioni in casi particolari.

Nella specie, la proposta di regolamento vieta l'uso di sistemi di intelligenza artificiale "progettati per manipolare il comportamento umano, le decisioni o le opinioni, per un fine dannoso". Stessa sorte per le tecnologie in cui l'impiego di sistemi di intelligenza artificiale abbia la finalità di predire il comportamento o di sfruttare le vulnerabilità di persone o di gruppi sociali. Inoltre, in linea con il dettato del GDPR, con cui la nuova regolamentazione dovrà dialogare in modo stretto e costante, essendo i dati il principale nutrimento degli algoritmi[24], la Commissione, pur non arrivando a vietare qualsiasi tipo di trattamento automatizzato, impone severe limitazioni.

Di seguito ci si soffermerà nel dettaglio sul contenuto delle quattro pratiche proibite, così come identificate nella proposta di regolamento.

3.1.1. La manipolazione

L'articolo 5 (1), lettera a), vieta «l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico».

La norma introduce la nozione di manipolazione. Rispetto alle prime versioni del testo, il concetto ha subito delle modifiche ed è stato dettagliato in maniera più precisa[25]. Nella proposta così come

[24] Cfr. G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, cit., p. 207 ss.

[25] L'articolo 4 della versione non ufficiale della proposta recitava «AI systems designed or used in a manner that manipulates human behaviour, opinions or decisions through choice architectures or other elements of user interfaces, causing

adottata, la Commissione si focalizza, non tanto sulla struttura del sistema di intelligenza artificiale, ma sull'utilizzo di "tecniche subliminali" che agiscono senza che l'utilizzatore ne abbia conoscenza.

Quanto agli effetti, la versione definitiva della proposta, rispetto alle prime elaborazioni, ne ha ristretto l'ambito[26]. Il divieto riguarda, infatti, unicamente l'impiego di quelle "tecniche subliminali" che in maniera inconsapevole portano un soggetto a distorcere il proprio comportamento in modo tale da condurlo ad arrecare un danno fisico o psicologico, anche solo potenziale, a sé stesso o ad un'altra persona.

V'è da dire che così come proposta, la definizione fornita dalla Commissione scopre il fianco ad alcune criticità.

In primo luogo, non viene esplicitato il significato dell'espressione "tecniche subliminali" generando così, di fatto, incertezza tra operatori del settore ma anche tra gli utenti e gli utilizzatori finali e, in secondo luogo, non viene chiarito che grado e che tipo di "mancanza di consapevolezza"[27] sia richiesta al soggetto nel momento in cui si trovi ad interagire con questi sistemi perché possa ricadersi nel divieto sancito dall'articolo 5. Anche l'identificazione del danno discendente dalla manipolazione potrebbe creare dei problemi, soprattutto quando ci si riferisce al danno di natura psicologica, notoriamente moto più complesso da provare rispetto al danno fisico. Peraltro, considerato che è certamente più verosimile che l'interazione con questi sistemi causi proprio danni psicologici piuttosto che fisici, l'incertezza derivante dalla mancanza di chiarezza, in definitiva, rischia di lasciare l'utilizzatore privo di tutela effettiva.

Il timore è fortemente accentuato dall'avvento sempre più prepotente del c.d. *Emotional Web* e dal crescente utilizzo di sistemi di

a person to behave, form an opinion or take a decision to their detriment».

[26] La versione precedente includeva tutte le possibili attività poste in essere dai sistemi idonee ad influenzare i comportamenti degli individui, incluse opinioni o decisioni, e ad arrecare un pregiudizio.

[27] Nella versione del testo in inglese, è utilizzato il termine *consciousness* che è stato osservato sembra conferire al divieto un significato metagiuridico e filosofico V. G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il Regolamento Europeo Sull'intelligenza Artificiale, Analisi informatico-giuridica,* cit., p. 12.

intelligenza artificiale in grado di identificare gli stati emotivi dei soggetti con cui interagiscono e, addirittura, di influenzarli[28].

Il rischio che si profila è che, seppur apprezzabile nell'intento, il divieto di manipolazione rimanga solo sulla carta e non trovi poi applicazioni nella pratica e, in ultima analisi, non risulti idoneo a tutelare effettivamente gli utilizzatori finali dinanzi ad eventuali tentativi di manipolazione perpetrati mediante l'impiego di sistemi di intelligenza artificiale.

3.1.2. Lo Sfruttamento di gruppi vulnerabili

A seguire, l'articolo 5 (1), lettera b), introduce la seconda pratica proibita che consiste nell'uso di un sistema «che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico».

Il divieto è dunque rivolto a tutelare unicamente gruppi specifici di persone considerati vulnerabili.

Anche in questo caso, però, la disposizione, così come concepita dalla Commissione, presenta delle lacune e ha suscitato diverse perplessità, anche in ordine alla stessa opportunità di un suo mantenimento in un eventuale testo definitivo.

È stato opportunamente osservato, infatti, che non viene fornito alcun chiarimento sul significato del termine "sfruttamento" e che per ciò che riguarda specificamente l'approccio concettuale alla questione della "vulnerabilità", si fa riferimento unicamente a gruppi accomunati da età o disabilità fisica e mentale ma non vengono prese in considerazione altre tipologie di vulnerabilità che ben potrebbero presentarsi e che senz'altro, nell'interazione con i si-

[28] C. BURR, N. CRISTIANINI, *Can Machines Read our Minds?,* in *Minds & Machines,* 29, 2019, pp. 461–494; S. MATZ, S. C. KOSINSKI, M. NAVE, G.D.J. STILLWELL, *Psychological targeting as an effective approach to digital mass persuasion, Proceedings of the National Academy of sciences*, 2017, pp. 12714-12719; V. PACKARD, *The hidden persuaders*, New York, 1957, cap. 3 ss.

stemi algoritmici, si presentano con maggiore frequenza. Ci si riferisce, in particolare, a vulnerabilità generate da esclusione ed emarginazione sociale, difficoltà finanziarie e differenze di genere.

Di recente, infatti, la nozione di vulnerabilità sta assumendo contorni diversi e molto più flessibili, che tengono in considerazione non solo le caratteristiche proprie di ciascun individuo, ma anche fattori esterni e transitori[29].

Peraltro, quando si parla di interazione con sistemi algoritmici, includere un concetto più ampio di vulnerabilità, non necessariamente connesso a caratteristiche proprie del singolo individuo, potrebbe risultare particolarmente opportuno posto che, nella maggior parte dei casi, gli utilizzatori di questi sistemi raramente sono classificati in base a categorie socioculturali mentre, molto più spesso, sono categorizzati sulla base dei comportamenti tenuti in rete o di preferenze espresse.

A ciò si aggiunga che la maggior parte delle volte in cui ci si trova ad interagire con sistemi di intelligenza artificiale, la vulnerabilità non ha origine nelle caratteristiche individuali e non è circoscritta a specifici gruppi, ma è intrinseca nell'algoritmo[30].

3.1.3. Il *social scoring* pubblico

L'articolo 5 (1), lettera c), vieta: «l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di perso-

[29] Si veda C. MACKENZIE, W. ROGERS, S. DODDS, *Vulnerability: New essays in ethics and feminist philosophy*, Oxford, 2014, p. 20 ss.

[30] Cfr. C. BURR, N. CRISTIANINI, J. LADYMAN, *An Analysis of the Interaction Between Intelligent Software Agents and Human Users*, in *Minds & Machines*, 28, 2018, pp. 735–774.

ne fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità».

La terza pratica vietata riguarda, dunque, quello che è comunemente noto come *social scoring*, ovvero la valutazione e la classificazione dell'affidabilità delle persone sulla base dei loro comportamenti in determinati contesti sociali o di altre caratteristiche individuali[31].

Il legislatore europeo proibisce la commercializzazione di tali sistemi e il loro utilizzo, ma unicamente nei casi in cui a farne uso sia l'autorità pubblica e solo nelle ipotesi in cui l'eventuale punteggio ricavato sia posto alla base di un trattamento pregiudizievole o sfavorevole per gli individui o per gruppi di persone fisiche. Ne consegue che il divieto si estende ai casi in cui: i) l'effetto dannoso si verifica in contesti sociali diversi da quelli in cui i dati utilizzati dal sistema sono stati originariamente generati o raccolti; oppure ii) il danno è ingiustificato o sproporzionato rispetto al comportamento sociale o alla sua gravità.

Anche in questo caso la disposizione suscita delle perplessità. In primo luogo non si comprende come mai il legislatore europeo abbia delimitato il divieto di utilizzo di questi sistemi alla sola autorità pubblica considerato che molto più spesso è il settore privato a farne uso, anche alla luce dell'ondata di privatizzazioni che, negli ultimi decenni in tutta Europa, ha interessato molti dei servizi essenziali[32]. Ne consegue che il fatto di non estendere il divieto anche ai

[31] Il divieto sembra volersi porre in contrasto con la deriva cinese. Nei paesi asiatici, infatti, i sistemi di *social scoring* sono diffusi. In particolare in Cina, i cittadini cinesi, a seconda del comportamento tenuto (es. pagare puntualmente le bollette, fare volontariato, onorare gli impegni contrattuali assunti etc…), possono accumulare punti o perderli. In base al profilo, il sistema ricompensa o penalizza i cittadini in modo importante, ad esempio, agevolando l'accesso al credito, i viaggi e gli spostamenti o, viceversa, limitando i diritti di voto, escludendoli da determinate scuole private o rallentando la connessione *Internet*.

[32] Si pensi, ad esempio, all'accesso ai servizi essenziali quali la fornitura di gas e di acqua, ai servizi di accesso al credito o assicurativi, fino alla possibilità di be-

casi di sistemi di *scoring* usati da privati, che risultano molto diffusi in Europa, sia nel campo dei servizi finanziari sia nelle procedure di *recruiting*, rappresenta una lacuna problematica e molto insidiosa che potrebbe generare un impatto negativo sulla tutela dei diritti fondamentali e, particolarmente sul divieto di discriminazione[33].

3.1.4. L'Identificazione biometrica a distanza in tempo reale

L'ultima pratica vietata prevista dall'articolo 5 (1), questa volta alla lettera d), è l'identificazione biometrica a distanza[34], salvo che non ricorrano delle ipotesi specifiche. Nella specie, la disposizione introduce il divieto di: «uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto».

In linea generale, dunque, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di identificazione biometrica a distanza in tempo reale, ovvero quei sistemi idonei ad effettuare il riconoscimento facciale e vocale[35], risultano vietati.

Nondimeno, la norma prevede talune eccezioni, per il raggiungimento di fini specifici. In particolare, è previsto che si possano utilizzare tali sistemi nel caso in cui l'impiego possa risultare utile: a

neficiare di servizi per il tempo libero sulle piattaforme *online*. Airbnb ha recentemente brevettato un sistema di IA in grado di generare un punteggio sociale per determinare l'affidabilità dei consumatori sulla base di una serie di dati di *social media*. Se operativa, questa applicazione di IA, porterà probabilmente alla discriminazione di alcuni gruppi sociali nel mercato delle case vacanza, che non sarebbe oggetto del divieto di cui all'art. 5, lett. c).

[33] Si rimanda per approfondimenti al capitolo V del presente scritto.

[34] Il riconoscimento biometrico è un sistema algoritmico automatizzato che permette l'identificazione di una persona, anche a distanza, attraverso l'analisi di caratteristiche fisiche uniche e intrasferibili come, ad esempio, le impronte digitali, l'iride, i lineamenti del viso o la voce.

[35] Tali sistemi sono definiti, al punto 37 dell'articolo 3, come sistemi "in cui la cattura dei dati biometrici, il confronto e l'identificazione avvengono senza un ritardo significativo". La definizione è intesa a coprire non solo l'identificazione istantanea, ma anche quella effettuata a breve distanza di tempo; altri tipi di identificazione biometrica sono considerati come "sistema di identificazione biometrica a distanza".

rintracciare potenziali vittime di specifici reati, inclusi i minori scomparsi; a prevenire il verificarsi di un attacco terroristico o comunque a scongiurare una minaccia imminente che metta in pericolo la vita e l'incolumità fisica o, infine, a rintracciare l'autore (o sospettato tale) di un reato che sia punibile nell'ordinamento dello Stato membro interessato con una pena superiore a tre anni.

La prima eccezione riguarda, pertanto, la possibilità di utilizzo di tali sistemi al fine di porre rimedio alle conseguenze di reati quali, ad esempio, la sottrazione di minore o i rapimenti a fini di estorsione. In questi casi, l'utilizzo di sistemi avanzati di riconoscimento facciale o vocale potrebbe facilitare significativamente il ritrovamento della vittima del reato.

La seconda è una misura di tipo preventivo che facoltizza l'utilizzo di tali sistemi ogni qual volta ci si trovi nella necessità imminente di fronteggiare una minaccia specifica che ponga a rischio la vita o l'incolumità fisica delle persone ovvero di impedire il verificarsi di un attacco terroristico.

L'ultima eccezione riguarda invece la giustizia penale[36] e prevede la possibilità di utilizzo di tali sistemi a fini investigativi per assicurare l'autore di un reato alla giustizia. L'utilizzo però non può essere indiscriminato, la norma prevede, infatti, anche in questo caso non senza suscitare qualche perplessità, che l'impiego di tali sistemi sia consentito solo superata una certa soglia di gravità del reato, ovvero che lo stesso sia punito, secondo la legislazione di ciascuno Stato membro, con una pena o una misura di sicurezza privativa della libertà personale della durata massima di almeno tre anni. È evidente quindi che, tenuto conto della mancanza di armonizzazione in questo specifico settore tra i sistemi interni dei vari Stati membri, così come formulata, la disposizione potrebbe generare disparità di trattamento nei vari ordinamenti coinvolti.

[36] Cfr. A. LAVORGNA, G. SUFFIA, *La nuova proposta europea per regolamentare i sistemi di intelligenza artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*, in *Diritto Penale Contemporaneo*, 2021, pp. 88-103.

L'utilizzo di tali sistemi resta comunque subordinato al rispetto di una serie di condizioni, anche procedurali, secondo quanto stabiliscono i punti 2 e 3 dell'articolo 5.

In primo luogo, valutata la natura della situazione, è necessario effettuare un bilanciamento, tra la gravità, la probabilità di aggravamento e l'entità del danno che il mancato uso del sistema causerebbe, da una parte, e le conseguenze che, al contrario, il suo utilizzo generebbe per i diritti e le libertà di tutte le persone coinvolte, dall'altra.

La norma richiede che siano inoltre rispettate le tutele e le condizioni necessarie e proporzionate in relazione all'uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali.

In ogni caso, ciascun singolo utilizzo di tali sistemi è subordinato ad una preventiva autorizzazione da parte dell'autorità giudiziaria, o di un'autorità amministrativa indipendente dello Stato membro, rilasciata su domanda motivata in conformità alle previsioni interne. Tuttavia, è altresì previsto che, in presenza di una "situazione di urgenza debitamente giustificata", risulti possibile ritardare la richiesta di autorizzazione e presentarla anche in fase di utilizzo o subito dopo l'avvenuto impiego del sistema.

L'autorità competente può concedere l'autorizzazione solo se, sulla base di prove oggettive o di chiare indicazioni presentate, l'uso del sistema in questione risulti effettivamente necessario e proporzionato al raggiungimento di uno degli obiettivi consentiti dalla proposta.

In base a quanto dispone la norma, gli Stati membri restano comunque liberi di prevedere la possibilità di autorizzare in via generale l'uso di tali sistemi di identificazione biometrica, sempre nei limiti e alle condizioni di cui ai paragrafi 1, lettera d), 2 e 3.

Quest'ultima previsione, che di fatto amplia notevolmente la possibilità di utilizzo di tali sistemi e, soprattutto, lascia agli Stati un'eccessiva discrezionalità sul punto, potrebbe generare problemi sia livello interpretativo sia di applicazione nella pratica oltre, ovviamente, a generare incertezza giuridica.

3.2. *I sistemi "ad alto rischio" e i requisiti da soddisfare*

All'interno del titolo III, all'articolo 6, è disciplinata la categoria dei sistemi c.d. ad alto rischio, con un richiamo ai contenuti degli allegati II e III.

In linea generale, sono considerati ad alto rischio tutti quei sistemi che, in base alla definizione fornita, «creano un rischio elevato per la salute e la sicurezza o i diritti fondamentali delle persone fisiche».

L'uso di questi sistemi seppur non *a priori* vietato è subordinato al rispetto di una serie di requisiti e ad una valutazione di conformità da effettuarsi *ex ante*, prima che questi sistemi possano essere commercializzati o utilizzati.

L'articolo 6 chiarisce che un sistema di intelligenza artificiale per essere considerato ad alto rischio deve soddisfare contemporaneamente due condizioni, ovvero deve essere destinato a essere utilizzato come componente di sicurezza di un prodotto, o deve essere esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II[37].

La norma specifica che vengono considerati ad alto rischio anche i sistemi elencati all'interno dell'allegato III che include otto macro-aree[38]. Rientrano in questa lista i sistemi di riconoscimento

[37] Che include a titolo esemplificativo la direttiva 2009/48/CE sulla sicurezza dei giocattoli oppure il regolamento (UE) 2017/746 relativo ai dispositivi medico-diagnostici in vitro.

[38] Le aree elencate sono: l'identificazione biometrica; la gestione delle infrastrutture critiche; l'istruzione e la formazione professionale; l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo; l'accesso a prestazioni, servizi pubblici e privati e la fruizione degli stessi; le attività di contrasto; la gestione della migrazione, dell'asilo e del controllo delle frontiere e l'amministrazione della giustizia e dei processi democratici. La Commissione, in tale valutazione di rischio, tiene conto di alcuni criteri, tra i quali, ad esempio, la finalità prevista dal sistema di IA, la misura in cui è usato o verrà impiegato, la portata dell'eventuale danno o impatto negativo su una pluralità di persone, o l'eventuale previsione di legge di contromisure efficaci volte anche a prevenire o ridurre sostanzialmente i rischi. L'elenco è comunque soggetto a continua revisione proprio al fine di aggiornarlo qualora fossero introdotti nuovi sistemi di IA che, incidendo sui settori elencati, potrebbero costituire un rischio di danno per la salute e la sicurezza, o

biometrico, l'amministrazione della giustizia ma anche l'accesso al mondo del lavoro e le attività di contrasto in ambito penale[39].

I sistemi di intelligenza artificiale che fanno parte delle categorie sopra elencate devono rispettare una serie rigorosa di requisiti che includono: la creazione di un sistema di addestramento e validazione[40], un obbligo di qualità e accuratezza nella scelta dei dati[41]; la redazione di documentazione tecnica e i requisiti di trasparenza nei confronti dell'utilizzatore[42].

In particolare, i fornitori di tali sistemi devono predisporre un sistema di gestione della qualità conforme ai requisiti enunciati, il cui rispetto garantisca la conformità di tali sistemi a quanto prescritto dalla proposta di regolamento. Devono inoltre: redigere la documentazione tecnica, conservare i *logs* generati autonomamente ed effettuare una procedura di valutazione sulla conformità, prima di poterlo immettere sul mercato o in servizio. In caso di esito positivo, devono apporre la marcatura CE, come previsto dall'articolo 49 della proposta di regolamento e, in ogni caso, dovranno rendersi

un rischio di impatto negativo sui diritti fondamentali in misura pari o superiore a quelli già previsti dallo stesso allegato.

[39] Nell'ambito della giustizia penale si tratta di quei «sistemi di IA destinati a essere utilizzati dalle autorità di contrasto [...] per la valutazione dell'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati", "per individuare i *deep-fake*", "per la profilazione delle persone fisiche", e "per l'analisi criminale riguardo alle persone fisiche, che consentono alle autorità di contrasto di eseguire ricerche in *set* di dati complessi, correlati e non correlati, resi disponibili da fonti di dati diverse o in formati diversi, al fine di individuare modelli sconosciuti o scoprire relazioni nascoste nei dati».

[40] Proposta di regolamento*,* cit., art. 9.

[41] Proposta di regolamento*,* cit., art. 10.

[42] Proposta di regolamento*,* cit., art. 13. Il legislatore europeo prevede che siano fornite all'utente tutta una serie di informazioni, quali a titolo di esempio i dati di contatto del fornitore, le finalità del sistema, i rischi connessi ad un uso conforme o improprio. Orbene queste informazioni hanno, tra gli altri, lo scopo di consentire all'utente una valutazione di impatto sulla protezione dei dati a norma dell'articolo 35 del Regolamento UE 2016/679. Per il rapporto tra GDPR, tutela dei dati e proposta di regolamento si rimanda alla seconda parte del presente lavoro al successivo capitolo IV.

disponibili, in una logica di cooperazione, a dimostrare la conformità del sistema su richiesta di un'autorità nazionale competente.

In aggiunta, come ulteriore condizione ai fini dell'immissione sul mercato o della messa in servizio di sistemi ad altro rischio, l'articolo 9 prevede che debba essere strutturato, attuato, documentato e mantenuto un sistema di gestione del rischio, attraverso un costante e sistematico aggiornamento, che provveda ad identificare e analizzare i rischi noti e prevedibili, a stimare e valutare i rischi potenzialmente nascenti da un uso conforme alla finalità e quelli connessi ad un uso improprio; a valutare altri eventuali rischi derivanti dai dati analizzati successivamente alla immissione sul mercato e ad adottare tutte le necessarie misure di gestione. Questa previsione ricorda molto quanto prevede il GDPR, all'articolo 35, laddove prescrive di effettuare obbligatoriamente una "valutazione di impatto sulla protezione dei dati" in tutti quei casi in cui il trattamento possa comportare un rischio elevato per i diritti e le libertà degli interessati[43].

La proposta introduce inoltre un sistema di certificazioni, istituisce una "dichiarazione di conformità europea"[44] e introduce la marchiatura CE per tali sistemi[45]. Viene inoltre mantenuto, anche all'interno della proposta, la valutazione di impatto, già introdotta dal AI HLEG, che ogni attore coinvolto dovrà utilizzare per valutare la propria tecnologia di intelligenza artificiale[46].

Nel caso in cui, anche successivamente alla messa in commer-

[43] La valutazione d'impatto sulla protezione dei dati è richiesta, in particolare, nei seguenti casi: Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; Il trattamento, su larga scala, di categorie particolari di dati personali (art. 9, paragrafo 1 del GDPR) o di dati relativi a condanne penali e a reati (art. 10); La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

[44] Proposta di regolamento*,* cit., art. 48. Per un'analisi della valutazione di conformità si veda J. MÖKANDER, M. AXENTE, F. CASOLARI, L. FLORIDI, *Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI Regulation,* in *Minds and Machines*, 2021, pp. 1–28.

[45] Proposta di regolamento, cit., titolo V.

[46] *Ibidem*, art. 49.

cio, i sistemi evidenzino delle non conformità, è previsto, ai sensi dell'articolo 62 della proposta di regolamento, che gli operatori, in un'ottica di cooperazione, informino le autorità nazionali competenti degli Stati membri in cui hanno messo a disposizione o in servizio il sistema algoritmico dell'esito negativo della procedura di valutazione di conformità, qualora questa sia stata effettuata in un momento successivo, ovvero degli eventuali incidenti rilevati, così come delle misure correttive adottate per correggere le criticità riscontrate.

In un'ottica di responsabilizzazione dell'intera catena di produzione e distribuzione e al fine di evitare rimpalli di responsabilità, è previsto inoltre che gli stessi importatori e distributori, prima di poter immettere sul mercato tali sistemi, dovranno accertarsi che il fornitore abbia effettivamente adempiuto alla procedura di conformità, alla redazione della documentazione tecnica necessaria e all'apposizione della marcatura CE.

3.3. *I sistemi c.d. "a medio rischio" e gli obblighi di trasparenza*

Se tutele maggiori all'interno della proposta di regolamento sono imposte per i sistemi ad alto rischio, anche per l'ultima categoria, ovvero i sistemi a c.d. medio rischio destinati ad interagire con le persone fisiche, è previsto il rispetto di alcuni requisiti relativi, soprattutto, a garantire l'osservanza degli obblighi di trasparenza, quest'ultima intesa come il diritto dell'interessato ad essere informato del fatto che si trovi ad interagire con un sistema intelligenza artificiale[47].

Tale categoria è disciplinata all'interno del titolo IV che, ancora una volta, comprende un solo articolo[48]. All'interno sono elencati tre tipologie di sistemi che, sempre nel rispetto dell'approccio *risk-based* adottato e a causa dei rischi legati al loro potenziale manipo-

[47] Il concetto di "trasparenza" previsto per questi sistemi differisce da quello di "spiegabilità" richiesto dall'art. 13 per i sistemi ad alto rischio. In questo caso, infatti, si richiede di rendere noto all'utilizzatore finale del fatto che sta interagendo con un sistema di IA.

[48] Proposta di regolamento, cit., art. 52.

lativo, devono ottemperare a specifici obblighi di trasparenza nei confronti degli utilizzatori finali del sistema.

Il primo gruppo rientrante in questa categoria include i sistemi "destinati a interagire con le persone fisiche". La definizione, che si ritiene essere stata elaborata in modo volutamente ampio, è stata introdotta dalla Commissione con l'obiettivo di regolamentare l'utilizzo di *software* che impiegano sistemi automatici di intelligenza artificiale, come ad esempio le *chatbot*[49].

A tutela dell'utilizzatore del sistema, si richiede che le persone fisiche siano informate del fatto che si trovino ad interagire con una macchina o che comunque tale situazione risulti "evidente dalle circostanze e dal contesto di utilizzo".

Ancora una volta è prevista un'esclusione da tale obbligo nel settore della giustizia penale nel caso in cui l'uso sia autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o sia necessario per l'esercizio del diritto alla libertà di espressione, seppur nel rispetto dei diritti e delle libertà dei terzi.

Il secondo gruppo, disciplinato dall'articolo 52, include i sistemi di intelligenza artificiale che sono utilizzati per identificare le emozioni[50] o per rilevare dati biometrici[51]. Quest'ultima categoria si differenzia da quella disciplinati dall'articolo 5 lett. d) e dall'allegato III, n. 1, classificati ad alto rischio, in quanto, pur raccogliendo dati ritenuti particolarmente sensibili, non hanno come fine l'identificazione dell'utilizzatore finale.

Da ultimo, il terzo gruppo di sistemi include tutte quelle pratiche che prevedono l'utilizzo di sistemi di intelligenza artificiale con la finalità di generare o manipolare un contenuto, sia esso immagi-

[49] Una *chatbot* è un *software* che simula ed elabora le conversazioni umane (scritte o parlate), consentendo agli utenti di interagire con i dispositivi digitali come se stessero comunicando con una persona reale.

[50] Alla prima categoria possono essere ricondotti, ad esempio, i sistemi di intelligenza artificiale che applicano tecniche di analisi del sentimento o di profilazione psicografica.

[51] Alla seconda categoria possono essere ricollegati invece alcuni *wearable* come gli *smartwatch*, che utilizzano dati biometrici per effettuare valutazioni sullo stato di salute di chi li indossa, ma anche sistemi di riconoscimento vocale come gli assistenti virtuali, si pensi a *Siri* o *Alexa*.

ne, audio o video, che assomiglia sensibilmente a persone, luoghi, oggetti o altre entità o eventi esistenti e che apparirebbe, in maniera ingannevole, all'utilizzatore come autentico o veritiero (*deepfake*). In questi casi, è fatto obbligo agli utenti di rendere noto all'utilizzatore che il contenuto sia stato generato o manipolato artificialmente.

4. Regime sanzionatorio e *governance* europea

Per ciò che riguarda la *governance* europea in materia di intelligenza artificiale, la proposta di regolamento prevede l'istituzione di un Comitato che dovrà lavorare a stretto contatto con le singole autorità nazionali[53]. È inoltre prevista l'istituzione di una rete di *monitoring* e di *reporting* destinata a tenere traccia degli incidenti più gravi.

Sebbene il regime sanzionatorio previsto dalla Commissione sia particolarmente severo, anche più di quello già rigoroso introdotto dal regolamento sulla protezione dei dati personali, si tratta ancora una volta unicamente di sanzioni di tipo economico che, quando si parla di *Smart Tech, Big Tech*, OTT (*Over The Top*), ovvero pochi colossi che si contendono, impedendo l'ingresso a nuovi concorrenti, il dominio digitale sul mondo[54], probabilmente non riescono a sortire l'effetto dissuasivo auspicato[55]. Per i produttori che non si conformeranno alle nuove norme sono previste sanzioni pecuniarie che possono arrivare fino a trenta milioni di euro o al 6% del fatturato globale annuo nel caso delle violazioni più gravi generate da

[53] Proposta di regolamento, cit., art. 56.

[54] Per avere un'idea si consideri che la somma dei titoli quotati a Wall Street solo di Microsoft, Amazon, Apple, Google, e Facebook raggiunge un valore complessivo di 5,2 miliardi di dollari, pari al 18% dell'intero indice S&P500. Un valore più alto dei Pil di Italia e Francia messi insieme, si veda: *Google raggiunge Apple e Microsoft nel club dei mille miliardi. Ma la corsa dei big tech potrebbe essere finita*, in *Business Insider Italia*, 22 gennaio 2020, disponibile *online*.

[55] Si rimanda per alcune ulteriori considerazioni su questo aspetto alle conclusioni del presente scritto.

sistemi di intelligenza artificiale che rientrano tra quelli non consentiti.

La proposta di regolamento introduce una serie di obblighi di prova *ex ante*, di gestione dei rischi e di sorveglianza umana, per ridurre al minimo la possibilità di decisioni errate o distorte assistite dall'intelligenza artificiale. Cionondimeno, nel caso in cui, nonostante vengano rispettati tutti i requisiti, si dovessero comunque verificare violazioni dei diritti fondamentali, la proposta richiede che, a favore delle persone lese, venga riconosciuto e garantito il diritto ad un ricorso effettivo reso possibile assicurando la trasparenza e la tracciabilità dei sistemi di intelligenza artificiale unitamente a rigidi controlli *ex post*.

Tali controlli, posti a carico degli operatori del settore, impongono, di fatto, alcune restrizioni alla libertà d'impresa che a ben vedere, rispondono ad un concetto di "innovazione responsabile" e risultano necessarie al fine di assicurare il rispetto di motivi imperativi d'interesse pubblico, quali la salute pubblica, la sicurezza sociale, la tutela dei consumatori ma anche, dal punto di vista individuale, la tutela della *privacy* e la protezione contro eventuali discriminazioni.

Nella relazione che accompagna la proposta di regolamento si evidenzia, infatti, come gli stessi obblighi di trasparenza imposti agli operatori non incidano in maniera sproporzionata sul diritto alla protezione della proprietà intellettuale poiché sono limitati soltanto alle informazioni minime necessarie affinché le persone possano esercitare il loro diritto a un ricorso effettivo e a garantire la necessaria trasparenza presso le autorità di controllo.

Da ultimo, per ciò che riguarda l'onere probatorio, nella proposta si introduce un regime che presenta molti punti di somiglianza con la responsabilità oggettiva[56]. In caso di lesioni ai diritti individuali, infatti, è il produttore del sistema a dover dimostrare di avere seguito tutte le prescrizioni e di aver effettuato tutti i controlli e che, dunque, il danno non è conseguenza di un difetto di realizzazione o di progettazione della tecnologia.

[56] Si veda G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, cit., p. 214.

L'iter procedimentale di approvazione dell'atto sta procedendo. Le istituzioni mirano a licenziarlo entro il 2024. Attualmente la proposta ha ricevuto una prima approvazione con emendamenti da parte del Parlamento europeo[57].

5. La tutela dei diritti fondamentali nell'ordinamento dell'Unione europea

Dopo aver illustrato l'attuale quadro giuridico in tema di intelligenza artificiale, appare ora opportuno delineare il sistema europeo di tutele in materia di diritti fondamentali, al fine di evidenziare, nell'indagine successiva, i possibili impatti negativi che potrebbero discendere dall'impiego di sistemi di intelligenza artificiale,

[57] Il presente scritto è aggiornato al 30 aprile 2023. Il Parlamento europeo, lo scorso 27 aprile, ha raggiunto un accordo politico provvisorio sulla proposta. La relazione è stata approvata con 84 voti a favore, 7 contrari e 12 astenuti nel corso della riunione congiunta delle commissioni per il Mercato interno e la protezione dei consumatori (Imco) e per le Libertà civili, la giustizia e gli affari interni (Libe). La relazione, presentata dai co-relatori Brando Benifei (S&D) e Dragoş Tudorache (Renew Europe) dovrà ora essere votata alla prossima sessione plenaria in programma tra il 12 e il 15 giugno, in vista dei negoziati interistituzionali con il Consiglio dell'Ue. Il Parlamento ha confermato le proposte della Commissione di imporre obblighi più severi ai modelli di base, ha specificato che i sistemi di IA generativa dovranno essere progettati nel rispetto del diritto europeo e delle libertà fondamentali. Il Parlamento ha inoltre esteso il divieto sui *software* di identificazione biometrica, nella proposta vietati solo per l'uso in *real time*, prevedendo una possibilità di utilizzo *ex post* solo per reati gravi e previa autorizzazione del giudice. Inoltre, l'uso del *software* di riconoscimento delle emozioni è vietato nei settori dell'applicazione della legge, della gestione delle frontiere, del lavoro e dell'istruzione. Inoltre, sulla base dello scandalo olandese degli assegni familiari, che ha visto migliaia di famiglie incriminate erroneamente per frode a causa di un algoritmo, il Parlamento ha esteso il divieto di controllo predittivo dai reati alle infrazioni di tipo amministrativo. Il Parlamento europeo ha, altresì, proposto di includere, tra i sistemi ad alto rischio, anche quelli che possono provocare danni alla salute, alla sicurezza o ai diritti fondamentali. Infine, secondo il Parlamento, sono considerati ad alto rischio anche i sistemi di raccomandazione delle piattaforme *online* di grandi dimensioni, come definiti dal *Digital services act*. Previsto, inoltre, un incremento delle tutele per l'utilizzo di dati sensibili con controlli più stretti su come i *provider* di sistemi ad alto rischio possono elaborarli. Il comunicato stampa è disponibile al seguente *link* https://www.europarl.europa.eu/news/it/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.

particolarmente, su diritti quali la *privacy* degli utenti *online* e i rischi connessi a possibili discriminazioni[58].

È, infatti, indiscutibile che l'Unione europea, in considerazione delle prospettive di sviluppo dell'intelligenza artificiale e, particolarmente, di quella generativa[59], si trovi a dover affrontare alcune sfide attuali e inevitabili in tema di tutela di diritti fondamentali.

5.1. *I diritti fondamentali in Europa: prima e dopo Lisbona*

Il principio di uguaglianza, della non discriminazione, della parità di trattamento, così come la tutela della *privacy*, rappresentano oggi tasselli fondamentali del moderno modello sociale europeo[60]. Ma non è sempre stato così. Lo sviluppo di un'anima solidaristica incentrata sui diritti fondamentali rappresenta una delle conquiste più faticose[61] rispetto all'originaria vocazione mercantilistica[62] che, per lunghi anni, ha connotato, quasi in via esclusiva, l'allora Comunità economica europea. Nell'immediato dopoguerra, infatti, lo scopo perseguito era eminentemente la creazione di uno spazio di libero scambio per incentivare la ripresa economica e non si riteneva che tale obiettivo potesse incidere, o avesse a che fare, con la protezione – o tantomeno la promozione – dei diritti fondamentali.

Nondimeno, la caduta dei totalitarismi, la fine della seconda guerra mondiale e gli orrori perpetrati in quegli anni drammatici

[58] Si rimanda ai capitoli IV e V del presente scritto.

[59] Si veda *infra* cap. IV, par. 7.

[60] R. CHERCHI, A. DEFFENU, *Le politiche comunitarie di lotta alla discriminazion*e, in *Rassegna di diritto pubblico europeo*, 1, 2004, p. 43 ss. e M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione europea,* in M. Cartabia (a cura di), *I diritti in azione*, Bologna, 2007, p. 15 ss.

[61] B. VENEZIANI, *Nel nome di Erasmo da Rotterdam. La faticosa marcia dei diritti sociali fondamentali nell'ordinamento comunitario*, in *Riv. Giur. Lav*., n. 1/2000 p. 779 ss.; N. PARISI, G. URSO, *I principi di eguaglianza e di non discriminazione nell'ordinamento dell'Unione europea,* in *Osservatorio sul rispetto dei diritti fondamentali in Europa,* 2011, n. 24, disponibile *online*.

[62] Secondo R. FOGLIA, *La politica sociale nell'ordinamento comunitario*, in A. Tizzano, *Il diritto privato dell'Unione europea*, Torino, 2000, II, p. 807, l'ordinamento comunitario fino al 2000 «ha privilegiato la componente mercantilistica del mercato interno rispetto alla componente sociale».

nei confronti dell'umanità intera, che hanno contributo a scrivere una delle pagine più buie della storia dell'uomo, hanno altresì dato inizio ad un inarrestabile processo di emersione e graduale riconoscimento dei diritti individuali e sociali[63] e di consacrazione all'interno dei testi costituzionali, molti dei quali hanno visto la luce proprio in quegli anni.

La matrice di tale processo può essere individuata nella positivizzazione[64] del principio di dignità umana descritto in dottrina come «fine cui tutte le libertà costituzionalmente protette dovrebbero tendere»[65] ma, in realtà, si potrebbe anche affermare, principio primo da cui tutti gli altri diritti individuali e sociali promanano.

V'è da dire che, in questo settore, l'opera interpretativa della Corte di giustizia ha rivestito, nel corso del tempo, un'importanza particolarmente rilevante. Già a partire dagli anni settanta, infatti, la Corte aveva riconosciuto la propria competenza ad assicurare l'osservanza dei diritti fondamentali "in quanto parte integrante dei principi generali del diritto"[66]. In seguito, la Corte aveva affermato che anche gli atti nazionali ricadenti nel campo del diritto della (al-

[63] Si veda in dottrina per un quadro dei passaggi evolutivi in tema di diritti sociali all'interno dell'Unione A. ADINOLFI, *Le innovazioni previste dal Trattato di Amsterdam in tema di politica sociale*, in *Il Diritto dell'Unione europea*, 1998, p. 563 ss.

[64] Per Peter Häberle la dignità umana è il primo degli elementi ideali e reali di cui si compone lo Stato costituzionale P. HÄBERLE, voce *Stato costituzionale I) Principi generali*, trad. it. di F. Politi, S. Rossi, in *Enc. giur. Trecc.*, Aggiornamento, Vol. IX, Roma, p. 1; ID., *I diritti fondamentali nelle società pluraliste e la Costituzione del pluralismo*, in M. Luciani (a cura di), *La democrazia alla fine del secolo*, Roma-Bari, 1994, p. 97, sostiene che «la premessa culturale e antropologica del modello dello «Stato costituzionale» va individuata nel valore della dignità dell'uomo; la conseguenza organizzativa di tale modello è costituita dalla democrazia pluralista».

[65] Si veda R. CONTI, *CEDU e Carta UE dei diritti fondamentali, tra contenuti affini e ambiti di applicazione divergenti, in I diritti fondamentali fra Carte e Costituzioni europee,* in *Scuola superiore della magistratura, Quaderno 11*, Roma, 2022, p. 49 ss.

[66] Causa 11-70 Sent. *Internationale Handelsgesellschaft,* 17 dicembre 1970, in Racc. *01125,* ECLI:EU:C:1970:114.

lora) Comunità europea dovessero essere conformi ai diritti fondamentali che lo stesso proteggeva in quanto principi generali[67].

Nondimeno, al fine di stabilire la sussistenza di una connessione fra i diritti fondamentali nazionali e quelli tutelati a livello comunitario, la Corte di Giustizia aveva anche affermato che essa era tenuta "ad ispirarsi alle tradizioni costituzionali comuni agli Stati Membri"[68]. Similmente, la Corte si era riferita ai "trattati internazionali per la tutela dei diritti umani a cui gli Stati Membri hanno collaborato o dei quali siano firmatari" in quanto costituenti una fonte di "linee guida"[69].

Un primo passo importante, nella direzione di una tutela specifica dei diritti fondamentali all'interno dell'Unione europea, è avvenuto con l'entrata in vigore del Trattato di Maastricht[70] e, seppure in misura minore, con il Trattato di Amsterdam.

Con l'istituzione dell'Unione Europea e la nota struttura a tre pilastri, infatti, è stata segnata una tappa importante verso l'integrazione politica e sociale europea. Tra le grandi innovazioni introdotte dal Trattato di Maastricht figura certamente l'istituzione della cittadinanza europea (articolo 20 TFUE), «quale simbolo dell'intensità dei vincoli tra gli Stati membri dell'Unione»[71]. Lo *status* di cittadino, che si aggiunge e non si sostituisce alla cittadinanza nazionale, conferisce una serie di diritti e prerogative che vanno nella direzione della valorizzazione dell'individuo all'interno del sistema dell'Unione.

Ma è certamente con l'entrata in vigore del Trattato di Lisbo-

[67] Causa C-60/84, Sent. *Cinéthèque*, § 26.

[68] Causa 4-73, Sent. *Nold*, cit., § 13.

[69] *Ibidem*.

[70] V. F. MOSCONI, *Il trattato di Maastricht: una costituzione per l'Europa?,* in *Il Politico*, Vol. 57, No. 3, luglio-settembre 1992, pp. 421-438.

[71] Si vedano G. GAJA, A. ADINOLFI, *Introduzione al diritto dell'Unione europea*, Bari, 2020, cap. I par. 3. La Corte di Giustizia nella pronuncia *Baumbast* Causa C-413/99, EU:C:2002:493, ha evidenziato che l'istituzione dello *status* di cittadino dell'Unione europea «è destinato ad essere lo *status* fondamentale dei cittadini degli Stati membri». Si veda altresì G. TESAURO, *Manuale di diritto dell'Unione europea*, a cura di De Pasquale P., Ferraro F., volume I, Napoli, 2021, spec. p. 448.

na[72], con cui si è inteso consolidare ulteriormente la partecipazione dei cittadini alla vita democratica dell'Unione, che dal punto di vista della tutela dei diritti fondamentali, le cose sono notevolmente cambiate.

Innanzitutto, come noto, la Carta di Nizza ha acquisito carattere giuridico vincolante[73] pari a quello dei Trattati[74], secondo quanto previsto dall'articolo 6, paragrafo 1, TUE[75].

Diversamente da quanto avveniva in passato, quindi, si può affermare che con il Trattato di Lisbona, la protezione e la promozione dei diritti fondamentali, tanto in una prospettiva interna quanto esterna, sono divenuti tra i principali obiettivi delle istituzioni europee.

[72] Si vedano per alcune considerazioni di ordine generale M. CONDINANZI, *Il "livello comunitario" di tutela dei diritti fondamentali dell'individuo*, in P. Bilancia, E. De Marco (a cura di), *La tutela multilivello dei diritti*, Milano, 2004, pp. 35-55; L. DANIELE, *La protezione dei diritti fondamentali nell'Unione europea dopo il trattato di Lisbona: un quadro d'insieme,* in *Il Diritto dell'Unione europea*, 4/2009, p. 640 ss., e, con specifico riguardo al ruolo dei principi generali di diritto dopo Lisbona, si rinvia a C. AMALFITANO, *Il diritto non scritto nell'accertamento dei diritti fondamentali dopo la riforma di Lisbona*, in *Il Diritto dell'Unione europea*, 1, 2016, p. 21 ss.

[73] Come noto la Carta fu proclamata prima a Nizza, in occasione del Consiglio europeo del 7 dicembre 2000, ma fino al 2009, conteneva esclusivamente un «solenne impegno assunto dalle istituzioni di conformare la loro azione al pieno rispetto dei diritti ivi enunciati», ma rimaneva priva di effetti giuridici vincolanti, così G. STROZZI, R. MASTROIANNI, *Diritto dell'Unione europea*, Torino, 2017, p. 256.

[74] La Carta ha quale principale obiettivo – come risulta dal suo preambolo – di riaffermare «i diritti derivanti, in particolare, dalle tradizioni costituzionali e dagli obblighi internazionali comuni agli Stati membri, dal Trattato sull'Unione europea e dai trattati comunitari, dalla (…) [CEDU], dalle carte sociali adottate dalla Comunità e dal Consiglio d'Europa, nonché i diritti riconosciuti dalla giurisprudenza della [Corte] e da quella della [Corte EDU]». Si veda, in tal senso, CGUE, *Parlamento c. Consiglio*, C-540/03, EU:C:2006:429, punto 38. L'art. 6 co. 1 del Trattato di Lisbona conferisce alla Carta di Nizza lo stesso valore giuridico dei Trattati istitutivi. Per ciò che attiene alla giurisprudenza della Corte di Giustizia si veda, CGUE, *Dereci e a.*, C-256/11*,* 15 novembre 2011, *in Racc.* I-11315; ID., *Gerardo Ruiz Zambrano c. Office national de l'emploi (ONEm)*, 8 marzo 2011, *8 marzo 2011*, *C-34/09*, in *Racc.* 2011, I-1177.

[75] Secondo cui «[l]'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati».

Oggi, tali diritti e principi costituiscono dei valori irrinunciabili[76] e capisaldi fondanti dell'ordinamento sovranazionale[77].

In questo senso depone anche il contenuto dell'articolo 51, paragrafo 1 della Carta di Nizza, secondo cui «le istituzioni e gli Stati membri devono rispettare i diritti, e devono osservare i principi[78] contenuti nella Carta promuovendone l'applicazione»[79].

V'è però da dire che nel dopo Lisbona, la Corte di giustizia è sempre stata molto attenta, nell'elaborare la propria giurisprudenza[80], ad escludere che l'articolo 51, paragrafo 1, della Carta potesse applicarsi agli Stati membri in ipotesi diverse da quelle che riguardino l'attuazione del diritto dell'Unione.

D'altronde, una simile giurisprudenza trova conforto tanto nel

[76] Commissione delle Comunità Europee, *Libro Verde. Uguaglianza e non discriminazione nell'Unione Europea allargata*, Bruxelles, 28.05.2004, COM(2004)379 def, p. 3.

[77] M. ROCCELLA, T. TREU, *Diritto del lavoro della Comunità Europea*, Padova, 2002, pp. 64 e 65.

[78] A tale riguardo è stato osservato che le diverse formule verbali sono espressione efficace della differente intensità del vincolo a cui gli Stati membri sono tenuti, in quanto la «soggezione dei destinatari della previsione rispetto ai diritti piuttosto che ai principi è indubbiamente segno di una concezione quasi programmatica del principio, contrapposta al carattere imperativo del diritto» così M. CONDINANZI, *Diritti, principi e principi generali nell'ordinamento giuridico dell'Unione europea*, in L. D'Andrea, G. Moschella, A. Ruggeri, A. Saitta, *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, Torino, 2016, p. 83.

[79] Per quanto riguarda i principi, occorre ricordare quanto dispone l'art. 52, par.5, secondo cui le disposizioni contenenti principi possono trovare attuazione attraverso provvedimenti normativi ed esecutivi europei o nazionali si veda il commento di F. FERRARO, N. LAZZERINI, *Articolo 52*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p.1061. Si vedano inoltre le considerazioni di C. AMALFITANO, *Principi e diritti nella Carta e principi generali: sovrapposizioni, interferenze e assimilazioni*, in *I diritti fondamentali fra Carte e Costituzioni europee*, *Scuola superiore della magistratura*, Quaderno 11, Roma, 2022, disponibile *online*, p. 31 ss.

[80] Si veda al riguardo Corte giust., C-617/10, 26 febbraio 2013, *Åkerberg Fransson*, punto 19 e giurisprudenza *ivi* citata e Corte di Giustizia, Sez.VII, 4 giugno 2020, n.C-32/20 – *Pres.Xuereb – Avv.gen.Kokott – TJ c.Balga Srl.*

ricordato articolo 6, paragrafo 1, TUE, quanto nel richiamato articolo 51, paragrafo 2 della Carta di Nizza. Entrambe le norme precisano che il carattere vincolante riconosciuto alla Carta di Nizza non ha comportato un'estensione delle competenze dell'Unione né una modifica delle stesse, rispetto a quanto già stabilito nei Trattati[81].

5.2. *Il rilievo della Convenzione europea per la salvaguardia dei diritti dell'uomo nell'ordinamento dell'Unione europea*

Notoriamente, la Carta di Nizza non è l'unica fonte che tutela i diritti fondamentali in ambito europeo. Ci si riferisce, chiaramente, alla Convenzione europea per la salvaguardia dei diritti dell'uomo (CEDU).

Come noto, la Convenzione si applica agli Stati aderenti al Consiglio d'Europa, fra cui si annoverano i Paesi membri dell'Unione, ma non anche direttamente l'Unione europea e le sue istituzioni, che lo sono solo sulla carta.

Il Trattato di Lisbona, infatti, a completamento del sistema di tutele dei diritti fondamentali in ambito sovranazionale e del processo di integrazione, ha previsto l'adesione dell'UE alla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[82] senza

[81] Corte giust., 6 marzo 2014, causa C-206/13, *Cruciano Siragusa;* ID., Grande Camera, 19 novembre 2019, cause riunite C585/18, C624/18 e C625/18, *A.K.*, 77, ID., 15 novembre 2011, C-256/11, *Dereci* e a., p. 71. Nello stesso senso la Dichiarazione n. 1, relativa alla Carta dei diritti fondamentali dell'Unione europea allegata all'atto finale della Conferenza intergovernativa all'esito della quale è stato adottato il Trattato di Lisbona ove si legge che «[l]a Carta non estende l'ambito di applicazione del diritto dell'Unione al di là delle competenze dell'Unione, né introduce competenze nuove o compiti nuovi per l'Unione, né modifica le competenze e i compiti definiti dai trattati» e anche il protocollo n. 8 relativo all'articolo 6, paragrafo 2 allegato al TUE prevede che l'accordo relativo all'adesione dell'Unione alla CEDU debba garantire "che siano preservate le caratteristiche specifiche dell'Unione e del diritto dell'Unione [omissis]". Si veda R. CONTI, *CEDU e Carta UE dei diritti fondamentali, tra contenuti affini e ambiti di applicazione divergenti*, in *I diritti fondamentali fra Carte e Costituzioni europee*, cit., p. 49 ss., spec. p. 55.

[82] Si veda per un'analisi sul tema M. PARODI*, L'adesione dell'Unione Europea alla Cedu*: *dinamiche sostanziali e prospettive formali*, Padova, 2020, p. 20 ss.

che tale adesione abbia però comportato un ampliamento delle competenze delle istituzioni europee[83].

L'articolo 6, paragrafo 2, TUE – che in qualche modo si pone quale conseguenza del ruolo riconosciuto alla CEDU dalla Corte di giustizia[84] – prevede, come è noto, l'adesione dell'Unione alla CEDU. Tale previsione, così come formulata, ha riacceso sulla questione un dibattito in dottrina solo apparentemente sopito[85].

[83] Il protocollo n. 8 relativo all'articolo 6, paragrafo 2 allegato al TUE prevede che l'accordo relativo all'adesione dell'Unione alla CEDU debba garantire "che siano preservate le caratteristiche specifiche dell'Unione e del diritto dell'Unione [omissis]".

[84] Si vedano, in particolare, le sentenze *ERT*, C-260/89, EU:C:1991:254, punto 41, nonché *Kadi e Al Barakaat International Foundation/Consiglio e Commissione*, C-402/05 P e C-415/05 P, EU:C:2008:461, punto 283.

[85] La dottrina sul tema è particolarmente copiosa. Senza alcuna pretesa di esaustività, si vedano: G. GAJA, *Opinion 2/94, in Common Market Law Review*, 1996, p. 973 ss.; ID., *Una mancata disconnessione relativamente alla Convenzione europea dei diritti dell'uomo?,* in *Rivista di diritto internazionale*, 2015, p. 148 ss.; G. TESAURO, *Bocciatura del progetto di accordo sull'adesione dell'Unione europea alla CEDU: nessuna sorpresa, nessun rammarico*, in *Foro Italiano*, 2015, 4, p. 77 ss.; L. S. ROSSI, *Il parere 2/94 sull'adesione della comunità europea alla Convenzione europea dei diritti dell'uomo*, in *Il diritto dell'Unione europea*, 1996, p. 839 ss.; ID., *Il Parere 2/13 della CGUE sull'adesione dell'UE alla CEDU: scontro fra Corti?,* 22 dicembre 2014, in *Sidi Blog*, disponibile on line; O. DE SHUTTER, Y. LEJEUNE, *L'adhésion de la Communauté à la Convention européenne des droits de l'homme à propos de l'avis 2/94 de la Cour de justice des Communautés*, in *Cahiers de doit euroéenne*, 1996, p. 555 ss; C. ZANGHÌ, *Un'altra critica al parere 2/94 della Corte sull'adesione della Comunità alla Convenzione europea dei diritti dell'uomo*, in *Scritti in onore di Giuseppe Federico Mancin*i, Milano, 1998, p. 1101 ss; A. BULTRINI, *La questione dell'adesione della Comunità europea alla Convenzione europea dei diritti dell'uomo di fronte alla Corte di giustizia*, in *Rivista di diritto internazionale privato e processuale*, 1997, p. 97 ss; D. FANCIULLO, *Parere 2/13 della Corte di giustizia dell'Unione europea: la novissima quaestio dell'adesione dell'Unione europea alla CEDU*, in *Federalismi, Focus Human Rights*, 3 aprile 2015, disponibile online; F. DONATI, *L'adesione dell'Unione europea alla CEDU alla luce del parere 2/13,* in *Rassegna Astrid*, 3/2016, disponibile online; S. DOUGLAS-SCOTT, *Opinion 2/13 on EU accession to the ECHR: a Christmas bombshell from the European Court of Justice,* in *UK Constitutional Law Association, disponibile online*; C. FAVILLI, *La Corte di giustizia rinvia a data da destinarsi l'adesione dell'UE alla CEDU*, in *Questione giustizia*, 2015, disponibile online; D. HALBER-

D'altronde, anche la questione dell'adesione al Protocollo n. 16[86], che prevede la possibilità per le giurisdizioni delle Alte Parti Contraenti di richiedere alla Corte EDU pareri consultivi su questioni di principio relative all'interpretazione o all'applicazione dei diritti e delle libertà definiti dalla Convenzione o dai suoi protocolli, ha sollevato diverse criticità.

STAM, *"It's the Autonomy, Stupid!" A modest defense of Opinion 2/13 on EU Accession to the ECHR, and the Way Forward*, in *German law journal*, 2015, Vol. 16, 1, p. 105 ss.; N. LAZZERINI, *"Questo matrimonio (così?) non s'ha da fare": il parere 2/13 della Corte di giustizia sull'adesione dell'Unione Europea alla Convenzione europea sui diritti dell'uomo*, in *Osservatorio sulle fonti*, disponibile online; S. VEZZANI, *"Gl'è tutto sbagliato, gl'è tutto da rifare!": la Corte di giustizia frena l'adesione dell'UE alla CEDU*, in *Sidi Blog*, disponibile online; T. LOCK, *Oops! We did it again – the CJEU's Opinion on EU Accession to the ECHR*, 18 dicembre 2014, disponibile online.

[86] Con specifico riferimento al meccanismo previsto dal Protocollo 16 si rimanda a E. LAMARQUE (a cura di), *La richiesta di pareri consultivi alla Corte di Strasburgo da parte delle più alte giurisdizioni nazionali: prime riflessioni in vista della ratifica del Protocollo 16 alla Convenzione europea dei diritti dell'uomo*, Milano, 2015, *p.* 91 ss.; T. VOLAND, B. SCHIEBEL, *Advisory Opinions of the European Court of Human Rights: Unbalancing the System of Human Rights Protection in Europe?*, in *Human Rights Law Review*, 2017, p. 73 ss.; P. DE SENA, *Caratteri e prospettive del Protocollo 16 nel prisma dell'esperienza del sistema interamericano di protezione dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2014, p. 593 ss.; L.-A. SICILIANOS, *L'élargissement de la compétence consultative de la Cour européenne des droits de l'homme – À propos du Protocole n° 16 à la Convention européenne des droits de l'homme*, in *Revue trimestrielle des droits de l'homme*, 2014, p. 9 ss.; G. ASTA, *Il Protocollo n. 16 alla CEDU: chiave di volta del sistema europeo di tutela dei diritti umani?*, in *La Comunità internazionale*, 2013, p. 773 ss.; R. CONTI, *La richiesta di "parere consultivo" alla Corte europea delle Alte Corti introdotto dal Protocollo n. 16 annesso alla CEDU e il rinvio pregiudiziale alla Corte di Giustizia UE. Prove d'orchestra per una nomofilachia europea*, in *Consulta Online*; E. NALIN, *I Protocolli n. 15 e 16 alla Convenzione europea dei diritti dell'uomo*, in *Studi sull'integrazione europea*, 2014, p. 117 ss. In particolare, sulla mancata ratifica italiana di tale protocollo, si veda D. VIGONI, *Entra in vigore (ma non per l'Italia) il Protocollo n. 16 alla CEDU che consente di richiedere alla Corte EDU un parere consultivo*, in *Processo Penale e Giustizia*, 2018, p. 6 ss. e sia consentito altresì di rinviare a C. GRIECO, *Il Protocollo n. 16 allegato alla CEDU e la funzione consultiva della Corte Europea dei Diritti dell'Uomo anche alla luce della futura e ancora incerta ratifica italiana*, in *Cuadernos de Derecho Transnacional*, 2022, vol. 14, n. 1, p. 313 ss.

Nel dopo Lisbona, il primo tentativo di dare attuazione al contenuto dell'articolo 6, paragrafo 2, TUE è stato posto in essere tra il 2010 e il 2013 dal cosiddetto gruppo *ad hoc* dei "47+1". Al termine di un complesso negoziato, il gruppo di esperti era giunto ad elaborare un progetto di accordo d'adesione[87] sottoposto, su richiesta della Commissione, *ex* articolo 218, paragrafo 11, TFUE, al vaglio della Corte di giustizia.

Con il discusso parere 2/2013[88], la Corte ha negato, in maniera decisa, che il progetto di accordo di adesione dell'Unione alla CEDU potesse considerarsi compatibile con i trattati istitutivi [89]. Que-

[87] Consiglio d'Europa, *Fifth negotiation meeting between the CDDH and ad hoc negotiation group and the European Commission on the accession of the European Union to the European Convention on Human Rights. Final Report to the CDDH*, (47+1(2013)008Rev2), Strasburgo, 13 giugno 2013.

[88] Corte di Giustizia (Seduta Plenaria), 18 dicembre 2014, Parere 2/13, *Adesione dell'Unione europea alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, ECLI:EU:C:2014:2454.

[89] La Corte, ribadendo l'impossibilità per la UE di aderire al sistema CEDU, al punto 154, chiarisce che tale adesione rimarrebbe caratterizzata da importanti particolarità e che, per effetto dell'adesione, la CEDU, al pari di qualsiasi altro accordo internazionale concluso dall'Unione, vincolerebbe, a norma dell'articolo 216, paragrafo 2, TFUE, le istituzioni dell'Unione e gli Stati membri e formerebbe dunque parte integrante del diritto dell'Unione (sul punto sentenza *Haegeman*, 181/73, EU:C:1974:41, punto 5; parere 1/91, EU:C:1991:490, punto 37; *sentenze IATA e ELFAA*, C-344/04, EU:C:2006:10, punto 36, nonché *Air Transport Association of America e a.*, C-366/10, EU:C:2011:864, punto 73). Inoltre, al punto 181, la Corte ha altresì evidenziato che aderendo alla CEDU, al pari di qualsiasi altra Parte contraente, l'Unione e le sue istituzioni – ivi compresa dunque la stessa Corte – sarebbero sottoposte ai meccanismi di controllo previsti dalla CEDU e – chiaramente – anche alla giurisdizione della Corte EDU. La Corte di giustizia, inoltre, invoca il principio di mutua fiducia tra gli Stati, sottolineando che tale adesione esigerebbe da uno Stato membro la verifica del rispetto dei diritti fondamentali da parte di un altro Stato membro, compromettendo così l'equilibrio sul quale l'Unione si fonda, nonché l'autonomia del diritto dell'Unione. Da ultimo, con riferimento al Protocollo n. 16 che autorizza le più alte giurisdizioni degli Stati membri a rivolgere alla Corte EDU domande di pareri consultivi in merito a questioni di principio relative all'interpretazione o all'applicazione dei diritti e delle libertà garantiti dalla CEDU o dai suoi protocolli, la Corte evidenzia ancora una volta un'incompatibilità non sanabile poiché il diritto dell'Unione esige che, a tale scopo, gli stessi giudici propongano

sto nuovo diniego, giunto nell'ambito del "secondo atto" di questa annosa vicenda[90], come evidenziato, ha riaperto con forza quello stesso dibattito sull'opportunità di procedere all'adesione che già il primo diniego, intervenuto all'inizio degli anni novanta, aveva originato. D'altronde, anche in questo caso, la Corte di giustizia è risultata molto puntuale nel contestare la compatibilità di gran parte delle previsioni contenute nel progetto di accordo con il diritto dell'Unione europea.

È indubbio che l'adesione alla CEDU avrebbe necessariamente comportato un controllo giurisdizionale aggiuntivo nel settore della tutela dei diritti fondamentali in ambito europeo, conferendo alla Corte europea dei diritti dell'uomo la competenza a controllare, ai fini del rispetto dei diritti sanciti nella Convenzione, anche l'operato delle istituzioni europee, non ultimo, quello della stessa Corte di giustizia. È proprio su quest'ultimo punto che l'*iter* ha subito un'importante battuta di arresto. In definitiva, ad oggi, continua a rimanere un'adesione programmatica, sebbene non ancora del tutto *"off the table"*[91].

la questione alla stessa Corte di giustizia mediante il meccanismo del rinvio pregiudiziale ai sensi dell'articolo 267 TFUE.

[90] Come si ricorderà, un primo no all'adesione era arrivato con il parere 2/94, *Adesione della Comunità europea alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, del 28 marzo 1996, ECLI:EU:C:1996:140. In quell'occasione la Corte di giustizia, ai punti 34 e 35, aveva ritenuto che "allo stato del diritto comunitario vigente a quell'epoca", la Comunità europea non era competente ad aderire alla CEDU. Infatti, tale adesione avrebbe determinato un mutamento sostanziale del regime comunitario esistente di tutela dei diritti dell'uomo, in quanto avrebbe comportato l'inserimento della Comunità in un sistema istituzionale internazionale distinto, nonché l'integrazione del complesso delle disposizioni di detta convenzione nell'ordinamento giuridico comunitario. Una siffatta modifica del regime della tutela dei diritti dell'uomo nella Comunità, le cui implicazioni istituzionali sarebbero risultate parimenti fondamentali, tanto per la Comunità quanto per gli Stati membri, avrebbe avuto portata costituzionale ed avrebbe quindi esorbitato, per sua propria natura, dai limiti dell'articolo 235 del Trattato CE (divenuto articolo 308 CE), disposizione oggi contenuta nell'articolo 352, paragrafo 1, TFUE, il che avrebbe potuto essere realizzato soltanto mediante una modifica del suddetto trattato.

[91] Il 22 giugno 2020 il gruppo *ad hoc* dei "47+1" si è incontrato per un primo *meeting* informale. In quella occasione la Commissione ha illustrato la posi-

Ne consegue che la Corte EDU non è competente a sindacare gli atti e le previsioni del diritto dell'Unione europea in rapporto alla CEDU. Per converso, essa è competente a pronunciarsi sugli atti degli Stati membri, inclusi quelli che danno attuazione agli obblighi discendenti dal diritto dell'Unione. Tuttavia, la Corte EDU riserva da sempre un regime speciale agli atti degli Stati Membri quando essi danno attuazione ad un obbligo discendente dal diritto europeo che non concede alcun margine di discrezionalità nell'implementazione. La Corte di Strasburgo non va a sindacare tali atti, dando come assunto che la tutela dei diritti fondamentali garantita nel sistema dell'Unione sia quantomeno equivalente a quella assicurata dalla CEDU[92].

Nonostante, dunque, l'adesione dell'UE alla CEDU non si sia ancora perfezionata, ciò non implica che la Convenzione non abbia alcuna rilevanza giuridica per il diritto dell'Unione europea, tutt'altro.

Al momento, la CEDU e la giurisprudenza della Corte di Strasburgo che la interpreta svolgono due funzioni. Innanzitutto, ai sensi dell'articolo 52 paragrafo 3[93] della Carta di Nizza, i diritti così come tutelati dalla Convenzione si pongono come *standard* minimi di tutela per la protezione dei diritti fondamentali, anche in ambito

zione dell'Unione sul tema dell'adesione. In seguito a questo incontro preliminare, il negoziato è ripreso in via ufficiale con il primo *meeting* formale, svoltosi tra il 29 settembre e il 1° ottobre 2020, con la partecipazione di circa novanta delegati, M. PARODI*, L'adesione dell'Unione Europea alla Cedu*: *dinamiche sostanziali e prospettive formali*, Padova, 2020. ID., *L'adesione dell'Unione europea alla CEDU: un "nuovo" inizio?*, in *Osservatorio sulle fonti*, 3/2020, disponibile online.

[92] Non si tratta di una presunzione assoluta, qualora infatti la tutela appaia manifestamente carente la Corte EDU, come evidenziato nel caso *Bosphorus* da cui la "presunzione *Bosphorus*", potrà intervenire cfr. Corte EDU, Sent. *Bosphorus Hava Jollari Turizm ve Ticaret c. Irlanda* del 30 giugno 2005, (ric. 45036/98).

[93] L'articolo 52, paragrafo 3, recita: «Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa». In dottrina, F. FERRARO, N. LAZZERINI, *Articolo 52*, cit., p. 1061 ss.

europeo[94]. A ciò si deve aggiungere che, in base a quanto dispone il paragrafo 1 dello stesso articolo, ogni limitazione dei diritti fondamentali deve essere prevista dalla legge, deve rispondere effettivamente a obiettivi di interesse generale riconosciuti dall'Unione e dovrà superare il vaglio dei criteri della necessità e della proporzionalità[95].

I diritti fondamentali fungono pertanto da parametri interpretativi[96]. Ciò implica che gli atti dell'Unione europea debbano essere

[94] A tale riguardo va solo precisato che la presunzione di equivalenza fra la tutela convenzionale e quella che discende dai diritti fondamentali di matrice sovranazionale presuppone che la Corte di giustizia abbia in concreto esaminato la vicenda escludendo la violazione – si veda Corte EDU, *Michaud c. Francia*, 6 dicembre 2012, parr.112/116 – a meno che il rinvio pregiudiziale non sia stato sollecitato in mancanza di dubbi interpretativi sul diritto UE – cfr. Corte EDU, *Avotins c. Lettonia*, 23 maggio 2016, § 109/116; ID., 20 settembre 2011, ric.nn.3989/07 e 38353/07, *Ullens de Schooten e Rezabek c. Belgio*; ID., 10 aprile 2012, *Vergauwen c. Belgio*, ric.n.4832/04; ID., 8 aprile 2014, *Dhahbi c. Italia,* ric.n.17120/09; ID., 21 luglio 2015, *Schipani c. Italia* – ric.n.38369/09; ID., 8 settembre 2015, *Wind telecomunicazioni spa c. Italia*; ID., 24 aprile 2018, *Ilkay Baydar c. Olanda*, ric.n.55385/14.

[95] Così si è espressa più volte anche la Corte di giustizia, si vedano, a titolo esemplificativo: Corte di giust., C-73/07, *Satakunnan Markkinapörssi e Satamedia*, 16 Dicembre 2008, par. 56; ID., Cause riunite C-92/09 e C-93/09; *Volker und Markus Schecke e Eifert GbR e Hartmut Eifert*, 9 novembre 2010, par. 77; ID., Cause riunite C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, par. 52; ID., C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 ottobre 2015, par. 92; e C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-es Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 dicembre 2015, parr. 69 e 80-82.

[96] Cfr*., ex multis*, Corte EDU (Grande Sezione) dell'8 aprile 2014, *Digital Rights Ireland Ltd*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238; CGUE, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 ottobre 2015, paragrafi 94-95; ID, *Khelili v. Switzerland*, No. 16188/07, 18 October 2011; ID, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008; ID, *K & T v. Finland*, No. 25702/94, 12 July 2001; ID, *Z v. Finland*, No. 22009/93, 25 February 1997; ID, *Huvig v. France*, No. 11105/84, 24 April 1990; ID, *Leander v. Sweden*, No. 9248/81, 26 March 1987.

[96] Corte EDU, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 dicembre 2008, par. 112.

letti in modo che sia garantito il rispetto dei diritti fondamentali tutelati dalla CEDU[97]. Qualora si prestino a più interpretazioni, si dovrà prediligere quella più idonea ad assicurare il rispetto e la salvaguardia dei diritti fondamentali all'interno dell'Unione europea[98].

6. Piano della successiva indagine

A partire dal quadro generale delineato in materia di diritti fondamentali, l'indagine che seguirà, nella seconda parte del presente lavoro, prenderà in esame specificamente le fonti che regolano il diritto alla *privacy* e il divieto di discriminazione all'interno dell'ordinamento dell'Unione europea. A seguire si analizzerà in quale rapporto questi diritti si pongono con la nuova proposta di regolamento in tema di intelligenza artificiale e come ne vengono interessati.

Come evidenziato nei paragrafi precedenti, i diritti potenzialmente interessati dallo sviluppo dell'intelligenza artificiale, con maggiore o minore intensità, sono pressocché tutti, dai diritti collettivi a quelli individuali. Tuttavia, la posizione in cui gli utenti *online* si trovano, dinanzi all'emergere di sistemi di intelligenza artificiale, appare particolarmente complessa e vulnerabile.

A motivo di ciò, nell'ambito della presente analisi, si è deciso di concentrarsi unicamente sulla tutela dei diritti individuali e, in par-

[97] Per esempio, nel Caso C-131/12 *Google Spain*, la Corte di Giustizia ha interpretato la Direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, alla luce degli Articoli 7 e 8 della Carta dell'UE, sul diritto al rispetto della vita privata e al diritto alla protezione dei dati di carattere personale. Benché la Direttiva non contenga alcuna previsione al riguardo, la Corte ha affermato che essa deve essere interpretata nel senso che riconosce un "diritto all'oblio": il diritto di una persona di ottenere, da parte del gestore del motore di ricerca, la rimozione delle informazioni che la concernono.

[98] Per esempio, nel Caso C-293/12 *Digital Rights Ireland*, la Corte di Giustizia ha dichiarato invalida la Direttiva 2006/24/CE sulla conservazione dei dati, in quanto le sue disposizioni non predisponevano sufficienti tutele per assicurare che i dati personali venissero trattati in modo conforme agli articoli 7 e 8 della Carta.

ticolare, su quelli che le applicazioni pratiche, che si esamineranno nei paragrafi a seguire, hanno dimostrato di porre maggiormente a rischio, ovvero *privacy* e non discriminazione. Nella specie, la prospettiva di analisi che si è scelto di adottare è proprio quella della tutela degli utenti *online* che, normalmente, si trovano in una posizione di debolezza e di incoscienza, quando si trovano ad interagire con le tecnologie digitali. Molto spesso, infatti, all'interno della rete, anche i servizi che vengono proposti come gratuiti, in realtà, richiedono indirettamente un prezzo da pagare. Generalmente, quel prezzo sono proprio i dati degli utenti, i gusti e le preferenze.

Eppure, nessuno vorrebbe rinunciare ai vantaggi che il digitale è in grado di garantire. Per questo è ragionevole supporre che si sia già arrivati ad un punto di non ritorno oltre il quale non è più ipotizzabile poter fare a meno dell'intelligenza artificiale. A motivo di ciò, e probabilmente a maggior ragione, l'attenzione per la tutela degli utenti *online*, particolarmente dinanzi allo strapotere dei colossi del digitale, deve essere mantenuta alta.

Questo è un momento storico fondamentale e, dal punto di vista normativo, rappresenta un punto di non ritorno.

PARTE II

I POSSIBILI IMPATTI NEGATIVI DEI SISTEMI DI INTELLIGENZA ARTIFICIALE SU PRIVACY E NON DISCRIMINAZIONE

CAPITOLO QUARTO

INTELLIGENZA ARTIFICIALE E PRIVACY

SOMMARIO. 1. Introduzione. – 2. Quadro normativo internazionale ed europeo in materia di protezione dei dati. – 3. Il coordinamento normativo e applicativo tra la proposta di Regolamento sull'intelligenza artificiale e il Regolamento europeo sulla protezione dei dati personali. – 4. I rischi legati all'applicazione cumulativa della proposta di Regolamento sull'intelligenza artificiale e il Regolamento europeo sulla protezione dei dati personali: i profili di interferenza: *a)* consenso; *b)* decisioni automatizzate e diritto alla spiegazione; *c)* titolare del trattamento e responsabilità. – 5. I c.d. "spazi di sperimentazione" per l'addestramento uomo-macchina come opportunità per garantire una migliore tutela della *privacy*. – 6. Intelligenza artificiale e tutela dei dati: il caso degli assistenti vocali casalinghi e la posizione del Garante italiano per la Protezione dei Dati Personali. – 7. Il caso ChatGPT.

1. Introduzione

Nel capitolo precedente, si è cercato di fornire un quadro normativo il più possibile esaustivo di quelle che sono state le iniziative intraprese dalle istituzioni europee in materia di intelligenza artificiale, nonché di delineare una cornice giuridica dei diritti fondamentali a livello internazionale ed europeo.

Tutti gli atti esaminati, per ciò che riguarda il settore dell'intelligenza artificiale, evidenziano una tensione dialettica tra opportunità e rischiosità. Se certamente benvenuti sono quei sistemi che migliorano l'efficientamento energetico o semplificano la produzione, meno lo sono quelli che utilizzano algoritmi per valutare il *credit scoring* o il rischio di recidiva in ambito penale[1]. Dalla proposta di regolamento, in particolare, si evince una volontà delle istituzioni europee di porre i diritti fondamentali al primo posto[2] e la necessità

[1] Si veda per appro *infra* cap. V.

[2] Cfr. A. ADINOLFI, *L'unione europea dinanzi allo sviluppo dell'intelligenza ar-*

di adottare ma, soprattutto, promuovere un modello di trasformazione sociale "antropocentrico" che rafforzi la dimensione umana dell'ecosistema digitale sul mercato unico.

La parola chiave resta "bilanciamento". Appare come non mai imperativo tracciare una linea netta, che divida ciò che deve considerarsi lecito da ciò che non lo è, preservando la libertà degli individui e garantendo, allo stesso tempo, la certezza del diritto e un quadro giuridico sufficientemente flessibile che risulti idoneo ad adattarsi ai veloci mutamenti che avvengono in ambito tecnologico. Un compito decisamente complesso.

Se evidenti sono le potenzialità dell'intelligenza artificiale, anche quale possibile mezzo per promuovere i diritti fondamentali ed aprire ampi spazi di *e-democracy*[3]*,* altrettanto palesi sono i rischi che l'utilizzo di questi strumenti possa amplificare la diffusione di violazioni di diritti e la messa in pericolo di principi ormai consolidati[4].

V'è da dire che sebbene la Commissione, con la proposta di regolamento sull'intelligenza artificiale, si sia orientata verso l'adozione di una disciplina orizzontale e uniforme, in un'ottica d'insieme, ciò che emerge è ancora un quadro assai frammentario poiché molti aspetti sono regolati in maniera parziale e da fonti diverse. Per ciò che attiene in particolare ai diritti fondamentali, la questione si complica ulteriormente vista la frammentarietà della tutela affidata a fonti di rango diverso. Norme sono rinvenibili, infatti, certamente nel diritto primario dell'Unione[5], nel diritto inter-

tificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali, in S. Dorigo (a cura di) *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., p. 14 ss.

[3] A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), in *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 1, *Diritti fondamentali, dati personali e regolazione*, p. 131 ss.

[4] Si veda E. LONGO, *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), in *Intelligenza artificiale e diritto: una rivoluzione?,* cit., p. 352.

[5] Si veda *supra* cap. II.

nazionale ma, settorialmente, anche all'interno di diverse fonti di diritto derivato che ne regolano particolari profili[6].

La Commissione, preso atto di tale stato di cose, ha evidenziato, da un lato, che appare necessaria una "risposta normativa specifica" all'intelligenza artificiale e, dall'altro, che gli interventi devono seguire un approccio proporzionato volto ad "evitare l'eccesso di regolamentazione".

In questo scenario e, primariamente per il settore dell'intelligenza artificiale, il governo dei dati costituisce un punto sostanziale su cui soffermarsi.

Per garantire il buon funzionamento del mercato unico digitale, infatti, i dati devono poter circolare liberamente all'interno dell'Unione ma, allo stesso tempo, devono essere messi in sicurezza e ne deve essere garantita la riservatezza e la protezione.

In un simile contesto, i dati personali occupano un posto privilegiato, giacché forniscono all'algoritmo la possibilità di mettersi in contatto e di interagire con la realtà circostante, di analizzare le abitudini di vita e le preferenze dei soggetti a cui tali dati appartengono[7].

Sulla base dei dati personali acquisiti, spesso in forma aggregata, gli algoritmi elaborano predizioni e assumono decisioni che, inevitabilmente, avranno ripercussioni anche sulla vita dei singoli. A motivo di ciò, la sfera di protezione dei dati personali rischia di risultare seriamente minacciata da un'intelligenza artificiale eccessivamente pervasiva e non sottoposta ad adeguati controlli e limiti[8].

Il rischio che si corre è che l'essere umano, seppur non voluta-

[6] A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, cit., p. 141.

[7] Anche i dati non personali rivestono un'importanza rilevante nel caso degli algoritmi si veda per un commento G.M. RUOTOLO, *I dati non personali: l'emersione dei* big data *nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, p. 97 ss.

[8] S. MARANELLA, *La protezione dei dati personali contro un uso distopico dell'AI*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale, Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, p. 51.

mente, diventi parte del meccanismo[9] e venga trattato come un semplice strumento nel funzionamento dei sistemi informatici[10]. In particolare, ciò che preoccupa, e che purtroppo in parte sta già avvenendo, è che si verifichi "un uso umano degli esseri umani", cioè che gli esseri umani vengano trattati alla stregua di "mezzi di produzione digitale" o di meri clienti da influenzare[11].

Occorre anche considerare, come peraltro evidenziato dallo stesso Parlamento europeo all'interno della Risoluzione sui *Big Data*[12], che i dati processati mediante algoritmi sono spesso utilizzati per individuare determinate correlazioni, tendenze e modelli e che i progressi delle tecnologie di comunicazione, l'uso massiccio dei *social media* e di dispositivi che comunicano informazioni senza intervento umano, hanno portato allo sviluppo di enormi insiemi di dati in costante crescita che tracciano un quadro senza precedenti del comportamento umano, della vita privata e della società.

Ancora il Parlamento europeo, all'interno della stessa Risoluzione, questa volta richiamando la Carta di Nizza e il GDPR, evidenzia che il moltiplicarsi dei trattamenti e dell'analisi di grandi insiemi di dati personali (e non personali) provenienti da una serie di fonti diverse e l'elevato numero di soggetti coinvolti, seppur generando opportunità significative, hanno anche creato una grande incertezza per i cittadini e per gli operatori economici, che faticano ad avere un quadro chiaro di quali siano i requisiti specifici da rispettare per garantire la conformità dei propri sistemi alla vigente legislazione europea in materia. Inoltre, il Parlamento auspica che venga favorita una maggiore cooperazione e coerenza tra le varie autorità di regolamentazione e di vigilanza della concorrenza, di tu-

[9] L. FLORIDI, *Etica dell'intelligenza artificiale, Sviluppi, opportunità, sfide*, cit., p. 59.

[10] E. KANT, *Critica della ragion pratica*, trad. Francesco Capra, Bari, 1909; revisione della traduzione di Eugenio Garin (basata sull'edizione dell'Accademia di Prussia), Glossario e Indice a cura di Vittorio Mathieu, Bari, 1971; Introduzione di Sergio Landucci, Bari, 1997.

[11] N. WIENER, *The Human Use of Human Beings: Cybernetics and Society*, Boston, 1954, p. 45 ss.

[12] Risoluzione del Parlamento europeo C 263/82, *Implicazioni dei Big Data in termini di diritti fondamentali,* cit.*,* considerando A e C.

tela dei consumatori e di protezione dei dati a livello nazionale e dell'Unione, al fine di garantire un approccio coerente alle implicazioni dei *Big Data* per i diritti fondamentali e la loro corretta comprensione[13].

Alla luce di quanto sin qui evidenziato, appare evidente che per poter trarre appieno beneficio dalle prospettive e dalle opportunità offerte dai sistemi di intelligenza artificiale e, appunto, dai *Big Data*, è necessario che la fiducia pubblica in tali tecnologie sia garantita da un rigoroso rispetto dei diritti fondamentali, dalla conformità alla vigente legislazione dell'Unione, nonché dalla certezza giuridica per tutti i soggetti coinvolti.

Occorre, in particolare, aumentare la consapevolezza per comprendere che l'analisi predittiva, basata sui *Big Data,* è in grado di offrire solo una probabilità statistica e, pertanto, non potrà mai anticipare, con precisione, il comportamento individuale.

Il legislatore europeo si trova a dover affrontare una sfida – al contempo scomoda e complessa – che richiede uno sforzo importante per comporre esigenze che appaiono, almeno ad una primissima analisi, contrastanti. Da un lato, assicurare la circolazione e la valorizzazione, anche economica, dei dati personali come nutrimento dei sistemi di intelligenza artificiale e, dall'altro, proteggere il di-

[13] Il PE auspica altresì che venga promossa l'istituzione di una struttura di coordinamento digitale (*Digital Clearing House*), in dottrina si veda E. CIRONE, *Big Data e tutela dei diritti fondamentali*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., p. 143 ss. Inoltre nella risoluzione del Parlamento europeo, 20 ottobre 2020, recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)), cit., si legge: «il quadro giuridico dell'Unione dovrebbe applicarsi all'intelligenza artificiale, alla robotica e alle tecnologie correlate, inclusi i *software* e algoritmi e i dati utilizzati o prodotti da tali tecnologie; prende atto che le opportunità basate sull'intelligenza artificiale, la robotica e le tecnologie correlate si basano sui *Big Data* e che è necessaria una massa critica di dati per addestrare gli algoritmi e perfezionare i risultati; si compiace, a tale proposito, della proposta della Commissione di creare uno spazio comune dei dati nell'unione per rafforzare lo scambio di dati e sostenere la ricerca nel pieno rispetto delle norme europee in materia di protezione dei dati».

ritto alla *privacy* degli individui, sempre più minacciato negli ambienti digitali[14].

2. Quadro normativo internazionale ed europeo in materia di protezione dei dati

La normativa in tema di tutela dei dati è piuttosto eterogenea e multilivello.

Sebbene nel corso della presente analisi ci si soffermerà particolarmente sui profili di interferenza e di coordinamento tra il regolamento europeo sulla protezione dei dati personali e la proposta di regolamento sull'intelligenza artificiale, appare comunque opportuno fornire una cornice giuridica, dell'attuale quadro normativo, internazionale ed europeo, in tema di tutela dei dati[15].

Nell'ordinamento delle Nazioni Unite manca un riconoscimento testuale alla *privacy* come diritto fondamentale. Nondimeno, tale tutela viene ricompresa in quella assicurata nell'ambito del rispetto della vita privata. Tale ultimo diritto, disciplinato dall'articolo 12[16] della Dichiarazione universale dei diritti dell'uomo (UDHR)[17], al contrario, riceve riconoscimento esplicito tra i diritti umani protetti.

A partire dal 2013, le Nazioni Unite, presa consapevolezza della necessità di "modernizzare" ed adeguare il concetto di rispetto di vita privata e di *privacy*, alla luce della rivoluzione tecnologica in atto e degli scandali legati alle rivelazioni sulle pratiche di sorveglian-

[14] Si veda G. FINOCCHIARO, *Considerazioni su intelligenza artificiale e protezione dei dati personali,* in U. Ruffolo (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, cit., p. 332.

[15] Si veda FRA, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, 2018, spec. p. 20 ss.

[16] Secondo cui: nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni.

[17] Dichiarazione universale dei diritti umani, approvata dall'Assemblea Generale delle Nazioni Unite a Parigi il 10 dicembre del 1948.

za di massa attuate da alcuni Stati[18], hanno adottato una serie di risoluzioni[19]. L'intento di tali atti, non giuridicamente vincolanti, era proprio quella di condannare tali pratiche ed evidenziare l'impatto che potrebbero avere sulla tutela della *privacy*, della vita privata, sulla libertà di espressione nonché sullo stesso buon funzionamento di una società democratica[20].

Il tema è divenuto di tale importanza che anche l'Alto Commissariato per i diritti umani (OHCHR) ha iniziato ad interessarsene[21] e,

[18] Ci si riferisce in particolare al noto caso Snowden o *Datagate* che nel 2013 portò alla luce una serie di rivelazioni sulle attività di sorveglianza di massa compiute dall'agenzia statunitense Nsa e dal governo britannico nei confronti dei cittadini statunitensi e stranieri. Il caso si è aperto in seguito alla pubblicazione di alcuni documenti riservati diffusi da Edward Snowden, un *ex* consulente dell'Nsa, entrato in possesso dei *files* mentre lavorava per una società, la Booz Allen Hamilton, che collabora con il dipartimento della difesa e i servizi di *intelligence* degli Stati Uniti. The Guardian, *NSA collecting phone records of millions of Verizon customers daily*, disponibile online.

[19] Le prime due risoluzioni, rispettivamente del 2013 e del 2014, pongono particolarmente l'accento sugli effetti negativi della sorveglianza di massa: ONU, ASSEMBLEA GENERALE, *Resolution on the right to privacy in the digital age*, A/RES/68/167, New York, 18 dicembre 2013; e ID., *Revised draft resolution on the right to privacy in the digital age*, A/C.3/69/L.26/Rev.1, New York, 19 novembre 2014. Le successive due risoluzioni, del 2016 e del 2017, riaffermano la necessità di limitare i poteri delle agenzie di *intelligence* e di condannare le pratiche di sorveglianza di massa ma evidenziano altresì che le crescenti capacità delle imprese di raccogliere, trattare e utilizzare dati personali possono rappresentare un rischio per il godimento del diritto alla vita privata nell'era digitale, ONU, ASSEMBLEA GENERALE, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/71/L.39/Rev.1, New York, 16 novembre 2016; ONU, CONSIGLIO PER I DIRITTI UMANI, *The right to privacy in the digital age,* A/HRC/34/L.7/Rev.1, 22 marzo 2017.

[20] Con tali risoluzioni è stato altresì istituito un relatore speciale sul diritto alla vita privata, con il mandato di promuovere e tutelare tale diritto.

[21] Sono stati pubblicati una serie di *report* sul tema: OHCHR, *The right to privacy in the digital age,* 2018, HRC/39/29; ID., *The impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, 2020, A/HRC/44/24; ID., *The right to privacy in the digital age*, 2021, A/HRC/48/31; ID., *The right to privacy in the digital age*, 2022, A/HRC/51/17, tutti i documenti sono consultabili sul sito dell'Alto Commissariato.

proprio con riferimento alle tecnologie di intelligenza artificiale, ha evidenziato che: «digital technologies do not exist in a vacuum. They can be a powerful tool for advancing human progress and contribute greatly to the promotion and protection of human rights. However, data-intensive technologies, such as artificial intelligence applications, contribute to creating a digital environment in which both States and business enterprises are increasingly able to track, analyze, predict and even manipulate people's behavior to an unprecedented degree. These technological developments carry very significant risks for human dignity, autonomy and privacy and the exercise of human rights in general, if applied without effective safeguards»[22]

Per ciò che riguarda il versante europeo, poco dopo l'adozione della UDHR, sono cominciati i primi riconoscimenti di un diritto alla tutela dei dati.

All'interno della Convenzione europea dei diritti dell'uomo, così come avvenuto in seno alle Nazioni Unite, la tutela dei dati personali viene ricompresa nell'ambito del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza disciplinato dall'articolo 8[23] della CEDU e ciò nonostante il diritto alla protezione dei dati personali abbia una portata più ampia rispetto a quello della vita privata. Invero, la protezione dei dati coinvolge tutti i trattamenti, indipendentemente dal fatto che abbiano o meno un rapporto o un impatto sulla vita privata e familiare. Peraltro, l'avvento di *Internet* e delle nuove tecnologie ha portato alla definizione di un nuovo concetto di vita privata, spesso definito come diritto all'«autodeterminazione informativa»[24], e ha fatto emergere un

[22] Così si legge sul sito dell'Alto Commissariato per i diritti umani che ha avviato altresì una consultazione pubblica *Call for inputs*: *The relationship between human rights and technical standard-setting processes for new and emerging digital technologies (2023) - Report of the High Commissioner for Human Rights*.

[23] Tale norma statuisce che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

[24] Ad esempio la Corte costituzionale federale tedesca ha affermato un diritto all'autodeterminazione informativa in una sentenza del 1983, *Volkszählungsurteil, BVerfGE* Vol. 65, p. 1 ss. chiarendo che l'autodeterminazione informativa sorge dal diritto fondamentale al rispetto della personalità, protetto dalla costituzione

crescente bisogno di norme più dettagliate per regolamentare la tutela dei dati personali degli individui, anche in contesti digitalizzati.

A motivo di ciò, intorno alla metà degli anni '70, il Comitato dei Ministri del Consiglio d'Europa ha adottato varie risoluzioni in materia di protezione dei dati personali, proprio facendo riferimento all'articolo 8 della CEDU[25].

Più tardi, nel 1981, è stata aperta alla firma la Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale[26] che rappresenta un *unicum* poiché era, e rimane, l'unico strumento internazionale giuridicamente vincolante[27] in materia di tutela dei dati personali[28].

tedesca. Anche la Corte EDU, nella sentenza *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, n. 931/13, 27 giugno 2017, punto 137, ha riconosciuto che l'articolo 8 della CEDU «prevede il diritto ad una forma di autodeterminazione informativa».

[25] Consiglio d'Europa, Comitato dei Ministri (1973), Risoluzione (73) 22 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore privato, 26 settembre 1973; Consiglio d'Europa, Comitato dei Ministri (1974), Risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico, 20 settembre 1974.

[26] Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Consiglio d'Europa, STCE n. 108, 1981.

[27] La Convenzione n. 108 è vincolante per gli Stati che l'hanno ratificata ma è aperta all'adesione anche al di fuori del sistema del Consiglio d'Europa. Ad oggi conta 55 parti contraenti, ovvero gli Stati membri del Consiglio d'Europa, oltre a Uruguay, Tunisia, Senegal, Marocco, Messico, Mauritius, Capo Verde, Burkina Faso e Argentina. La Convenzione n. 108 non è soggetta al controllo giudiziario della Corte EDU, ma è stata tenuta in considerazione nella giurisprudenza della Corte, nel quadro dell'articolo 8 della CEDU. Nel corso degli anni, la Corte ha stabilito che la protezione dei dati personali è una parte importante del diritto al rispetto della vita privata (articolo 8), e ha fatto riferimento ai principi sanciti dalla Convenzione n. 108 per determinare se vi sia stata o meno un'ingerenza in questo diritto fondamentale, si veda in tal senso, Corte EDU, *Z c. Finlandia*, n. 22009/93, 25 febbraio 1997.

[28] Peraltro lo strumento, pur mantenendo fermi gli obiettivi principali perseguiti, è stato oggetto di un processo di ammodernamento. Si legge sul sito del Comitato che: «the modernisation of Convention 108 pursued two main objectives: to deal with challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implemen-

Quanto all'ambito di applicazione *ratione materiae*, la Convenzione n. 108 si applica a tutti i trattamenti di dati personali, sia nel settore privato sia in quello pubblico, compresi quelli effettuati da autorità giudiziarie e di polizia. La finalità perseguita nel testo convenzionale è quella di proteggere gli individui dagli abusi che possono accompagnare i trattamenti e di regolamentare i flussi transfrontalieri di dati personali. La Convenzione introduce, inoltre, una serie di principi che riguardano, in particolare, la correttezza e la liceità della raccolta e il trattamento per scopi legittimi. Sono stati introdotti, inoltre, regole per ciò che riguarda la durata del trattamento, la qualità, l'adeguatezza, la pertinenza, la non eccessività (proporzionalità) nonché l'esattezza dei dati. La Convenzione, inoltre, in assenza di adeguate garanzie giuridiche, vieta il trattamento dei dati «sensibili», come la razza, le opinioni politiche, la salute, la religione, l'orientamento sessuale o il casellario giudiziale.

Vengono poi previsti una serie di diritti a tutela degli individui, molti dei quali, oggi, si ritrovano all'interno del GDPR: ovvero essere informati della conservazione di informazioni che li riguardano e di chiederne l'eventuale rettifica.

Possibili restrizioni possono essere imposte solo se in gioco ci sono interessi superiori, quali la sicurezza o la difesa dello Stato. Inoltre, la Convenzione ha previsto la libera circolazione dei dati personali tra le parti contraenti, imponendo alcune limitazioni su tali flussi verso Paesi in cui la regolamentazione giuridica non conferisce una protezione equivalente.

Tutti gli Stati membri dell'Unione hanno ratificato la Convenzione n. 108, che è stata altresì soggetta a modifica per poter consentire l'adesione anche da parte della stessa Unione.[29]

tation». Cfr. in dottrina S. KIERKEGAARD, N. WATERS, G. GREENLEAF, L. A. BYGRAVE, I. LLOYD, S. SAXBY, *30 years on – The review of the Council of Europe Data Protection Convention 108, Computer Law & Security Review*, Vol. 27, n. 3, 2011, pp. 223-231.

[29] Articolo 23, paragrafo 2, della Convenzione n. 108, Consiglio d'Europa, emendamenti alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n.°108) che consente alle Comunità europee di accedervi, adottati dal Comitato dei Ministri, a Strasburgo, il 15 giugno 1999.

Per ciò che riguarda specificamente il diritto europeo, con l'adozione del Trattato di Lisbona[30] e la modifica dello *status* giuridico della Carta di Nizza a livello di diritto primario, anche la tutela dei dati ha subito un mutamento di prospettiva[31].

Innanzitutto, è stato inserito un riferimento esplicito alla protezione dei dati personali all'interno dell'articolo 16 TFUE[32], collocato, come noto, all'interno della sezione dedicata ai principi generali dell'ordinamento sovranazionale. Peraltro, questa norma assume un'importanza duplice poiché, oltre a prevedere una tutela diretta della *privacy* a livello di diritto primario, ha creato una nuova base giuridica, conferendo all'Unione la competenza a legiferare in materia[33]. Questo cambiamento ha portato all'adozione, nel 2016[34], del più volte menzionato regolamento generale sulla protezione dei dati e della direttiva sulla protezione dei dati in ambito penale[35].

[30] Per una disamina completa delle novità apportate dal Trattato di Lisbona, si vedano G. GAJA, A. ADINOLFI, *Introduzione al diritto dell'Unione europea*, cit., spec. cap. I par. 1 e cap. VI par. 3; TESAURO G., *Manuale di diritto dell'Unione europea*, cit., spec. p. 15 ss. e p. 123 ss.

[31] G. GONZÁLEZ FUSTER, G. GELLERT, *The fundamental right of data protection in the European Union: in search of an uncharted right*, in *International Review of Law, Computers and Technology*, Vol. 26, 1, 2012, pp. 73-82 e anche O. LYNSKEY, *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order*, in *International and Comparative Law Quarterly,* 2014, Vol. 63, n. 3, pp. 569-597.

[32] H. HIJMANS, *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Brussels, 2016, p. 4 ss. e spec. p. 32 ss.

[33] Si tratta di uno sviluppo particolarmente rilevante posto che, inizialmente, la legislazione dell'UE in materia di protezione dei dati, ovvero la Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (direttiva sulla tutela dei dati), GU L 281 del 1995 (in vigore fino al maggio 2018), era stata adottata sulla base giuridica del mercato interno e sulla necessità di ravvicinare le legislazioni nazionali per non ostacolare la libera circolazione dei dati nell'UE.

[34] Regolamento (UE) n. 2016/679 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), GU L 119 del 2016.

[35] Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini

Prima dell'adozione del regolamento, infatti, a livello di normazione secondaria, il principale strumento giuridico in materia di protezione dei dati era la direttiva 95/46/CE[36], adottata in un momento in cui diversi Stati membri avevano già previsto, a livello interno, delle normative di settore[37] e si poneva, pertanto, un'esigenza di armonizzazione per consentire il libero flusso dei dati all'interno dell'Unione. I contenuti della direttiva, seppur ampliati, erano visibilmente ispirati a quelli della ricordata Convenzione n. 108.

Nondimeno, sebbene già con la direttiva 95/46 si fosse raggiunto un discreto livello di protezione per gli individui, non altrettanto poteva dirsi per ciò che riguardava l'uniformità normativa intereuropea. Il margine di discrezionalità lasciato agli Stati dallo strumento normativo nel recepimento della stessa, infatti, aveva generato difformità applicative, in certi casi anche marcate. A motivo di ciò, si è arrivati all'adozione del regolamento 679/2016 sulla protezione dei dati[38], prediligendo, questa volta, uno strumento avente portata generale e di immediata applicabilità in tutti gli Stati membri.

Si tratta di un testo articolato e complesso, il cui esame specifico, al di là delle disposizioni che si esamineranno per valutare i possibili profili di interferenza con la proposta di regolamento in materia di intelligenza artificiale, esula dalla presente analisi.

Basti dire che il GDPR si pone in una linea di continuità con la

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 (protezione dei dati in materia di autorità di polizia e giudiziarie), GU L 119 del 2016.

[36] V. S. SIMITIS, *Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?,* in *Neue Juristische Wochenschrift*, 1997, n. 5, pp. 281-288.

[37] Il *Land* tedesco dell'Assia ha adottato la prima legge al mondo sulla protezione dei dati nel 1970, la quale era applicabile solo in tale Stato. La Svezia ha adottato il *Datalagen* nel 1973; la Germania ha adottato il *Bundesdatenschutzgestez* nel 1976; e la Francia ha adottato la *Loi relative à l'informatique, aux fichiers et aux libertés* nel 1977. Nel Regno Unito, il *Data Protection Act* è stato adottato nel 1984. Infine, i Paesi Bassi hanno adottato la *Wet Persoonregistraties* nel 1989.

[38] V. per un commento sul passaggio dalla direttiva al regolamento, *ex multis*, P. DE HERT, V. PAPAKONSTANTINOU, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, in *Computer Law & Security Review*, 2012, Vol. 28, n. 2, pp. 130-142.

precedente direttiva, preserva e sviluppa i principi e i diritti fondamentali conferiti all'interessato, impone nuovi obblighi che richiedono alle organizzazioni di attuare la protezione dei dati fin dalla progettazione e la protezione dei dati per impostazione predefinita, introducendo i ben noti concetti di *privacy by design* e *privacy by default* che, peraltro, sono ripresi dalla stessa Commissione nella proposta di regolamento sull'intelligenza artificiale.

Trattandosi di un regolamento, le istituzioni europee sono riuscite ad ottenere l'auspicata uniformità normativa e applicativa all'interno dell'Unione, eccezion fatta per taluni aspetti secondari, lasciati alla scelta dei singoli ordinamenti nazionali.

Da ultimo, occorre analizzare quanto dispone, in materia di tutela dei dati, la Carta di Nizza.

Nella specie, l'articolo 8, che ha esplicitamente innalzato il rango della tutela della *privacy* a quello di un diritto fondamentale nell'ambito del diritto dell'Unione, non solo disciplina espressamente il diritto alla protezione dei dati personali, ma enuncia, altresì, una serie di principi collegati a tale diritto. La norma stabilisce, in particolare, che il trattamento dei dati personali debba avvenire secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o su un fondamento legittimo previsto dalla legge. Si prevede, inoltre, che gli individui abbiano il diritto di accedere ai propri dati personali e di ottenerne la rettifica e che il rispetto di tali diritti sia monitorato da un'autorità indipendente.

Ciò posto, delineato il quadro normativo in tema di tutela dei dati da un punto di vista internazionale ed europeo, appare ora opportuno soffermarsi sui possibili profili di interferenza che emergono tra il regolamento 679/2016 sulla protezione dei dati personali e la proposta di regolamento in tema di intelligenza artificiale, posto che molti dei dati processati dai sistemi di intelligenza artificiale sono qualificabili come personali e, pertanto, il GDPR costituisce "l'argine normativo" fondamentale nei confronti di queste nuove tecnologie[39].

[39] V. *infra* paragrafi 3 e 4.

3. Il coordinamento normativo e applicativo tra la proposta di Regolamento sull'intelligenza artificiale e il Regolamento europeo sulla protezione dei dati personali

Seppur con i dovuti distinguo, nell'era dell'intelligenza artificiale, la tutela della circolazione del dato acquisisce un ruolo essenziale al pari della tutela del dato stesso e la trasformazione digitale sembra aver in qualche modo alterato il senso stesso e i confini della tutela della *privacy*, collocandola all'interno di nuovi paradigmi popolati da soggetti, necessità e meccanismi di azione del tutto nuovi[40].

Occorre dunque capire se, in questo scenario, l'impostazione adottata dal GDPR[41] e la logica del consenso[42], basata su un elemento volontaristico, risultino effettivamente adeguate e sufficientemente protettive per gli utilizzatori.

L'imporsi rapido e su larga scala sui mercati internazionali di tecnologie di intelligenza artificiale, a distanza relativamente breve da quella che è stata definita come una "riforma epocale della disciplina sulla protezione dei dati personali", può essere dunque pensato come uno *"stress test"* della tenuta stessa del quadro normativo europeo in materia di *privacy*.

Il rapporto tra dati e sistemi di intelligenza artificiale è molto stretto. Si tratta, a ben vedere, di un rapporto necessario e di tipo strumentale[43]. Più ampia è la massa di dati che i sistemi di intelli-

[40] Così M. BASSINI, O. POLLICINO, *Intelligenza artificiale e protezione dei dati personali*, in A. Pajno, F. Donati, A. Perrucci (a cura di), in *Intelligenza artificiale e diritto: una rivoluzione?*, cit., p. 269.

[41] M. FUMAGALLI MERAVIGLIA, *Le nuove normative europee sulla protezione dei dati personali,* in *Diritto comunitario e degli scambi internazionali*, 2016, p. 12; C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Napoli, 2018, p. 25 ss.

[42] Si veda per alcune riflessioni critiche L. CURREN, J. KAYE, *Revoking consent: a "blind spot" in data protection law?,* in *Computer Law & Security Review*, 2010, Vol. 26, n. 3, pp. 273-283.

[43] Si veda A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali*, cit., p. 329.

genza artificiale possono elaborare, più accurate saranno le risultanze delle elaborazioni. Dalla prospettiva inversa, tuttavia, maggiore sarà la quantità di dati di cui potrà disporre l'algoritmo, più intenso sarà il sacrificio richiesto all'utilizzatore in termini di cessione di dati a cui conseguirà, necessariamente, una compressione della propria sfera della *privacy*.

Nonostante una correlazione così stretta, le fasi della raccolta e del trattamento dei dati non trovano spazio all'interno dalla proposta di regolamento sull'intelligenza artificiale. Ne consegue che la disciplina debba necessariamente essere rinvenuta altrove e, in particolare, all'interno del GDPR[44]. Tale considerazione porta con sé un'ulteriore naturale conseguenza, i due atti devono coordinarsi in modo appropriato per scongiurare il rischio di vuoti normativi o di contrasti tra norme che vadano a minare il diritto alla *privacy*[45].

I profili di somiglianza – *rectius* di interferenza – tra GDPR e proposta di regolamento sull'intelligenza artificiale sono molteplici. A tale riguardo non può sottacersi che il legislatore europeo, evidentemente considerando il GDPR un esperimento particolarmente riuscito, ha riproposto, come ricordato, all'interno della proposta di regolamento sull'intelligenza artificiale, molti dei contenuti già noti, non ultimo il principio di *accountability* e il concetto di *by design*. Entrambi gli atti prevedono restrizioni per gli operatori economici non europei nella circolazione dei loro beni e servizi all'interno dell'Unione; in ambedue gli atti è previsto che le regole si applichino indipendentemente dal fatto che gli operatori economici interessati siano stabiliti all'interno dell'Unione europea; anche nella proposta di regolamento sull'intelligenza artificiale viene riproposto l'approccio basato sul rischio già sperimentato con il GDPR; in entrambi gli atti sono previsti sistemi di controllo per monitorare le autorità deputate a certificare il rispetto delle regole

[44] Si veda G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale la protezione dei dati personali*, cit., p. 217.

[45] In dottrina si vedano sul punto O. POLLICINO, M. BASSINI, *Art. 8*, *Protezione dei dati personali*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 134 ss.; S. CALZOLAIO, *Protezione dei dati personali*, in *Digesto delle Discipline Pubblicistiche, Aggiornamento*, Torino, 2017, p. 594 ss.

ma anche a supervisionare e controllare il mercato; inoltre, in ambedue gli strumenti, il regime sanzionatorio in caso di infrazioni è molto gravoso in termini economici per gli operatori.

Nonostante i molteplici profili di somiglianza, il rischio di mancato coordinamento tra i due strumenti è più alto di quanto possa apparire ad un primo esame. Resta, infatti, assolutamente prioritario garantire che i dati personali elaborati dai sistemi di intelligenza artificiale siano trattati in conformità con i principi fondamentali posti alla base del GDPR, in modo da assicurare agli utilizzatori un'adeguata protezione nell'utilizzo dei propri dati personali, così da preservare e, ove necessario, eventualmente riequilibrare, il rapporto sinallagmatico che lega interessato e titolare del trattamento.

La stessa Commissione, consapevole dei rischi legati ad un eventuale mancato coordinamento tra i due strumenti, nella relazione esplicativa che accompagna la proposta di regolamento, ha chiarito in modo esplicito che la nuova disciplina sull'intelligenza artificiale "non pregiudica il regolamento generale sulla protezione dei dati"[46].

Considerato che, come evidenziato, le fasi della raccolta e del trattamento esulano dall'ambito di applicazione *ratione materiae* contenuto nella proposta di regolamento, appare plausibile ritenere che entrambe ricadranno sotto il governo del GDPR.

Occorre però domandarsi cosa accade nella fase successiva, ovvero una volta che i dati siano stati immessi all'interno del sistema di intelligenza artificiale.

Come è già stato osservato in dottrina, i potenziali conflitti tra le due norme, considerando che il GDPR dà attuazione ad un diritto disciplinato a livello di fonte primaria[47], non potranno essere risolti facendo ricorso al principio di specialità. Ne consegue che le due normative dovranno essere applicate cumulativamente[48].

[46] *Relazione esplicativa alla Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, cit., p. 4.

[47] Si veda *supra,* in questo capitolo, par. 3.

[48] G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, cit., pp. 217 e 218. L'A. evidenzia, in particolare, che a favore di tale conclusione depone il contenuto del considerando n. 24 della

A tale conclusione può giungersi anche confortati da quanto chiarito dalla stessa Commissione che, preso atto dello stretto collegamento che intercorre tra le due normative, ha previsto, all'interno del considerando n. 72 della proposta di regolamento dedicato ai c.d. spazi di sperimentazione[49], che la creazione di tali spazi avvenga in linea con l'articolo 6, paragrafo 4[50] del GDPR, nei casi in cui la raccolta dei dati non possa avvenire dietro il consenso dell'interessato.

Chiarito quindi che i due regolamenti debbano trovare applicazione cumulativa, il problema immediatamente successivo che si pone è il loro esatto coordinamento.

Un rapporto chiaramente definito tra la proposta sull'intelligenza artificiale e la vigente legislazione in materia di protezione

proposta di regolamento sull'intelligenza artificiale che, nel descrivere le modalità di raccolta di dati biometrici, prevede che «qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica (...) dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679».

[49] Gli articoli 53 e 54 della proposta di regolamento insieme ai considerando 71 e 72 sono dedicati agli spazi di sperimentazione ovvero di spazi a sostegno dell'innovazione all'interno dei quali "addestrare" i sistemi di intelligenza artificiale. Si veda per un approfondimento *infra* par. 4.

[50] L'articolo 6, paragrafo 4, regolamento 2016/679 recita: «Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione».

dei dati[51] rappresenta un prerequisito fondamentale per assicurare e preservare il rispetto e l'applicazione dell'*acquis* dell'Unione europea nell'ambito della protezione dei dati personali[52]. A motivo di ciò è importante scongiurare *a priori* incongruenze tra le due discipline ed eventuali conflitti, non soltanto per garantire la certezza del diritto ma anche per evitare che la nuova regolamentazione sull'intelligenza artificiale, una volta definitiva, ponendosi in contrasto con il GDPR, finisca addirittura per compromettere o limitare, direttamente o indirettamente, il diritto fondamentale alla protezione dei dati personali tutelato, dal GDPR ma anche, come ricordato, dall'articolo 16 del TFUE e dall'articolo 8 della Carta di Nizza.

Alla luce di quanto sopra, considerata la stretta relazione che intercorre tra dati personali e intelligenza artificiale, si pone necessariamente l'esigenza di indagare quali principi fondamentali in tema di *privacy*[53], debbano trovare piena applicazione e attenta osservanza anche in tale settore[54].

Peraltro, come considerazione di ordine generale, potrebbe osservarsi che il GDPR contiene dei principi, come ad esempio la minimizzazione dei dati, la limitazione delle finalità e delle decisioni automatizzate, che, almeno in prima battuta, potrebbero sembrare addirittura incompatibili con il funzionamento stesso dei sistemi di intelligenza artificiale che, al contrario, si basano proprio sull'automatizzazione dei processi[55].

[51] G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *Federalismi.it*, n. 16, 2020, p. 269 ss.

[52] Si veda EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on (Artificial Intelligence Act),* par. 56, reperibile online.

[53] V. *supra* cap. II.

[54] Si veda A. ADINOLFI, *L'unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., pp. 30-31.

[55] In una recente pronuncia, la terza sezione del Consiglio di Stato, sentenza n. 7891 del 25/11/2021, al paragrafo 9.1, ha avuto occasione di delineare una distinzione tra algoritmi e intelligenza artificiale. In particolare, secondo i giudici di Palazzo Spada, la nozione generalmente conosciuta di algoritmo «è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. Il grado e la frequenza dell'intervento umano

Ciò posto, nei paragrafi che seguono, ci si soffermerà, in primo luogo, sul profilo del consenso e su quanto possa essere effettivamente sensato, nel settore dell'intelligenza artificiale, discutere di "libero consenso" e, in secondo luogo, si tenterà di capire come debbano essere declinati il divieto di trattamenti totalmente automatizzati, il c.d. "diritto" alla spiegazione, l'individuazione del titolare del trattamento e il concetto di responsabilità, allorquando ci si trovi ad interagire con questi sistemi.

4. I rischi legati all'applicazione cumulativa della proposta di Regolamento sull'intelligenza artificiale e il Regolamento europeo sulla protezione dei dati personali: i possibili profili di interferenza: *a)* consenso; *b)* decisioni automatizzate e diritto alla spiegazione; *c)* titolare del trattamento e responsabilità

In linea generale, sono diversi gli articoli[56] ed i principi del

dipendono dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare». Diverso è, nella prospettiva del Consesso amministrativo, il concetto di intelligenza artificiale poiché, in quest'ultimo caso, «l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole *software* e i parametri preimpostati (come fa invece l'"algoritmo tradizionale") ma, al contrario, elabora costantemente nuovi criteri di interferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico».

[56] Si ricordano in particolare i seguenti articoli:

Articolo 5 – *principi di protezione dei dati, ovvero: liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, accuratezza e limitazione della conservazione*

Articoli 6, 9 e 10 – *liceità del trattamento*

Articoli 12, 13 e 15 – *trasparenza del trattamento*

Articolo 22 – *diritti relativi al processo decisionale esclusivamente automatizzato (e altri diritti dell'interessato)*

Articolo 25 – *protezione dei dati fin dalla progettazione e per impostazione predefinita*

Articolo 32 – *garanzia che i sistemi di AI mantengano al sicuro i dati al loro interno*

Articolo 35 – *valutazioni d'impatto sulla protezione dei dati*

Articolo 36 – *consultazione preventiva.*

GDPR che potenzialmente potrebbero avere un impatto sulla regolamentazione delle tecnologie basate sull'intelligenza artificiale. In questo scenario così articolato, le istituzioni europee sono chiamate ad adottare uno *standard* di settore che possa, da una parte, scongiurare il verificarsi di pratiche di raccolta dati da parte dei sistemi di intelligenza artificiale che si pongano in contrasto con il GDPR e, dall'altra, ridurre al minimo i rischi per gli utilizzatori. A tale duplice obiettivo se ne aggiunge un terzo, di fondamentale importanza per lo sviluppo dell'industria europea, promuovere (e garantire) il buon funzionamento del mercato unico digitale[57].

a) Consenso

Uno dei profili più problematici è certamente quello del consenso.

Il consenso, attualmente, regola il flusso dei dati e costituisce una delle possibili, e più diffuse, basi giuridiche[58] che giustificano e

[57] La strategia del mercato unico digitale intende garantire a tutti gli *stakeholders* europei di trarre il massimo vantaggio possibile dalla rivoluzione digitale in atto. Così la Comunicazione della Commissione 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*. In tale prospettiva, un passo importante è stato compiuto non solo con l'adozione del GDPR ma anche del Regolamento (UE) 2014/1019 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Il regolamento è comunemente noto con la sigla "eIDAS" acronimo di *eletronic identification authentication signature.* Si veda per un commento L. GRECO, M.C. MENEGHETTI, *Articolo 3*, in F. Delfini, G. Finocchiaro (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014*, Torino, 2017, p. 29 ss. Si veda in dottrina G. CAGGIANO, *Il quadro normativo del mercato unico digitale*, in *Eurojus*, fascicolo speciale *Mercato Unico Digitale, dati personali e diritti fondamentali*, 2020, p. 13 ss.

[58] Il consenso costituisce la base giuridica più diffusa seppur non l'unica che può legittimare il trattamento. Il legislatore, infatti, sulla base del principio di *accountability*, ha previsto altre basi giuridiche che puntano alla responsabilizzazione del titolare del trattamento, come ad esempio il legittimo interesse o l'adempimento di un obbligo di legge. Il consenso, in base a quanto stabilisce

legittimano il trattamento da parte del titolare. Il consenso, per sua stessa natura, è un atto libero e volontario. Nondimeno, nel mondo altamente digitalizzato di oggi, gli utilizzatori della rete sono costantemente soggetti a numerosi trattamenti, anche non graditi, oppure, più frequentemente, di cui non sono in grado di comprendere appieno portata e conseguenze.

Come ricordato, secondo quanto dispone il GDPR, il consenso costituisce una delle basi che legittimano il trattamento dei dati[59].

l'art. 4 del GDPR consiste in qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano. Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo. Inoltre, in base al Considerando 32: «il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso». Sulla nozione di consenso nell'ambito della liceità del trattamento dei dati personali si vedano S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Rivista di diritto civile*, 2001, p. 621 ss. e F. CAGGIA, *Libertà ed espressione del consenso*, in V. Cuffaro, R. Dorazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2018, p. 253 ss.

[59] Sul punto si vedano D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali, in Giurisprudenza italiana*, 2019, n. 12, p. 2783 ss.; G. RESTA, *Codice della privacy e data protection*, Milano, 2021, p. 192 ss.; M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. Dorazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 179 ss.; F. RESTA, *Sub art punto 6, reg. UE n. 679/2016*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2018, pp.

In particolare, si prevede che il trattamento risulti legittimo solo nei limiti in cui "l'interessato abbia espresso il proprio consenso"[60]. L'articolo 7 del GDPR fornisce, al riguardo, chiarimenti circa le modalità e le condizioni necessarie affinché il consenso possa ritenersi validamente prestato. In particolare, per considerarsi validamente prestato, il consenso deve essere esplicito, libero, informato, deve essere fornito per uno scopo specifico. Inoltre, devono essere chiaramente indicati tutti i motivi del trattamento e deve essere fornito tramite un atto positivo, motivo per cui, l'onere di dimostrare la volontà dell'interessato di consentire l'utilizzo dei propri dati spetta al titolare del trattamento.

Quello del consenso è da sempre un tema particolarmente dibattuto. Ci si è spesso interrogati, infatti, su quanto effettivamente possa ritenersi una manifestazione libera e consapevole da parte dell'utente. La crescente diffusione in rete del modello commerciale che prevede di offrire dei servizi "gratuitamente", senza cioè la previsione di un corrispettivo in denaro, ma previa acquisizione del consenso al trattamento dei dati personali degli utenti, pone seri dubbi sulla validità – ed effettività – del consenso prestato.

D'altronde, si tratta di un modello estremamente diffuso nei rapporti online, che ha conosciuto peraltro una diffusione ancora maggiore, anche grazie all'evoluzione delle nuove tecnologie. Il solo utilizzo di determinati servizi da parte degli utenti genera una mole consistente di dati, che raccontano delle loro preferenze, delle abitudini di consumo e di vita, dei comportamenti, e che valgono mol-

63 ss.; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 103 ss.

[60] Art. 6 GDPR «1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità [*Omissis*]». Si vedano al riguardo le indicazioni fornite dal WP29, *Guidelines on consent under Regulation 2016/679 (2018)*, EDPB, *Guidelines 8/2020 on the targeting of social media users (2020)*, EDPB, *Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (2020)*, EDPB; *Guidelines 3/2019 on Processing of Personal Data through Video Devices (2020).*

tissimo sul mercato[61]. Peraltro, molto spesso, in sede di accesso a un servizio, viene richiesto all'utente di prestare il consenso al trattamento dei dati personali per fini ulteriori non strettamente necessari per consentire l'erogazione del servizio. Il problema è che spesso il consenso a tali trattamenti supplementari o complementari è posto come condizione necessaria per accedere al servizio principale: si tratta delle operazioni di *tying*[62]. In questo modo ha luogo uno scambio tra il servizio e i dati personali, che costituiscono, almeno di fatto, il corrispettivo per accedere alla controprestazione. Questo modello, trasformatosi ormai in una vera e propria prassi commerciale, solleva seri dubbi, riguardanti innanzitutto la liceità dello scambio dei dati personali con un servizio[63] che, in altre parole, significa interrogarsi sulla liceità di un "mercato dei dati" e sugli eventuali limiti[64].

In realtà, il Garante italiano è già intervenuto a più riprese sul punto[65] chiarendo, ad esempio, in maniera certamente condivisibi-

[61] Il valore economico dei dati personali è fuori discussione si veda, ad esempio, lo studio effettuato dalla ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OEDC Digital Economy Papers No. 220, 2013 disponibile online e in dottrina anche G. MALGIERI, B. CUSTERS, *Pricing privacy – the right to know the value of your personal data*, in *Computer Law & Security Review*, 34, 2017, pp. 294-297 e F.G. VITERBO, *Freedom of contract and the commercial value of personal data*, in *Contratto e impresa Europa*, 2, 2016, pp. 606-607.

[62] Con il termine *tying* si fa riferimento a tutti quei casi in cui la prestazione di un servizio è vincolata al conferimento del consenso dell'interessato per ulteriori e distinguibili finalità del trattamento, supplementari, quindi, rispetto a quella di interesse per l'utente.

[63] Si fa riferimento al mercato per così dire primario dei dati, nel senso di mercato in cui sono gli interessati stessi a immettere i dati in rete. Diverso è invece il discorso con riguardo al mercato secondario dei dati, in cui i titolari del trattamento, una volta raccolti tali dati, li fanno a loro volta circolare. In generale, sui problemi legati al mercato dei dati, in dottrina cfr. V. ZENO-ZENCOVICH, *Do "Data Markets" Exist?,* in *MediaLaws*, 1, 2019, p. 22 ss.

[64] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws*, 11, 2019, p. 132, disponibile online.

[65] Sono state pubblicate le *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679* [WP 259 rev.01] disponibili online.

le, che nel caso di pubblicità commerciale, il consenso deve essere separato rispetto a quello richiesto per la prestazione contrattuale da svolgersi a favore dell'utente poiché quest'ultimo "deve avere la possibilità di addivenire al contratto senza dover subire il ricatto di dover ricevere pubblicità commerciale"[66].

Diversamente, il rischio, certamente concreto, è che molti dei consensi ottenuti per poter usufruire di servizi *online* debbano essere ritenuti non validamente prestati[67].

Ma cosa succede nel caso dei sistemi algoritmici che lavorano su enormi quantità di dati?

La portata delle problematiche sopra sollevate potrebbe ampliarsi considerevolmente nel settore dell'intelligenza artificiale. Tali tecnologie, infatti, lavorano su un'ingente mole di dati, come evidenziato, e normalmente maggiore sarà il numero di dati immessi più accurato sarà il risultato che si potrà ottenere dalla loro elaborazione. Al contrario, il consenso da parte dell'interessato è regolato da principi esattamente opposti quali: la minimizzazione dei dati e la limitazione delle finalità, oltre che l'osservanza da parte del tito-

[66] L'AGCM nel provvedimento adottato contro Meta (Facebook) – *Condivisione dati con terzi,* 29 novembre 2018, n. 27432 ha evidenziato, ad esempio, che la qualifica delle condotte oggetto di esame come "aggressive" discende non tanto dal far seguire conseguenze negative alla revoca del consenso al trattamento, quanto (oltre che dal preselezionare l'opzione della prestazione del consenso) dal prospettare conseguenze negative maggiori di quelle effettivamente applicate. Anche lo *European Data Protection Board* (ex WP29) fornisce un esempio chiarificatore: una *app* per il fotoritocco che chiede il consenso per accedere alla geolocalizzazione e che utilizza i dati a fini di pubblicità comportamentale, considerato che né la geolocalizzazione né la pubblicità sono necessari per la fornitura del servizio di fotoritocco, se subordinasse l'utilizzo del servizio a tale consenso lo renderebbe non libero e, quindi, illecito.

[67] Si vedano in dottrina le considerazioni di C. LANGHANKE, M. SCHMIDT-KESSEL, *Consumer data as consideration*, in *Journal of European Consumer and Market Law*, 2015, 6, p. 218 ss.; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 67 ss.; A. METZGER, *Data as CounterPerformance: What Rights and Duties do Parties Have?,* in *Journal of Intellectual Property*, *Information Technology and Electronic Commerce Law*, 8, 2017, p. 1 ss.; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, p. 436 ss.

lare di specifici e puntuali doveri di informazione e di trasparenza[68]. Ciò implica che il titolare potrà (*rectius* dovrà) raccogliere i dati solo ed esclusivamente per finalità preventivamente determinate, esplicite e legittime e solo limitatamente a quei dati che risultano strettamente necessari per il raggiungimento di tali finalità. Il trattamento successivo dovrà avvenire in modo compatibile con tali finalità e non potrà travalicarle.

Ad un primo esame, dunque, sembrerebbe esserci un'evidente incompatibilità tra la logica sottesa alla prestazione del consenso e le modalità di funzionamento dei sistemi di intelligenza artificiale, particolarmente con la logica dei *Big Data*. Laddove si identifichi il titolare del trattamento in colui che gestisce il sistema di intelligenza artificiale[69], infatti, quest'ultimo si troverebbe nella necessità di rispettare le limitazioni qualitative, in termini di tipologie di finalità perseguita, ma anche quantitative nel senso di mole di dati e di soggetti coinvolti nel trattamento. A ciò deve aggiungersi che, secondo quanto dispone il GDPR, il consenso prestato dall'interessato deve rispettare determinate caratteristiche, ovvero deve essere espresso, libero, specifico e informato[70]. Inoltre si prevede che l'interessato debba avere sempre il controllo sui propri dati e possa eventualmente esercitare i diritti previsti dal GDPR[71].

I requisiti del consenso, inteso come base che legittima il trattamento, così come sopra enunciati, appaiono difficilmente conciliabili nella prospettiva di trattamento multiplo e automatizzato

[68] S. SANDULLI, *Algoritmi, trasparenza ed effettività del consenso*, in *Ius Civile*, 2021, 5, pp. 1528-1546.

[69] Sul punto si veda in questo capitolo la lettera c).

[70] Nella prassi si veda con riferimento ai requisiti del consenso nella giurisprudenza della Corte di Giustizia, CGUE, Grande Sez., 1/10/2019, Causa C-673/17, *Planet49*, in Raccolta Digitale, 2019 e CGUE, 11/11/2020, Causa C-61/19, Orange Romania c. ANSPDCP, *ibidem*, 2020. In ambito nazionale, la Cassazione sul punto ha chiarito che il consenso al trattamento dei dati personali non possa essere equiparato al consenso in generale richiesto ai fini negoziali, Cass., Sez. I, 2/7/2018, n. 17278, *Garante per la protezione dei dati personali c. Soc. Ad Spray*, in *Giurisprudenza italiana*, 2019, p. 530 ss., con nota di S. Thobani.

[71] Si veda A. ADINOLFI, *L'unione europea dinanzi allo sviluppo dell'intelligenza artificiale,* cit., pp. 30, 31.

spesso attuato dai sistemi di intelligenza artificiale. Emerge, infatti, una difficoltà intrinseca nel consentire all'utilizzatore, in qualsiasi momento, così come richiede il GDPR, di avere il pieno controllo sui propri dati.

Invero, nel caso di un trattamento effettuato da un sistema di intelligenza artificiale, spesso il funzionamento intrinseco della tecnologia sfugge alla comprensione stessa dell'utilizzatore medio, che avrà difficoltà a capire le modalità con cui viene effettuato il trattamento (automatizzato) dall'algoritmo e, di conseguenza, gli risulterà molto più difficile esercitare i propri diritti[72].

[72] Nel panorama giurisprudenziale italiano anche la Corte di Cassazione, nell'ordinanza n. 14381/2021, ha avuto modo di esaminare problematiche generate da sistemi algoritmici e di intelligenza artificiale con riferimento alla tutela dei dati. Nella specie, i giudici di Piazza Cavour sono stati chiamati a pronunciarsi circa la liceità dell'utilizzo di un servizio di *rating* reputazione da parte di un soggetto privato. Il ricorso era stato presentato dal garante per la protezione dei dati personali avverso una pronuncia del Tribunale di Roma che, in sostanza, aveva ridimensionato la portata di un provvedimento adottato dall'Autorità stessa teso a bloccare i trattamenti di dati eseguiti al fine di poter gestire tale servizio. La Cassazione ha accolto il ricorso, considerando non corretta la ricostruzione proposta dal Tribunale di Roma del sistema di garanzie che tutela il soggetto interessato dinanzi al trattamento dei propri dati personali. Pure avendo a che fare con trattamenti automatizzati realizzati attraverso l'utilizzo di tecniche algoritmiche, la Cassazione, nell'adottare la propria decisione, ha utilizzato un istituto ormai ben noto nell'ambito del GDPR, ovvero il consenso dell'interessato quale base giuridica che legittima il trattamento. Nella vicenda esaminata dalla Cassazione, infatti, la base giuridica del trattamento costituiva il vero punto critico. In particolare, era in dubbio sulla base di quale fondamento giuridico il sistema di *rating* potesse effettuare i trattamenti necessari e processare i dati raccolti. Tale pronuncia ha fornito alla Cassazione l'occasione per pronunciarsi sulla rilevanza del consenso degli interessati e sulla validità dello stesso alla luce delle particolari circostanze in cui veniva acquisito. A tale riguardo, con precipuo riferimento alla prestazione del consenso, la Cassazione sottolinea che debba esservi una precedente acquisizione di informazioni dettagliate che spieghino all'interessato le attività e questo requisito vale anche nell'ambito di un sistema algoritmico. Da tali premesse discende, non solo la natura informata del consenso prestato, ma anche la sua libertà e specificità. In altre parole, è necessario che l'interessato venga messo a conoscenza delle effettive modalità di funzionamento di un trattamento algoritmico onde potervi liberamente assentire. A tal proposito la Cassazione ha chiarito, all'interno del paragrafo settimo dell'ordinanza in esame, che «non può logicamente affer-

La circostanza inoltre che il GDPR pone in capo al titolare del trattamento l'obbligo di acquisire una nuova manifestazione positiva di volontà, ogni qualvolta la raccolta dati si discosti in maniera oggettiva o soggettiva da quelle che erano le finalità iniziali, pone un problema di bilanciamento tra diritti e obblighi. Ci si riferisce, in particolare, a quanto già previsto dal GDPR all'articolo 19, ove sono disciplinati gli obblighi di notifica nel caso di modifica o di esercizio dei diritti dell'interessato. In questi casi, però, la norma prevedeva già un limite a tale obbligo rinvenibile nell'eccessiva onerosità per il titolare del trattamento di assolvere a tali obblighi di notifica[73]. Si pone dunque, ancora una volta e probabilmente anche con intensità maggiore visti i costi e la complessità dei sistemi di intelligenza artificiale, un problema di bilanciamento tra la necessità di garantire il perseguimento degli obiettivi posti dalla norma e la sostenibilità economica della tipologia di interventi richiesti all'operatore economico[74].

Tutto ciò considerato appare dunque evidente che il meccanismo del consenso, basato sui concetti di limitazione, minimizzazio-

marsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato che si avvale di un algoritmo per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati».

[73] La Corte di giustizia ha chiarito che debba essere garantito un equo bilanciamento tra gli obiettivi normativi perseguiti e la sostenibilità economica da parte del soggetto che si deve far carico dell'attuazione della misura. Si vedano, al riguardo, le pronunce CGUE, 12/7/2011, C-324/09, *L'Orèal c. eBay e altri*, in Racc., 2011, p. I-06011 e anche CGUE, 4/11/2011, C-70/10, *Scarlet c. SABAM*, *ivi*, 2011, p. I-11959, par. 48 dove la Corte nel riferirsi all'obbligo posto in capo al FAI evidenzia che «causerebbe una grave violazione della libertà di impresa del file in questione, poiché l'obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a suo carico, il che risulterebbe peraltro contrario alle condizioni stabilite dall'articolo 3, n. 1, della Direttiva 2004/48, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose».

[74] Si vedano sul punto le riflessioni di G.M. RICCIO, G. GIANNONE CODIGLIONE, *La rilevanza delle basi giuridiche per il trattamento di dati personali mediante sistemi di intelligenza artificiale*, in A. Pajno, F. Donati, A. Perrucci (a cura di), in *Intelligenza artificiale e diritto: una rivoluzione?*, cit. pp. 285 ss.

ne, disponibilità e trasparenza, mal si concilia con il funzionamento intrinseco dei sistemi di intelligenza artificiale, basato su logiche esattamente opposte quali l'aggregazione dei dati ma, soprattutto, la raccolta di un maggior numero di dati possibili per addestrare gli algoritmi, elaborare modelli statistici e predittivi.

Occorrerà, dunque, una particolare cautela da parte legislatore europeo su questo specifico aspetto posto che, anche allo stato attuale della normativa in tema di *privacy*[75], nonostante le tutele ricordate e gli obblighi posti in capo agli operatori economici, molto spesso gli utenti tendono a sottovalutare le conseguenze legate al tema del consenso. Al punto che ci si potrebbe interrogare su quanto si tratti, in effetti, di una scelta volontaria o, piuttosto, se non si debba considerare un'adesione passiva. L'utente, infatti, navigando in rete, si imbatte in continue richieste di assenso al trattamento di dati personali e all'utilizzo di *cookies*. Di sovente queste *policy* sono congegnate in modo da scoraggiare dall'approfondire e, quindi, in evidenza viene posta la ormai ben nota scelta "accetta tutto" mentre, molto meno visibili, risultano le alternative "gestisci preferenze" o "rifiuta tutto", opzione, quest'ultima, peraltro neppure sempre presente.

Se la logica del consenso nei termini oggi conosciuti dovrà essere applicata anche ai sistemi di intelligenza artificiale, il rischio concreto è che questo stesso consenso, già oggi così sottovalutato, apra o quantomeno consenta l'utilizzo dei dati per il perseguimento di finalità non immediatamente percepibili dall'utilizzatore[76].

[75] I principi posti alla base del GDPR esistevano già nella direttiva 95/46 ma erano stati concepiti prima della diffusione massiccia di Internet e dello sviluppo dell'industria dei dati, G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, cit., p. 275 ss. Secondo la nota impostazione proposta da T. WU, *The Attention Merchants. The Epic Struggle to Get inside Our Heads*, New York, 2016, p. 25 ss. e di S. ZUBOF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma, 2019, p. 40 ss., i principi che sono alla base del GDPR, benché poco rispondenti al funzionamento dei sistemi di intelligenza artificiale, costituiscono tuttora il principale argine alla preponderanza delle multinazionali e agli abusi della *privacy* da parte di aziende operanti nel settore della raccolta e dello scambio dei dati.

[76] Si vedano le riflessioni di G. MOBILIO, *L'intelligenza artificiale e le regole*

Ciò posto, sarebbe forse il caso di introdurre delle tutele aggiuntive che potrebbero sostanziarsi nell'imposizione di obblighi di trasparenza più incisivi ovvero nel divieto di utilizzo della dicitura "accetta tutto" nei *banner* in modo da costringere l'utilizzatore a porre una maggiore attenzione a quanto decide di autorizzare nella rete.

b) Trattamenti totalmente automatizzati

Un ulteriore profilo di indagine riguarda il combinato disposto tra gli articoli 12 e 13 (che disciplinano il diritto ad ottenere tutte le informazioni riguardanti il trattamento), l'articolo 14 (che prescrive l'obbligo di notifica qualora i dati non siano ottenuti presso l'interessato) e l'articolo 22 (che prevede il diritto dell'interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato) del GDPR, letti alla luce del contenuto del considerando 71 dello stesso testo che, come noto, ha suscitato un importante dibattito in dottrina[77], nonché i limiti del cosiddetto "diritto alla spiegazione"[78].

giuridiche alla prova: il caso paradigmatico del GDPR, cit., p. 266 ss.

[77] Il contenuto di tale considerando ha diviso la dottrina tra quanti ne fanno discendere unicamente un diritto di accesso e di informazione S. WATCHER, B. MITTELSTADT, L. FLORIDI, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law*, 2017, n. 2 e quanti invece sostengono l'esistenza di un vero e proprio "diritto alla spiegazione" come A.D. SELBST, J. POWLES, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 2017, n. 4.

[78] I giudici interni hanno già iniziato a confrontarsi con tematiche legate all'intelligenza artificiale, seppur incidentalmente, esaminando questioni connesse al GDPR. Ad esempio nel 2018, il *Conseil Constitutionnel* si era pronunciato sulla legittimità di una norma che ampliava la possibilità per la pubblica amministrazione di ricorrere, seppure a titolo di eccezione, a decisioni in grado di produrre effetti giuridici sugli individui fondate su un trattamento automatico di dati personali. La stessa disposizione legittimava decisioni automatizzate nel caso in cui a) l'attività algoritmica non riguardasse dati sensibili, b) fosse percorribile una via di ricorso amministrativa e c) fossero fornite adeguate informazioni in relazione all'utilizzo di algoritmi. Di tale norma era stato dedotto un conflitto con la distribuzione dei poteri esecutivi prevista dall'art. 21 della Costituzione, soprattutto in relazione alle capacità di autoapprendimento degli algoritmi che avrebbero potu-

La problematica si pone in termini evidenti poiché l'articolo 22 del GDPR, che come ricordato prevede il diritto dell'interessato a non essere sottoposto ad una decisione discendente da un processo totalmente automatizzato, non include anche un vero e proprio diritto alla spiegazione. L'unica espressa menzione, al riguardo, si rinviene, infatti, all'interno del considerando 71, secondo il quale:

«l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguar-

to determinare l'applicazione di regole differenti da quelle preimpostate. Il *Conseil* ha escluso l'esistenza di profili di incostituzionalità, ritenendo che fossero state osservate tutte le garanzie necessarie alla salvaguardia dei diritti e delle libertà degli individui, tra cui, la limitazione dell'utilizzo a specifiche tipologie di decisioni, la previsione di specifiche condizioni legittimanti e la possibilità per l'individuo destinatario ultimo di una decisione di ottenere una spiegazione in modalità intellegibili e dettagliate del funzionamento del processo algoritmico. Circa un anno dopo, il Consiglio di Stato, nella sentenza del 13 dicembre 2019, n. 8472, con cui ha ripreso un suo precedente (ovvero la sentenza dell'8 aprile 2019, n. 2270), ha ribadito la necessità che venga garantita la conoscibilità e comprensibilità dell'algoritmo. In questa occasione i giudici di Palazzo Spada hanno preso a riferimento le norme del GDPR per porre in evidenza la particolare attenzione riservata dal legislatore europeo ai casi in cui il trattamento di dati sia interamente automatizzato. In tali ipotesi, infatti, il GDPR affianca, alle esigenze conoscitive – soddisfatte dalla previsione di un diritto di accesso – un espresso limite allo svolgimento di processi decisionali automatizzati (ex art. 22). Il Consiglio di Stato sottolinea, in particolare, che dal diritto europeo si possono evincere tre principi: ovvero il principio di conoscibilità, che si rafforza in principio di comprensibilità quanto si tratti di decisioni automatizzate adottate da soggetti pubblici; il principio di non esclusività della decisione algoritmica, che assicura un contributo umano in grado di controllare, validare o smentire la decisione automatica; il principio di non discriminazione algoritmica, che impegna il titolare dei trattamenti a mettere in atto quanto necessario a rettificare i fattori che comportano inesattezze, per minimizzare gli errori e impedire effetti discriminatori. Nel caso oggetto di esame, a parere del Consiglio di Stato, l'algoritmo non era stato utilizzato in modo conforme a tali principi, poiché non era chiaro il motivo per cui le legittime aspettative di alcuni soggetti collocati in una determinata posizione in graduatoria fossero andate disattese. Si veda M. BASSINI, G. GREGORIO, O. POLLICINO, *Il Gdpr e la protezione dei dati nella società algoritmica: i nuovi sviluppi normativi e giuridici*, in *Agenda Digitale*, 9 settembre 2021, disponibile *online*.

dano o incida in modo analogo significativamente sulla sua persona *(omissis)*».

È evidente quindi che sussiste una lacuna giuridica, poiché collocare una simile disposizione all'interno di un considerando, che per sua stessa natura non ha portata precettiva quanto piuttosto interpretativa, scopre il fianco ad un'incertezza giuridica circa l'effettiva portata della previsione, così come al rischio di vanificare la stessa *ratio* protettiva della norma.

Purtroppo, tale lacuna non sembra essere stata affrontata, almeno non in maniera compiuta, neppure all'interno della proposta di regolamento sull'intelligenza artificiale.

All'articolo 10[79], infatti, il legislatore si è limitato a prevedere

[79] Articolo 10 *Dati e governance dei dati* 1. I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli sono sviluppati sulla base di *set* di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5.

2. I *set* di dati di addestramento, convalida e prova sono soggetti ad adeguate pratiche di *governance* e gestione dei dati. Tali pratiche riguardano in particolare: a)le scelte progettuali pertinenti; b) la raccolta dei dati; c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione; d) la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino; e) una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari; f) un esame atto a valutare le possibili distorsioni; g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate. 3. I *set* di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei *set* di dati possono essere soddisfatte a livello di singoli *set* di dati o di una combinazione degli stessi. 4. I *set* di dati di addestramento, convalida e prova tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato. 5. Nella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo

che i dati di addestramento debbano soddisfare determinati requisiti e che, pertanto, debbano essere pertinenti, rappresentativi, esenti da errori e completi. Una risposta, seppure parziale, visto che si riferisce unicamente ai "sistemi ad alto rischio", si rinviene all'interno dell'articolo 13, paragrafo 1 della proposta secondo cui: «i sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'*output* del sistema e utilizzarlo adeguatamente». All'interno di tale disposizione si potrebbe, dunque, individuare anche l'obbligo da parte degli operatori economici di informare gli utilizzatori e di spiegare le logiche che regolano il trattamento dei dati[80].

Alla luce di quanto sopra, appare certamente opportuno un intervento del legislatore europeo di sistematizzazione volto a porre rimedio ad una situazione che rischia di generare ulteriore confusione e incertezza giuridica. Tale stato di cose, se dovesse essere confermato anche al termine dell'*iter* legislativo in corso, narrerebbe, infatti, la storia di un'occasione mancata.

Tale intervento appare quantomai necessario anche perché, allo stato attuale della normativa, è ancora in discussione la stessa esistenza di un diritto alla spiegazione sulla base del quale si potrebbe giustificare l'imposizione di un obbligo giuridico in tal senso in capo al titolare del trattamento.

Peraltro, come osservato, all'interno delle linee guida redatte dal Gruppo di lavoro articolo 29[81], occorre intendersi sul significato

1, del regolamento (UE) 2018/1725, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

[80] Come è stato osservato, appare piuttosto singolare che il legislatore europeo sembri aver tentato di risolvere alcuni dubbi ermeneutici relativi al GDPR all'interno di un diverso testo normativo (G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, cit., p. 227).

[81] Article 29 – *Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (amended version),* 6/2/2019, Bruxelles.

stesso del termine spiegazione[82], che può assumere diverse connotazioni, a seconda della prospettiva di indagine prescelta. Ad esempio, ci si può riferire al fatto di dover rendere noto il funzionamento di un determinato sistema ma anche all'obbligo di esplicitare le motivazioni che giustificano una determinata decisione. Da un punto di vista temporale, invece, si distingue tra spiegazione *ex ante* ed *ex post*. Nel primo caso si considerano i sistemi algoritmici che effettuano valutazioni di tipo generale, mentre, nel secondo, quelli che adottano decisioni relative a singoli casi[83].

Nel caso dei sistemi di intelligenza artificiale, il "diritto" alla spiegazione rischia di diventare un concetto assai fumoso, non solo per quanto già rilevato sul piano normativo, ma anche, e soprattutto, a causa dell'opacità che spesso caratterizza l'operatività di questi sistemi.

In questo particolare scenario, un diritto alla spiegazione che si limiti ad obbligare l'operatore economico a rendere nota la logica che si cela dietro il funzionamento di un algoritmo potrebbe risultare insufficiente [84] ad assicurare il grado di protezione per l'utilizzatore che la *ratio* stessa della normativa mostra di voler raggiungere. E, d'altronde, non può neppure escludersi che, anche ponendo in capo all'operatore economico un obbligo più ampio di informativa, che lo obblighi a rendere nota all'utilizzatore la logica sottesa al funzionamento dell'algoritmo, si riesca comunque ad ottenere l'effetto finale di tutela desiderato. L'esempio derivante dall'esperienza di interazione con i *cookies banner* può insegnare molto. L'utente medio, infatti, difficilmente ha, in primo luogo, le competenze per decifrare tali informazioni che, senza un adeguato *background*, risultano difficilmente intellegibili – *rectius* traducibili – in un linguaggio comune. In secondo luogo, l'utente spesso non

[82] In dottrina si veda il contributo di A. SIMONCINI, *Art. 22*, in R. D'Orazio, G. Finocchiario, O Pollicino, G. Resta (a cura di), *Codice della Privacy e data protection*, Milano, 2021, p. 387 ss.

[83] E. LONGO, *I processi decisionali automatizzati e il diritto alla spiegazione*, cit., p. 352.

[84] *Ibidem*, p. 353.

dedica tempo aggiuntivo sufficiente per comprendere le informazioni trasmesse.

Un altro profilo di analisi riguarda la tipologia di dati che vengono utilizzati per i trattamenti automatizzati e, in particolare, il possibile utilizzo di dati a carattere discriminatorio[85]. Si avrà modo di approfondire questo aspetto nel capitolo successivo, ma in questa sede appaiono opportune alcune considerazioni strettamente correlate alla tutela dei dati.

Come noto, l'articolo 9 del regolamento sulla protezione dei dati personali vieta di «trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

La disposizione poc'anzi citata regola, però, unicamente le discriminazioni di tipo diretto. Orfane di regolamentazione rimangono così le discriminazioni di tipo indiretto, ovvero quei casi in cui il trattamento, pur non utilizzando dati a carattere discriminatorio, al termine restituisce un risultato che risulta comunque, in qualche modo, discriminatorio.

L'unico riferimento utile in tal senso, seppure sbrigativo, si rinviene, ancora una volta, all'interno del considerando 71 ove si legge che «[a]l fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze il contesto specifici in cui dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impe-

[85] Si rimanda al capitolo successivo per approfondimenti ulteriori per ciò che riguarda l'analisi dei possibili profili di interferenza tra sistemi algoritmici e principio di non discriminazione.

disca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti».

Il quadro appare ancora più preoccupante se riferito al settore dell'intelligenza artificiale poiché il problema di questi sistemi non si esaurisce nella lettura di *input* e *output,* ma di tutto ciò che avviene nello spazio ricompreso tra questi due momenti, estendosi agli eventuali pregiudizi recepiti, che l'algoritmo potrebbe potenzialmente perpetrare all'infinito o, ancora, semplicemente agli errori di sistema. Spesso, peraltro, gli algoritmi utilizzati operano mediante correlazioni tra i dati e non analizzandoli attraverso la lente del nesso di causalità[86].

Il rischio è, dunque, che pur non impiegando dati originariamente discriminatori, il risultato finale restituito dall'algoritmo risulti comunque discriminatorio, potendo ben accadere che il sistema interiorizzi dei pregiudizi di programmazione o di *input* e li riproponga nella decisione finale. Discriminazioni indirette possono verificarsi anche quando un algoritmo utilizza un criterio apparen-

[86] Rimandando al successivo capitolo per approfondimenti, qui ci si limita ad evidenziare che, in un caso divenuto ormai di studio, le indagini effettuate sugli algoritmi utilizzati per calcolare la recidiva negli Stati Uniti hanno evidenziato che quest'ultimi, non funzionando secondo una logica di causazione ma di correlazione, hanno restituito nei risultati diversi "falsi positivi" e "falsi negativi", ovvero soggetti qualificati ad alto tasso di recidiva, che in realtà non hanno più commesso reati, e altri a cui invece l'algoritmo attribuiva un basso rischio di recidiva che, invece, una volta liberi, sono tornati a delinquere. A tal proposito è stato osservato che "Le macchine sono estremamente più efficienti di noi non umani nell'effettuare i calcoli complessi ma non hanno una "intelligenza situazionale" e la capacità di analogie nel caso in cui non siano state allenate con dati specifici", E. LONGO, *I processi decisionali automatizzati e il diritto alla spiegazione*, cit., p. 354. Sempre sul punto un altro autore ha evidenziato che a differenza di un essere umano, i sistemi di intelligenza artificiale non sanno cosa determina la recidiva e si limitano a leggere una serie di dati attraverso modalità che in pratica riproducono in buona sostanza il "metodo degli analoghi", cfr. S. AMATO, *Emozioni sintetiche e sortilegi al silicio*, in *Ars interpretandi*, 2021, p. 1.

temente neutrale che, in realtà, ha un impatto negativo su una determinata categoria di persone[87].

È importante che gli sviluppatori degli algoritmi e, in generale, dei sistemi di intelligenza artificiale, siano consapevoli delle possibili discriminazioni indirette che possono derivare da programmazioni imprecise o incomplete e che implementino severi controlli per evitare di perpetuare questi risultati non corretti e ingiusti. Ciò può includere la valutazione dell'impatto degli algoritmi su diverse categorie di persone e la creazione di meccanismi di trasparenza per consentire ai consumatori di comprendere come vengono utilizzati i loro dati. Come evidenziato, l'articolo 13 della proposta di regolamento prevede qualcosa di simile, tuttavia probabilmente, anche lato normativo, bisognerebbe circoscrivere meglio i confini della trasparenza e del diritto alla spiegazione, per non rischiare di lasciare zone d'ombra in cui gli operatori economici possano rifugiarsi per sottrarsi ai propri obblighi.

c) Titolare del trattamento e responsabilità

Il profilo dell'individuazione del titolare del trattamento è destinato a sollevare importanti problematiche.

Il titolare del trattamento dei dati personali, infatti, ha la responsabilità di garantire che il trattamento dei dati avvenga in modo legittimo, equo e trasparente. In particolare, deve garantire che i dati vengano trattati solo per gli scopi per i quali sono stati raccolti e che vengano protetti contro eventuali violazioni della *privacy*.

Quando si utilizza un sistema di intelligenza artificiale per effettuare il trattamento, il titolare deve essere in grado di garantire che i dati siano utilizzati in modo appropriato, che non vengano impiegati per finalità non autorizzate e che il sistema sia stato costruito in maniera sicura. In altre parole, il titolare del trattamento deve essere in grado di fornire informazioni su come i dati vengono utilizzati e su come vengono protetti e deve essere in grado di garantire agli

[87] Ad esempio, un algoritmo utilizzato per determinare l'idoneità al credito potrebbe utilizzare come criterio il quartiere di residenza, che potrebbe avere un impatto negativo sulla comunità di colore che vive in quella zona.

interessati l'esercizio dei propri diritti[88] e, soprattutto, deve poter dimostrare che i sistemi di intelligenza artificiale utilizzati siano stati progettati e sviluppati in modo da garantire la conformità alle normative sulla protezione dei dati personali.

Nondimeno, appare opportuno evidenziare che le prescrizioni di GDPR e quelle contenute all'interno della proposta di regolamento sull'intelligenza artificiale si indirizzano a soggetti diversi. Mentre quest'ultima impone dei comportamenti agli sviluppatori e ai fornitori di sistemi di intelligenza artificiale, gli obblighi previsti dal GDPR sono posti a carico del titolare del trattamento che, secondo quanto dispone la norma stessa, deve essere identificato in un soggetto unitario a cui l'utente può inoltrare le proprie richieste e nei confronti del quale esercitare i propri diritti. L'esatto opposto avviene nel caso di sistemi di intelligenza artificiale. Spesso, infatti, si tratta di sistemi che implicano l'intervento di più soggetti a livelli diversi. In questi casi, la raccolta dei dati può avvenire con strumenti diversificati, non necessariamente gestiti dal medesimo soggetto. Ne consegue che, o dovrebbe prevedersi una sorta di responsabilità oggettiva e cumulativa da porre a carico di uno solo dei soggetti coinvolti, magari applicando un criterio di prevalenza quantitativa o qualitativa, che tenga conto della tipologia dei dati trattati – soluzione difficilmente percorribile – oppure ci si dovrebbe rassegnare all'idea di avere più soggetti responsabili, con un sostanziale aggravamento della posizione di tutela dell'utilizzatore finale.

In questo senso, quindi, si pone, nell'applicazione cumulativa dei due strumenti, un problema di identificazione del soggetto responsabile, al fine di consentire agli utilizzatori finali di non trovarsi in balia del sistema, senza avere cognizione precisa del riparto di responsabilità e di chi sia il soggetto a cui rivolgersi per esercitare i propri diritti e nei confronti del quale muovere eventuali reclami.

[88] Si veda in dottrina A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale,* cit., p. 24 e ID., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 127 ss.

È stato sostenuto che il titolare del trattamento potrebbe identificarsi con lo stesso sistema di intelligenza artificiale[89]. Questo ovviamente implicherebbe di dover considerare i sistemi di intelligenza artificiale come esseri intelligenti capaci di ragionamento autonomo[90]. Tale aspetto, tuttavia, non viene contemplato nella proposta di regolamento, in quanto le istituzioni europee hanno esclu-

[89] G. SIMONE, *Machine Learning e tutela della Privacy alla luce del GDPR*, in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, p. 275 ss. In senso contrario però F. PIZZETTI, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 45 ss. che sul punto ha sostenuto: «Merita, inoltre, sottolineare che il titolare del trattamento può operare in un quadro di una pluralità di trattamenti che abbiano una comune finalità ma facciano capo a titolari diversi, così come può operare nell'ambito di una catena di trattamenti che abbiano ciascuno finalità diverse, che riguardano l'ambito dei singoli trattamenti da ciascun "anello" operanti, ma che, connessi l'uno con l'altro, producono effetti che nessuno dei trattamenti in catena potrebbe determinare da solo. Un fenomeno, questo, che specialmente nel mondo della robotica e del c.d. *IoT* [*Internet of things*] si sta delineando con riguardo al tema della responsabilità civile nel caso che le macchine producano danni sulla base di comportamenti o azioni a determinare i quali concorrono pluralità di trattamenti in catena uno con l'altro, compresi quelli che possono aver determinato l'utilizzazione da parte dell'algoritmo finale di dati imprecisi o inadeguati prodotti da trattamenti precedenti».

[90] Indagando il primato delle macchine sull'uomo, gli studiosi cercano di rispondere ad una domanda, ovvero se le macchine siano o meno dotate di una mente e di pensieri. In questo campo, si fronteggiano due teorie, quella dell'IA "forte", che si riferisce a macchine che hanno una mente o che, comunque, finiranno per averne una un giorno, e quella dell'IA "debole", che ritiene che le realtà delle macchine siano solo semplici simulazioni e non una duplicazione dell'intelligenza reale. Il bivio concettuale è tra la possibilità che le macchine possano essere veramente intelligenti o semplicemente in grado di comportarsi come se lo fossero. Secondo la distinzione operata dal filosofo americano John Searle, l'intelligenza artificiale debole agisce e pensa come se avesse un cervello, ma non è intelligente; si limita a emulare il cervello umano. Per offrire la migliore risposta a un problema, indaga su casi simili, li studia e sceglie la risposta più razionale. L'IA debole non comprende tutti i processi cognitivi umani, ma si occupa solo di risolvere i problemi; risponde ai problemi sulla base di regole conosciute. Al contrario, l'intelligenza artificiale forte ha capacità cognitive indistinguibili da quelle umane, ma secondo Searle, siamo ancora lontani da questa realtà.

so, almeno per il momento, la soggettività giuridica dei sistemi di intelligenza artificiale[91].

[91] Risulta quindi difficile imputare all'intelligenza artificiale una responsabilità giuridica per danni, rendendosi quindi necessario individuare altre strade, con le relative ed inevitabili forzature. Un primo approccio in tal senso è arrivato dal Parlamento Europeo con la Risoluzione del 20 ottobre 2020, con la quale è stata prospettata la possibilità di ricorrere alla responsabilità oggettiva del produttore regolata dalla Direttiva 85/374/CEE. In particolare, questa sussiste anche in assenza di colpa, qualora il danneggiato riesca a provare la difettosità del prodotto, il danno e il nesso di causalità tra quest'ultimo ed il difetto. A titolo di prova liberatoria, il produttore deve invece dimostrare, in base al c.d. rischio di sviluppo, l'imprevedibilità del difetto al momento della messa in circolazione o la sua sopravvenienza. Non mancano però i dubbi, soprattutto circa l'onere probatorio particolarmente proibitivo posto a carico del consumatore. È infatti improbabile che l'utente comune possa dimostrare il difetto, il danno subito e il nesso di causalità in relazione a dispositivi altamente tecnologici. Inoltre risoluzione 2015/2013(INL), al par. 59, lett. f), suggeriva alla Commissione di prevedere "l'istituzione di uno *status* giuridico specifico per i *robot* nel lungo termine, di modo che almeno i *robot* autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei *robot* che prendono decisioni autonome". Questa impostazione ha suscitato diverse critiche tanto che il Comitato economico e sociale europeo ha raccomandato "di adottare, nei confronti dell'IA, l'approccio *'human-in-command'* con la condizione essenziale che l'IA sia sviluppata in maniera responsabile, sicura e utile, e che la macchina rimanga macchina e l'uomo ne mantenga il controllo in ogni momento" (*Parere del Comitato economico e sociale europeo*, del 31 maggio 2017, *L'intelligenza artificiale – Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società, (parere d'iniziativa)* 2017/C288/01, p. 1-9). In dottrina si veda G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, cit., p. 209 ss.; B. ANDREA, *Artificial Intelligence does not exist!*, cit., p. 369; G. DE ANNA, *Automi, Responsabilità e diritto*, in *Rivista di filosofia del diritto*, 2019, p. 125 ss.; A. DRIGO, *Sistemi emergenti di intelligenza artificiale e personalità giuridica: un contributo interdisciplinare alla tematica*, in S. Dorigo (a cura di), *Il Ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., p. 179 ss.; G.P. CIRILLO, *I soggetti giuridici digitali*, in *Contratto e impresa*, 2020, p. 574 ss.; R. TREZZA, *Diritto e intelligenza artificiale. Etica-Privacy-Responsabilità-Decisione*, Pisa, 2020, p. 49 ss.; P. MORO, *Alle frontiere della soggettività: indizi di responsabilità delle macchine intelligenti*, in U. Ruffolo (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, cit., p. 55 ss.; U. RUFFOLO, *La personalità elettronica tra "doveri" e "diritti" della*

All'interno dello stesso GDPR si possono rinvenire delle disposizioni che militano nel senso di escludere la possibilità di identificare il titolare del trattamento in un sistema di intelligenza artificiale. Ci si riferisce, in particolare, all'articolo 4, paragrafo 1, n. 7, che definisce il titolare del trattamento come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi di trattamento». La lettura letterale della norma suggerisce dunque che debba esserci, anche nel caso di "servizio o altro organismo", la possibilità di identificare comunque un gestore fisico a cui attribuire la responsabilità del trattamento[92].

In termini di responsabilità[93], la prospettiva delle istituzioni eu-

macchina, in *XXVI Lezioni di diritto dell'intelligenza artificiale*, cit., p. 115 ss. e ID., *Intelligenza artificiale,* machine learning *e responsabilità da algoritmo*, in *Giurisprudenza Italiana*, 2019, 7, p. 1657 ss.

[92] Così G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza italiana*, 2019, p. 1670 ss. e particolarmente p. 1674 dove si legge: «La definizione di titolare contenuta nel regolamento chiaramente indica che il titolare debba essere persona giuridica o fisica o comunque soggetto giuridico».

[93] Si veda sul punto il contributo di A. MARCHINI, *Intelligenza artificiale e responsabilità civile: dal "Responsibility Gap" alla responsabilità elettronica dei robot*, in *Il Ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., p. 231 ss. Da segnalare, inoltre, l'iniziativa della Commissione europea che in data 28 settembre 2022 ha adottato due proposte per adattare le norme sulla responsabilità civile all'era digitale, all'economia circolare e all'impatto delle catene globali del valore. L'iniziativa della Commissione si propone, in primo luogo, di ammodernare le norme vigenti in materia di responsabilità oggettiva dei produttori per i prodotti difettosi (dalle tecnologie intelligenti ai farmaci) in modo da dare alle imprese la certezza del diritto e agevolare gli investimenti e, al contempo, di garantire che, in caso di danni, le vittime possano ottenere un giusto risarcimento quando i prodotti sono difettosi, inclusi quelli digitali. In secondo luogo, la Commissione propone, per la prima volta, un'armonizzazione mirata delle norme nazionali in materia di responsabilità per l'IA, rendendo più facile per le vittime ottenere un risarcimento e garantendo che possano beneficiare degli stessi *standard* di protezione quando vengono danneggiate da prodotti o servizi di IA, così come avverrebbe se il danno fosse causato in qualsiasi altra circostanza. Si prevede, inoltre, che cinque anni dopo l'entrata in vigore della direttiva sulla responsabilità civile in materia di IA, la Commissione valuti la necessità di introdurre norme sulla responsabilità senza colpa per i sinistri legati all'IA. *Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence*

ropee è di considerare comunque l'intelligenza artificiale un oggetto, sicuramente molto evoluto, ma il cui funzionamento continua ad essere basato sull'elaborazione di quantità più o meno grandi di dati immessi dall'esterno. Resta il fatto che il ruolo dell'uomo resta imprescindibile e la prospettiva "umanocentrica" irrinunciabile.

5. I c.d. "spazi di sperimentazione" per l'addestramento uomo-macchina come opportunità per garantire una migliore tutela della privacy

I c.d. "spazi di sperimentazione" normativa consentono, anche nel settore dell'intelligenza artificiale[94], di mettere in collegamento imprese innovative ed autorità di regolamentazione al fine di fornire degli ambienti controllati all'interno dei quali promuovere una cooperazione costruttiva e lo scambio di informazioni. Tale collaborazione tra autorità di regolamentazione ed imprese che innovano dovrebbe facilitare lo sviluppo, la prova e la convalida di tali tecnologie al fine di garantire, in ultima analisi, la conformità dei sistemi sviluppati ai requisiti normativi dettati all'interno della nuova proposta di regolamento in materia e, in quello che al termine dell'*iter* legislativo sarà il testo finale che verrà licenziato dalle istituzioni europee.

In particolare, l'obiettivo di tale collaborazione è di creare delle *best practices* e *guidelines* utili a consentire un facile utilizzo e una più agevole diffusione dei sistemi di intelligenza artificiale, consen-

(AI Liability Directive, Brussels, COM(2022) 496final.

[94] Un progetto pilota del primo spazio di sperimentazione normativa sull'intelligenza artificiale è stato presentato a giugno del 2022 dal governo spagnolo e dalla Commissione europea in occasione di un evento tenutosi a Bruxelles alla presenza delle autorità spagnole ed europee e di esperti di fama del settore. I primi *test* sono iniziati nell'ottobre 2022 e i risultati saranno pubblicati durante la presidenza spagnola del Consiglio dell'UE nel secondo semestre del 2023. L'esperienza acquisita all'interno dello spazio di sperimentazione sarà presentata sotto forma di *best practises* e *guidelines* e sarà messa a disposizione di tutti gli Stati membri e della Commissione europea e potrà essere utilizzata in preparazione dell'attuazione del futuro regolamento sull'intelligenza artificiale.

tendo anche alle *medium sized companies*, che da sole non avrebbero la forza economica di sostenere gli ingenti investimenti necessari per le attività di ricerca e sviluppo in questo specifico settore, di prendere parte alla progettazione di sistemi di intelligenza artificiale e di beneficiare dei risultati, in termini di efficientamento dei prodotti e di ottimizzazione dei processi.

All'interno della proposta di regolamento, l'articolo 56 paragrafo 6, rimanda la normazione specifica di questi spazi di sperimentazione a future linee guida che dovranno essere emanate dall'istituendo comitato europeo sull'intelligenza artificiale. Sarà dunque tra i compiti di tale organo dettare norme che risultino in grado di accordare i diritti e gli obblighi discendenti dall'uso dei dati personali con il funzionamento stesso di tali spazi, anche nel settore dell'intelligenza artificiale.

Al fine di garantire il buon funzionamento di questi spazi di sperimentazione, all'interno della proposta, il legislatore europeo sembra voler derogare (seppure temporaneamente e per finalità specifiche) ai diritti discendenti dal GDPR normalmente garantiti all'interessato – ci si riferisce all'accesso, alla rettifica, alla limitazione, alla cancellazione e alla portabilità. Tale deroga è però mitigata dalla previsione di alcuni obblighi aggiuntivi per le imprese che decidono di prendere parte allo spazio di sperimentazione. In particolare, si prevede che i dati debbano essere trattati in uno spazio "separato, isolato e protetto" e sotto il diretto controllo dei partecipanti alla sperimentazione, precludendone l'accesso ai terzi. Sono altresì previsti il divieto di trasmissione dei dati all'esterno dello spazio; l'obbligo di cancellazione dei dati una volta conclusa la sperimentazione e, infine, la conservazione di una descrizione accurata del processo di sperimentazione e della logica utilizzata.

In altre parole, il legislatore europeo, a fronte della compressione dei diritti che l'interessato potrebbe esercitare ai sensi degli articoli da 15 a 20 del GDPR, stabilisce che il trattamento avvenga secondo delle tutele specifiche e aggiuntive. Appare quindi evidente che, in questo caso particolare, la deroga all'esercizio dei diritti in tema di *privacy* discenda da una valutazione di opportunità e da un contemperamento di esigenze effettuate *a priori* dallo stesso legislatore che, in un'ottica di favorire più possibile lo sviluppo di sistemi

innovativi di intelligenza artificiale, ha valutato accettabile la compressione, beninteso rigorosamente circoscritta nello spazio e nel tempo, dei diritti dei singoli utilizzatori. In questo caso, le esigenze collettive sono state considerate prevalenti rispetto a quelle individuali[95]. D'altronde, come noto, i diritti degli interessati non sono concepiti nell'ambito del GDPR come diritti assoluti e, per questo, possono essere parzialmente sacrificati, seppur entro limiti ben determinati, a favore di esigenze collettive "superiori".

A tale riguardo, è stato osservato in dottrina, in maniera condivisibile, che la deroga prevista dalla proposta di regolamento per gli spazi di sperimentazione, in effetti, non si pone in contrasto con il GDPR e rappresenta un compromesso accettabile per consentire all'Europa di utilizzare anche questo strumento per colmare l'importante *gap* tecnologico che la divide da paesi tecnologicamente molto più avanzati.

6. Intelligenza artificiale e tutela dei dati: il caso degli assistenti vocali casalinghi e la posizione del Garante per la Protezione dei Dati Personali

Volgendo per un attimo lo sguardo verso le odierne iniziali applicazioni pratiche di sistemi di intelligenza artificiale, che hanno già manifestato di poter generare un impatto significativo sulla protezione dei dati, si può citare il caso degli assistenti vocali, che mostrano molte delle criticità esaminate nei paragrafi che precedono.

Gli assistenti vocali, più comunemente noti come *smart assistant* o *home assistant*, sono programmi in grado di comprendere ed interpretare il linguaggio umano proprio attraverso l'impiego di algoritmi di intelligenza artificiale. Questa tecnologia, ormai molto dif-

[95] Si vedano a tale proposito le formulazioni degli articoli 15, paragrafo 4 che regola il diritto di accesso o dell'articolo 17, par. 3, per il diritto all'oblio. Entrambe suggeriscono che vi è sempre un'esigenza di bilanciamento tra diritti individuali ed esigenze collettive. Sul punto in dottrina si vedano le riflessioni di G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, cit., p. 1675.

fusa, viene generalmente installata su vari dispositivi (quali *smartphone*, automobili, *speaker*, *computer*).

Elaborando i dati di *input*, questi sistemi hanno la capacità di dialogare con l'ambiente circostante e di soddisfare diverse tipologie di richieste come, ad esempio, fare ricerche su Internet, rispondere a chiamate telefoniche in ingresso, leggere messaggi di testo e, sempre più spesso, anche messaggi inviati tramite *app*, ricercare e indicare percorsi stradali e svariate altre funzionalità. Sono, altresì, in grado di compiere vere e proprie azioni come, ad esempio, concludere acquisti online, regolare la temperatura o l'illuminazione di un'abitazione, chiudere o aprire serrature di case o automobili o attivare elettrodomestici c.d. *smart*.

Questo tipo di tecnologia, che è sempre più amata, in quanto, sotto molti punti di vista, è in grado di semplificare la vita quotidiana, risulta, come ovvia conseguenza, anche sempre più diffusa. Secondo le recenti proiezioni degli esperti, infatti, le case del prossimo futuro saranno sempre più *smart* e digitalizzate, grazie a soluzioni tecnologiche sempre più avanzate a prezzi competitivi[96].

Certamente questi sistemi, che normalmente uniscono un modulo di *smart speaker* con uno di *virtual personal assistant*, consentono agli utilizzatori di risparmiare tempo e denaro, ma pongono

[96] Dai dati resi noti dall'Osservatorio *Internet of Things* della *School of Management* del Politecnico di Milano è emerso che il 46% degli italiani possiede almeno un dispositivo *smart*, ovvero connesso alla rete. Tra questi, la *smart tv* è l'oggetto più presente nelle case (72%), seguita dagli assistenti vocali (Alexa, Google Home, Siri) in grado di comandare gli oggetti domestici tramite la rete *wi-fi* con il 29%, da stampanti e lampadine *smart* (rispettivamente 23% e 20%). Ci sono poi gli elettrodomestici connessi tra cui la lavatrice (17%), il frigorifero (13%) e la lavastoviglie (10%), dati disponibili *online*.

Negli Stati Uniti circa il 24% della popolazione ha almeno un assistente vocale in casa fino ad arrivare, tra gli utilizzatori più assidui, ad una media di 2.6, v., *The Smart audio report*, *National Public Media*, 2020, disponibile *online*.

Nel Regno Unito, un sondaggio svolto tra la popolazione ha rivelato che il 26% dei soggetti intervistati possiede almeno un dispositivo *smart*, si veda EY, *Report Taking new steps into the smart home,* disponibile *online*.

Nei Paesi Bassi è stato stimato che circa il 19% della popolazione abbia un dispositivo simile in casa, v. *Smart home monitor*, *Multiscope*, 2020, disponibile *online*.

anche delle nuove importanti sfide in termini di tutela dei dati personali[97].

Gli assistenti digitali e gli altri dispositivi "connessi", infatti, sono in grado di raccogliere e memorizzare una grande quantità di dati personali, riguardanti, ad esempio, scelte, preferenze, abitudini relative a stili di vita, consumi, interessi, caratteristiche biometriche (riconoscimento vocale e del volto), geolocalizzazioni e, nei casi dei sistemi più avanzati, anche stati emotivi. Inoltre, la loro frequente collocazione in ambienti domestici, unitamente alla scarsa consapevolezza da parte degli utenti che li utilizzano, rischia di aumentare esponenzialmente le minacce per la tutela e la salvaguardia dei dati personali[98]. Tali sistemi, infatti, sono in grado di raccogliere informazioni non solo quando richiesto, ma anche quando sembrano inattivi o, più precisamente, quando si trovano in modalità *stand-by*[99].

Si sono verificati casi di ascolto di conversazioni strettamente riservate, come, ad esempio, scambi tra dottore e paziente, avvocato e cliente, ma anche semplicemente persone registrate in momenti particolarmente privati della vita quotidiana. Queste registrazioni sono spesso accompagnate da dati quali la localizzazione, i dettagli di contatto e, in generale, i dati immessi nel sistema che rendono molto facile l'identificazione dei soggetti coinvolti[100].

[97] N. NI LOIDEAIN, R. ADAMS, *From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistant and the Role of Data Protection Impact Assessments*, in *Computer Law and Security Review*, 2020, pp. 1-14.

[98] Accessnow*, Report Human rights in the Age of Artificial Intelligence,* p. 20, disponibile online. Per approfondimenti T. GILS, E. WAUTERS, B. BÉNICHOU, J. DE BRUYNE, P. VALCKE, *Artificiële Intelligentie en gegevensbescherming: een verkennende gids. Kenniscentrum Data & Maatschappij,* Brussel, 2020, disponibile online.

[99] J. LAU, B. ZIMMERMAN, F. SCHAUB, *Alexa are you listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviours with Smart Speakers*, in *Proceedings of the ACM on Human-Computer Interaction*, 2018, Vol. 2, Art. 102; D.J. DUBOIS, *Smart Speakers Study - When Speakers Are All Ears: Understanding When Smart Speakers Mistankenly Record Conversations*, *Mon(IoT)r Research Group*, 2020, disponibile *online*.

[100] Secondo quanto chiarisce l'articolo 4 paragrafo 1 del GDPR, deve considerarsi dato personale «qualsiasi informazione riguardante una persona fisica

Proprio in relazione all'identificabilità dei soggetti, il caso degli assistenti vocali[101] genera alcune criticità. Come detto, infatti, normalmente questi sistemi sono posizionati all'interno di ambienti domestici: questo implica che gli utenti che potrebbero trovarsi ad interagire con tali sistemi, anche inconsapevolmente, sono molteplici, inclusi minori[102].

Si è parlato a tale proposito di utilizzatori primari, secondari e incidentali. I primi sono quelli che consapevolmente acquistano il prodotto, lo collegano al loro *account* personale, inseriscono i loro dati al fine di consentire al sistema di rispondere correttamente alle richieste avanzate. I secondi sono normalmente coloro che condividono lo stesso ambiente domestico e che, magari, utilizzano tali dispositivi senza però avere conoscenza di quali dati vengano effettivamente raccolti e trattati. Infine, vi sono gli utilizzatori incidentali, ovvero gli ospiti o i frequentatori saltuari dell'ambiente che, ovviamente, risultano ignari del fatto che magari, nel corso della loro visita, siano in funzione dispositivi di assistenza vocale che, a seconda delle impostazioni, potrebbero registrare conversazioni e informazioni[103].

Questa circostanza pone delle questioni importanti circa la ca-

identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». In dottrina cfr. C. VANDER MAELEN, E. LIEVENS, J. VERMEULEN, I. MILKAITE, *AI and Data Protection: The Case of Smart Home Assistant,* in J. De Bruyne, C. Vanleenhove (a cura di) *Artificial Intelligence and the Law*, Cambridge, 2022, p. 181 ss.

[101] Per comodità espositiva e per diffusione si farà perlopiù riferimento al sistema di Amazon, Alexa.

[102] J. DE MEYER, *The Domestication of Smart Home Assistants: Recommendations for Data Controllers on How to Protect Children's Personal Data in Accordance with the GDPR – A Case of Study of Amazon Alexa, Google Assistant and Apple Siri,* Master's Dissertation in Law Ghent University.

[103] C. VANDER MAELEN, E. LIEVENS, J. VERMEULEN, I. MILKAITE, *AI and Data Protection: The Case of Smart Home Assistant,* cit., p. 179 ss.

pacità di tali sistemi di riconoscere gli utilizzatori[104]. Tale distinzione è fondamentale se osservata attraverso la lente del GDPR, poiché il discrimine tra la stessa possibilità di applicare o meno la normativa europea è rinvenibile nella possibilità di identificare le persone i cui dati sono oggetto di trattamento[105].

I dispositivi di assistenza vocale hanno normalmente una parola di attivazione che consente a questi sistemi di 'uscire' dalla modalità *stand-by* e mettersi in ascolto. Il dispositivo rileva tale parola di attivazione recependo gli impulsi sonori che le corrispondono. Una volta che la parola di attivazione viene rilevata, il dispositivo inizia a registrare l'audio da trasmettere al *cloud*, inclusa una frazione di secondo di suono precedente. L'audio rilevato viene trascritto attraverso un algoritmo che automaticamente riconosce e trascrive la conversazione e viene poi inviata al server *cloud* di archiviazione, rientrando così nella nozione di trattamento dettata dal GDPR. Questo trattamento riguarda normalmente dati personali, ma anche dati biometrici, laddove avvenga un riconoscimento vocale o visivo dell'utilizzatore.

Nessun audio dovrebbe essere registrato né inviato al *cloud* a meno che il dispositivo non rilevi la parola di attivazione o venga attivato manualmente con un pulsante. Tuttavia, si sono verificati

[104] È stato chiarito che alcuni dispositivi sono in grado di riconoscere e differenziare. Ad esempio leggendo le FAQ riguardanti il dispositivo Alexa si legge che: «Alexa memorizza nel *cloud* i modelli acustici creati. Se un utente smette di utilizzare Alexa e la sua voce non viene riconosciuta per un periodo di tre anni, il modello acustico relativo alla voce di tale utente verrà automaticamente cancellato. Qualora Alexa riconosca la tua voce al momento del tuo utilizzo di una *Skill* di terzi, tale *Skill* potrebbe ricevere un identificatore numerico così da permetterci di distinguerti dagli altri utenti del tuo Nucleo Familiare e quindi personalizzare meglio la tua esperienza».

[105] Il GDPR definisce il concetto di 'trattamento', all'articolo 4 paragrafo 2, come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

casi di attivazione involontaria che possono sollevare problemi per la tutela dei dati degli utilizzatori.

Nel caso del noto e diffusissimo dispositivo Alexa, ad esempio, Amazon ammette che vi possano essere casi in cui il dispositivo potrebbe interpretare un'altra parola o un altro suono come parola di attivazione (ad esempio, il nome "Alex" o qualcuno che dica "Alexa" alla radio o alla televisione). Tali comportamenti vengono trattati come "attivazioni involontarie"[106].

Nondimeno, l'incremento costante di raccolta di dati nell'era dell'IoT[107] può significativamente diminuire la sicurezza nel percepire anche gli spazi domestici, quelli che dovrebbero essere, per definizione, luoghi accoglienti e privati. La sensazione orwelliana di essere costantemente osservati, ascoltati e sorvegliati genera stati di ansia e, di fatto, limita la libertà di espressione anche all'interno delle mura domestiche.

Inoltre, la raccolta, il trattamento e l'eventuale trasferimento di dati di natura sensibile – quali dati sanitari, idee politiche, credenze religiose, orientamenti sessuali – se utilizzati a fini di profilazione, potrebbero facilmente sfociare in pratiche discriminatorie, seppure indirette, laddove scelte importanti vengano assunte proprio sulla base di tali profilazioni. L'impatto potrebbe essere ancora maggiore nel caso dei minori e il loro diritto ad uno sviluppo sano.

Il Garante, nell'esaminare la questione, ha redatto una sorta di

[106] Il problema si pone poiché, sebbene l'utilizzatore abbia la possibilità di cancellare le proprie registrazioni, accade nelle FAQ di Amazon viene chiarito che è possibile che le registrazioni relative alle interazioni tra l'utilizzatore e Alexa, incluse le registrazioni delle azioni intraprese da Alexa per rispondere alle richieste vengano mantenute, ai fini di miglioramento del servizio e che inoltre se la richiesta dell'utilizzatore è stata elaborata da una *Skill* di Alexa, la cancellazione delle registrazioni vocali non comporta l'eliminazione delle informazioni in possesso dello sviluppatore della *Skill* (sebbene gli sviluppatori delle *Skill* non ricevono le registrazioni vocali).

[107] L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., p. 11, l'A. evidenzia che «istruzione, affari e industrie, viaggi e logistica, banche, vendita al dettaglio e *shopping*, intrattenimento, *welfare* e sanità, politiche e relazioni sociali, in breve la vita stessa per come la conosciamo oggi, è diventata inconcepibile senza le tecnologie digitali».

vademecum per gli utilizzatori[108] invitando ad adottare un atteggiamento altamente prudenziale.

In particolare, all'interno del documento viene sottolineata l'importanza di fare un uso informato e consapevole di questi strumenti, per tutelare in modo adeguato i dati personali e quelli di tutte le persone che entrano, volontariamente o meno, nel campo di azione degli assistenti digitali.

L'invito da parte dell'Autorità è a verificare quali e quante informazioni saranno acquisite direttamente dall'assistente digitale; come vengono utilizzati i dati raccolti; se sia previsto il loro trasferimento a soggetti terzi; chi e come può ricevere i dati e se siano possibili, per qualsiasi ragione, accessi "in diretta" al microfono e alla videocamera dello *smart assistant* da parte di addetti della società che lo ha prodotto o della società che gestisce i servizi offerti; e, infine, dove vengono conservati i dati e per quanto tempo.

Ritornano con forza, nei consigli del Garante, i concetti di minimizzazione e di pseudonimizzazione. Gli utilizzatori sono invitati, infatti, a non dire troppe cose allo *smart assistant*, a fornire solo le informazioni specificamente necessarie per la registrazione e attivazione dei servizi ed eventualmente ad utilizzare pseudonimi per gli *account*, soprattutto se riferiti a minori.

Un'attenzione particolare, secondo l'Autorità, dovrebbe essere posta nel consentire all'assistente digitale di memorizzare informazioni delicate come quelle relative alla salute, a *password* di accesso a conti correnti o numeri di carte di credito. Inoltre, secondo il Garante sarebbe opportuno disattivare questi dispositivi quando non devono essere utilizzati, poiché si trovano da accesi in uno stato di *passive listening* in cui l'assistente digitale è potenzialmente in grado di "sentire" ed eventualmente anche di "vedere", tramite il microfono e la videocamera in dotazione al dispositivo, tutto quello che viene detto o fatto nel raggio di operatività dell'ambiente in cui si trova.

Il Garante mette, inoltre, in guardia gli utilizzatori dai potenziali

[108] Garante per la protezione dei dati personali, *Assistenti digitali (smart assistant): i Consigli del Garante per un uso a prova di privacy*, marzo 2021, disponibili *online*.

rischi che potrebbero derivare da alcune funzioni di controllo domotico che potrebbero consentire a malintenzionati di captare e clonare la voce dell'utente al fine di controllare elettrodomestici o sistemi di protezione della casa, oppure per "spiare" l'interno dell'abitazione utilizzando microfoni e videocamere.

Per limitare il trattamento dei dati personali raccolti dall'assistente digitale, l'Autorità consiglia di provvedere periodicamente: a cancellare la cronologia delle informazioni in esso registrate; verificare la crittografia della rete *Wi-Fi*; cambiare periodicamente le *password*; controllare se sul dispositivo in cui è installato lo *smart assistant* siano presenti sistemi di protezione *anti-virus* e tenerli costantemente aggiornati e, chiaramente, qualora si decida di disfarsene, di essere certi di non vendere o regalare, unitamente al dispositivo, anche i propri dati e quindi di esercitare, nei confronti dell'azienda produttrice, il diritto alla cancellazione.

Il Garante sottolinea, comunque, che anche questi dispositivi devono essere prodotti e configurati nel rispetto di quanto prevede il GDPR, al fine di ridurre al minimo la raccolta e il trattamento di dati personali, nel rispetto degli ormai ben noti principi della *privacy by design* e *privacy by default*, del generale principio di minimizzazione e di trasparenza riguardo al trattamento dei dati e dei diritti delle persone fisiche.

Quello degli assistenti vocali è solo una tra le più comuni applicazioni "domestiche" di sistemi di intelligenza artificiale, eppure ha già sollevato diversi profili problematici, al punto da richiedere un intervento specifico del Garante privacy. Peraltro, al di là dei contenuti, certamente condivisibili, questo intervento assume un'importanza ancora più rilevante poiché pone gli sviluppatori e distributori nella necessità di fornire spiegazioni e chiarire il proprio *modus operandi*, anche rispetto ai sistemi generati e immessi in commercio. D'altronde, i profili di responsabilità e di rischio, se non correttamente gestiti, potrebbero generare conseguenze sfavorevoli.

7. Il caso *ChatGPT*

Di recente si è parlato molto di *Generative AI*, ovvero di Intelligenza Artificiale Generativa[109].

Uno dei casi più discussi è stato certamente quello di ChatGPT (acronimo di *Generative Pretrained Transformer*), un sistema sviluppato da OpenAI[110].

ChatGPT utilizza sistemi di reti neurali artificiali multilivello con architetture basate su algoritmi di *deep learning*. Attraverso l'utilizzo di algoritmi avanzati di apprendimento automatico, tramite cui riesce a comprendere modelli e sfumature del linguaggio naturale, è in grado, basandosi sulla tecnologia del *Natural Language Processing* (NLP)[111], di generare risposte simili a quelle umane. Si tratta di algoritmi di *deep learning* supervisionati, che sono in grado di migliorarsi costantemente e automaticamente attraverso l'esperienza, partendo da dati di *training* immessi per poi effettuare predizioni senza essere stati esplicitamente e specificatamente programmati a farlo. Il sistema utilizza altresì il *reinforcement learning*, ovvero quella tecnica di *machine learning* in cui un *software* impara a svolgere un'attività tramite ripetute interazioni di tipo *trial-and-error* con un ambiente dinamico, ma anche il *deep learning* basato su reti neuronali profonde nelle quali il segnale di *input* viene trasmesso e modificato[112]. Le nuove tecniche matematiche hanno con-

[109] Con questa espressione si fa riferimento alla capacità di una macchina di generare un'informazione nuova e originale partendo da una serie di *input* immessi. Il sofisticato livello di informazione raggiunto dagli algoritmi consente di generare testi, modelli 3D, ma anche immagini, video e contenuti musicali.

[110] Si tratta di un'organizzazione americana *no profit* che opera nel settore della ricerca sull'intelligenza artificiale.

[111] Si tratta di una branca dell'intelligenza artificiale che si concentra sull'interazione tra *computer* e linguaggio umano.

[112] Per capire meglio di cosa si tratti è stato chiesto direttamente alla *chatbot*: "puoi descriverti brevemente per un articolo?", la risposta: «sono un modello di linguaggio addestrato da OpenAI e sono stato progettato per aiutare le persone a rispondere alle loro domande e fornire informazioni su una vasta gamma di argomenti. Sono in grado di capire e rispondere a domande in modo naturale, utilizzando la mia conoscenza di molti argomenti diversi e le mie capacità di comprensione del linguaggio umano. Sono un'intelligenza artificiale e non ho una

sentito a questi modelli, del tipo GPT-3, di incorporare *set* di dati molto più grandi rispetto ai loro predecessori e di impiegare strati molto più profondi di neuroni artificiali per il loro addestramento.

In brevissimo tempo, essendo stata diffusa in Italia a fine novembre 2022, ChatGPT è divenuto un eccezionale fenomeno di massa. Il successo è stato tale che in soli cinque giorni dal lancio si erano già registrati un milione utenti, tanti da mandare in *tilt* il sistema e da non consentire ulteriori registrazioni.

La *Chatbot* è stata diffusa in versione beta e gratuita. L'idea di OpenAI era quella di un *test* su larghissima scala che portasse poi al lancio, avvenuto già da qualche mese negli Stati Uniti, di una versione *premium* il più possibile libera da *bias* cognitivi.

Le potenzialità di questa tipologia di sistemi sono apparse subito molteplici. La capacità di immagazzinare testi estratti dalla rete e di prevedere statisticamente la sequenza di parole o frasi, partendo da un determinato *input*, rendono questi modelli di apprendimento innovativi nel panorama dell'intelligenza artificiale, in quanto capaci di affrontare compiti prima inimmaginabili. Allo stesso tempo, però, sono emerse le prime preoccupazioni, sia per i risvolti legati ad alcune applicazioni in determinati settori sia per la tutela dei diritti, anche fondamentali, degli individui.

Sebbene, infatti, ChatGPT sia stata sviluppata in modo tale da impedire che venga utilizzata per fornire istruzioni pericolose (come ad esempio quelle per creare una bomba o pianificare attentati terroristici) o risultati che inneggiano a posizioni estremistiche, in realtà il sistema possiede questi dati. Alcuni *test* effettuati hanno dimostrato che, ricorrendo ad alcuni accorgimenti linguistici, è possibile ottenere anche questo tipo di informazioni.

A tale proposito, nel giugno 2021, OpenAI ha pubblicato un documento nel quale veniva spiegato quale tecnica venisse impiegata per bloccare contenuti considerati pericolosi. Si tratta di un si-

forma fisica, ma sono disponibile online per aiutare le persone a ottenere le informazioni di cui hanno bisogno. Sono stato progettato per essere utile e rispondere alle domande il meglio possibile, basandomi sul mio addestramento e conoscenze», P. MADOTTO, *ChatGPT, ora basta giocare: ecco utilizzi e rischi (seri)*, in *Agenda Digitale*, 20 gennaio 2023, disponibile *online*.

stema chiamato PALMS che prevede, durante l'addestramento, una fase aggiuntiva finalizzata ad istruire la *chatbot* su quali risposte fornire nel caso in cui il sistema venga interrogato su questioni ritenute sensibili. Dalle prove effettuate è emerso che, se posti dinanzi a domande relative al razzismo o all'omosessualità, i sistemi addestrati con la tecnica PALMS riuscivano a mantenere una sorta di neutralità.

Tuttavia, queste tecniche di filtro introducono, inevitabilmente, in questi modelli dei pregiudizi, già nella fase iniziale, in cui si sceglie cosa debba essere considerato sensibile e cosa no. In pratica, questi sistemi vengono addestrati per riflettere la morale attuale e, dunque, per compiacere le opinioni della società ritenute più eque. In ogni caso, il modello etico viene fornito dagli sviluppatori, ne consegue che il sistema valoriale recepito dal sistema è quello imperante nella comunità in cui è destinato ad operare[113].

Alcune perplessità sono state sollevate anche in ambito didattico ed educativo. I principali timori sono stati sollevati per l'uso improprio che alcuni studenti avevano iniziato a fare di questo strumento, tanto da esserne stato espressamente vietato l'utilizzo nelle scuole pubbliche di New York ed aver dotato alcune strutture di "contro" *software* in grado di individuare testi scritti con ChatGPT. Il dibattito sull'opportunità di vietare l'utilizzo dell'intelligenza artificiale nelle scuole è, al momento presente, più che mai aperto.

Resta il fatto che, per stessa ammissione di OpenAI, ci sono dei possibili profili di rischio nell'utilizzo di ChatGPT tra cui vengono menzionati: la generazione di contenuti falsi o ingannevoli; la diffusione di informazioni non veritiere, di contenuti inappropriati e, ovviamente, i rischi di *bias* cognitivi. La raccomandazione, da parte della casa madre, è ad un utilizzo responsabile che passi da una puntuale verifica dell'affidabilità delle fonti e delle informazioni generate dal modello algoritmico.

OpenAI mette altresì in guardia dai rischi che ChatGPT potrebbe generare per i diritti delle persone, in particolare per la tutela della privacy e per i possibili esiti discriminatori. Sebbene

[113] Si rimanda a *infra* cap. V per approfondimenti sul tema della non discriminazione.

quest'ultimo profilo abbia un peso specifico rilevante, si è scelto di trattare questo caso nell'ambito del presente capitolo, in quanto le prime iniziative per arginare e tentare di regolamentare il fenomeno sono state assunte proprio dal Garante italiano per la protezione dei dati.

Con provvedimento del 30 marzo 2023[114], infatti, l'Autorità italiana è intervenuta, in via d'urgenza, nei confronti di OpenAI, individuata quale titolare del trattamento dei dati personali effettuato attraverso l'applicazione ChatGPT, ai sensi dell'articolo 58, par. 2, lett. f), del GDPR, e nelle more del completamento della necessaria istruttoria, imponendo la misura della limitazione provvisoria del trattamento di tutti i dati personali degli interessati stabiliti nel territorio italiano.

In particolare, il Garante ha agito, come si legge nel provvedimento, avendo rilevato la mancanza di un'informativa privacy da fornire agli utilizzatori e agli interessati, idonea a spiegare le finalità del trattamento effettuato da OpenAI (che poi è proprio quella di addestramento dell'algoritmo che consente il funzionamento di ChatGPT) e la base giuridica che legittima il trattamento dei dati raccolti. Ancora più grave, secondo l'Autorità, è l'assenza di qualsivoglia procedura idonea a stabilire l'età degli utilizzatori del servizio che, secondo i termini pubblicati dalla stessa OpenAI, dovrebbe essere riservato a soggetti che abbiano compiuto almeno i tredici anni. Non essendo previsti meccanismi di controllo, il Garante rileva che l'assenza di filtri potrebbe esporre i minori a risposte non idonee, in considerazione del grado di maturità e autoconsapevolezza raggiunti[115].

In seguito al provvedimento dell'Autorità italiana, OpenAI ha

[114] Provvedimento n. 112 del 30 marzo 2023, disponibile *online* sul sito del GDPD.

[115] Il Garante, quindi, ha rilevato che il trattamento effettuato da OpenAI si è posto in contrasto con gli articoli 5, 6, 8, 13 e 25 del GDPR che regolano rispettivamente: i principi applicabili al trattamento di dati personali (art. 5); la liceità del trattamento (art. 6); le condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (art. 8); Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (art. 13); *Privacy by design* e *Privacy by default* (art. 25).

risposto con una lettera in cui ha manifestato la propria disponibilità a collaborare, al fine di adottare le misure necessarie per risultare in *compliance* con la disciplina *privacy* europea e con quanto indicato dal Garante in merito al trattamento dei dati degli utenti italiani.

I termini della questione sono stati discussi nel corso di un incontro svoltosi *online* a cui hanno preso parte, oltre al Collegio dell'Autorità garante[116], i vertici di OpenAI[117], all'esito del quale, la società si è detta disposta ad introdurre delle misure correttive. Nell'occasione è stata presentata una lista di possibili soluzioni da implementare per rendere ChatGPT conforme alle previsioni del GDPR.

Per parte sua, il Garante, in modo significativo, pur sottolineando come non vi sia alcuna intenzione di porre un freno allo sviluppo dell'intelligenza artificiale e all'innovazione tecnologica, ha ribadito l'importanza che tale sviluppo avvenga nel pieno rispetto delle norme poste a tutela dei dai personali dei cittadini italiani ed europei.

Dopo un primo esame delle allegazioni istruttorie presentate da OpenAI, l'Autorità, con ulteriore provvedimento[118], ha sospeso le determinazioni precedentemente assunte e ha ingiunto a OpenAI di attuare una serie di misure e prescrizioni, ai sensi dell'articolo 58, paragrafo 2, lettera d), del GDPR. In particolare, è stato intimato alla società di pubblicare sul proprio sito internet un'informativa *privacy* estesa idonea a rendere edotti gli utilizzatori e gli interessati che si collegano dall'Italia, del fatto che i dati sono raccolti e trattati ai fini di addestramento degli algoritmi, illustrando le modalità del trattamento, la logica sottesa al funzionamento del servizio, i diritti loro spettanti in qualità di interessati e ogni altra informazione obbligatoriamente richiesta dal GDPR. Il Garante ha altresì richiesto alla società americana di prevedere strumenti utili a consentire agli

[116] Composto da Pasquale Stanzione, Ginevra Cerrina Feroni, Agostino Ghiglia e Guido Scorza.

[117] Sam Altman, CEO di OpenAI, Che Chang, *Deputy General Counsel*, Anna Makanju, *Public Policy Manager* e Ashley Pantuliano, *Associate General Counsel*.

[118] Provvedimento n. 114 dell'11 aprile 2023, disponibile *online* sul sito del GDPD.

utilizzatori e agli interessati, anche non utilizzatori, di esercitare in modo semplice e accessibile, il diritto di opposizione rispetto al trattamento dei loro dati personali per tale finalità.

Ad OpenAI, per poter riattivare il servizio in Italia, è stato altresì richiesto di modificare la base giuridica del trattamento, eliminando ogni riferimento all'esecuzione di un contratto e indicando, invece, in applicazione del principio di *accountability*, il consenso o il legittimo interesse quale base del trattamento, con tutti gli obblighi connessi in termini di redazione di un eventuale *data protection impact assessment*.

Per quanto riguarda la verifica dell'età dei minori, oltre all'immediata implementazione di un sistema di richiesta dell'età ai fini della registrazione al servizio, l'Autorità ha ordinato a OpenAI di predisporre un piano di azione che preveda, al più tardi entro il 30 settembre 2023, l'implementazione di un sistema di *age verification*, in grado di escludere l'accesso agli utenti infratredicenni e ai minorenni, in assenza di un'espressa manifestazione di volontà da parte di chi esercita sugli stessi la responsabilità genitoriale.

Da ultimo, alla società americana è stato richiesto di promuovere, di concerto con il Garante, una campagna di informazione su tutti i principali mezzi di comunicazione di massa italiani, finalizzata ad informare le persone dell'avvenuta probabile raccolta dei loro dati personali ai fini di addestramento degli algoritmi.

V'è da dire che, sebbene l'Autorità italiana sia stata la prima a muoversi, già altre autorità, di diversi Paesi membri, avevano sollevato talune perplessità su ChatGPT.

A motivo di ciò, le autorità nazionali, riuniti nel Comitato europeo per la protezione dei dati (EDPB), hanno deciso di lanciare, sulla base dell'articolo 65 del GDPR, una *task force* congiunta con l'obiettivo di promuovere la cooperazione e lo scambio di informazioni su eventuali iniziative intraprese a livello interno, come accaduto nel caso italiano, al fine di garantire la corretta applicazione del GDPR, con l'obiettivo di monitorare da vicino questi sistemi[119].

[119] Cfr. https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.

I rilievi del Garante italiano appaiono parzialmente condivisibili.

La totale assenza di una informativa *privacy*, idonea a rendere noto agli utilizzatori e agli interessati che i loro dati loro venissero utilizzati eminentemente a fine di addestramento degli algoritmi, non appare giustificabile e rappresenta una grave mancanza di trasparenza da parte di OpenAI. Così come, l'assenza di qualsivoglia controllo sul possibile utilizzo del servizio da parte di minori di tredici anni, per cui appare certamente opportuno l'obbligo di prevedere un sistema di *age verification*.

Al contrario, non convince la richiesta del Garante di organizzare una campagna informativa da trasmettere sui principali media nazionali. Una richiesta che appare obiettivamente eccessiva, sotto diversi punti di vista e che sembra tradire una difficoltà nel gestire la situazione. Chiedere di organizzare una campagna pubblicitaria da trasmettere sui principali media, innanzitutto, fornirebbe a ChatGPT una maggiore visibilità e, di conseguenza, un bacino di utenza molto più ampio. Considerando che ancora persistono dei dubbi su come OpenAI utilizzi realmente i dati raccolti e sulle eventuali implicazioni di tale trattamento, non sembra una strategia adeguata, laddove l'obiettivo finale sia la protezione dei diritti fondamentali degli individui. Da ultimo, questa richiesta sembrerebbe suggerire che l'Autorità voglia costringere OpenAI ad una pubblica assunzione di responsabilità, che non sembra però né utile né funzionale allo scopo di proteggere gli utilizzatori e gli interessati.

Occorrerà attendere per capire come evolverà la questione, anche a livello europeo e nei confronti dei nuovi programmi di intelligenza artificiale generativa che sono tuttora in fase di sviluppo. Tutte le *Big Tech*, infatti, stanno lavorando alacremente alla loro "personale versione di ChatGPT", nessuno intende rimanere indietro.

Nel frattempo, sottolineando una particolare solerzia da parte di OpenAI, il servizio è stato ripristinato in Italia, posto che la società statunitense si è conformata alle condizioni che il Garante le aveva imposto, almeno in questa fase iniziale[120].

[120] Nella pagina al posto del messaggio che annunciava l'impossibilità per gli utenti italiani di accedere al servizio si legge ora: «Welcome back, Italy! We're

Qualche considerazione appare necessaria, anche in merito all'effettività dei primi rimedi introdotti. In particolare, il sistema di verifica dell'età implementato, seppur ci si augura provvisorio in attesa di una procedura di *age verification* più strutturata, appare obiettivamente inadeguato. In pratica altro non è che un *banner* dove si legge «to continue on ChatGPT, please confirm that you are 18+ or are 13+ and have consent from your partner or gurdian to use ChatGPT». Per un utente dodicenne, o anche di età inferiore, è sufficiente flaggare la casella di conferma per poter accedere, senza restrizioni e senza difficoltà, al servizio. Non pare che quello introdotto da OpenAI possa considerarsi un rimedio effettivo. Se davvero si intende bloccare l'utilizzo di questi sistemi ai minori di anni tredici, occorre prevedere una procedura di verifica dell'età che risulti davvero idonea allo scopo e non basterà, a questo fine, un comune *banner* semplicissimo da aggirare da qualsiasi minore con un minimo di alfabetizzazione informatica.

pleased to resume offering ChatGPT in Italy. To continue on ChatGPT, please confirm that you are 18+ or are 13+ and have consent from your partner or gurdian to use ChatGPT. For information about how we collect and use personal data, please see our Privacy policy. For information about how we develop and train ChatGPT, please see this help center article».

CAPITOLO QUINTO

INTELLIGENZA ARTIFICIALE E DIVIETO DI DISCRIMINAZIONE

SOMMARIO. 1. Introduzione. – 2. Il divieto di discriminazione nel diritto internazionale. – 2.1. *Segue.* Il divieto di discriminazione nel sistema del Consiglio d'Europa. – 2.2. *Segue.* Le norme che regolano il principio di non discriminazione nell'Unione europea. – 3. *Bias*, e *math washing*: la non discriminazione alla prova dell'intelligenza artificiale. – 4. Discriminazione basata sull'etnia: il caso degli Uyghur. – 5. Discriminazione basata sul genere con particolare riguardo all'accesso al mercato del lavoro e all'istruzione. – 6. Discriminazioni basate sulla razza: il rischio di procedure elettorali inique e la pratica del *Gerrymandering*, la valutazione del rischio di recidiva penale e i pericoli evidenziati nell'utilizzo dell'algoritmo COMPAS. – 7. Discriminazioni basate su religione, credenze e opinioni politiche. – 8. Conclusioni.

1. Introduzione

All'interno del capitolo precedente, sono stati messi in luce i possibili rischi che le tecnologie di intelligenza artificiale potrebbero comportare per la tutela della *privacy*.

Nel corso di tale analisi, a dimostrazione di quanto le problematiche siano tra loro strettamente interconnesse, sono emersi anche profili di rischio per taluni individui legati a possibili discriminazioni che potrebbero derivare dai dati concretamente utilizzati per istruire i sistemi algoritmici.

Potrebbe infatti accadere, come si avrà modo di evidenziare nei paragrafi che seguono, che la tecnologia venga utilizzata in modo non equo e restituisca dei risultati discriminatori. È molto preoccupante che tale circostanza possa accadere non solo – o almeno non necessariamente – quando i dati utilizzati risultino *ab origine* discriminatori. Invero, è stato rilevato, che i sistemi di intelligenza artificiale possono facilmente replicare i pregiudizi presenti all'in-

terno dei dati di addestramento se la tecnologia non è sottoposta ad un rigoroso processo di controllo in fase di progettazione e, soprattutto, se non viene utilizzata in modo adeguato e consapevole. A titolo esemplificativo, un algoritmo di riconoscimento facciale che sia stato addestrato su un insieme di dati raccolti principalmente da persone appartenenti ad una determinata razza o genere potrebbe avere difficoltà a riconoscere persone di altre razze o generi e, dunque, discriminarli. Invero, può accadere che le analisi predittive creino discriminazioni all'interno della società legate a età, etnia, lingua, soprattutto a danno delle categorie più deboli.

Da un punto di vista generale, la discriminazione, prendendo in prestito le parole di Lochak, è in sostanza, «la distinction ou la différence de traitement illégitime: illégitime car arbitraire, et interdite puisqu'illégitime»[1].

Il termine "discriminazione" può essere inteso in senso sia estensivo sia riduttivo: nel primo caso, sarà considerata discriminatoria qualsiasi differenza di trattamento che non sia giustificata da una differenza di situazioni di partenza[2]. Nel secondo caso, al contrario, si parlerà di discriminazione per indicare un trattamento sfavorevole riservato a persone appartenenti a gruppi particolarmente vulnerabili proprio in ragione della loro appartenenza a tale gruppo, generalmente definito da una particolare caratteristica (genere, razza o origine etnica, disabilità, orientamento sessuale)[3].

Chiaramente, quando si tratta di discriminazioni dirette, comunque di per sé vietate, tutto risulta più semplice perché la "lesione" è facilmente identificabile, così come l'individuo o la categoria di soggetti lesi.

Appare evidente, che le discriminazioni di tipo diretto siano anche quelle che pongono minori problemi da un punto di vista giu-

[1] V. D. LOCHAK, *Réflexion sur la notion de discrimination,* in *Droit social*, 1987, pp. 778-790.

[2] ID., cit., p. 18 «toute différence de traitement qui n'est pas justifiée par une différence de situation».

[3] ID., cit., p. 19 «le traitement défavorable dont sont victimes des personnes particulièrement vulnérables en raison de leur appartenance à un groupe défini par une caractéristique particulière (le sexe, la race ou l'origine ethnique, le handicap, l'orientation sexuelle…)».

ridico e pratico. Dalla prima prospettiva, in quanto devono considerarsi *tout court* illegittime e, dunque, vietate, dal lato pratico poiché, essendo facilmente individuabili ed identificabili, potrebbero essere evitate tentando di programmare gli algoritmi in modo equo, già nelle primissime fasi di sviluppo e di implementazione, in modo che non basino le decisioni elaborate – almeno non unicamente – su determinate caratteristiche[4].

Il problema si complica in relazione a caratteri formalmente e apparentemente neutrali, ma che ricorrono con frequenza in determinate categorie di soggetti o che, comunque, indirettamente, sono idonei ad identificare determinate categorie. Si pensi al codice fiscale come indicativo dell'appartenenza ad una certa comunità. Il sistema di apprendimento, in questi casi, potrebbe attuare dei collegamenti basati su associazioni di dati che se dovessero condurre a risultati discriminatori risulterebbero più insidiosi e di difficile rilevazione[5].

Stratificando i dati, con il moltiplicarsi delle connessioni associative, il rischio è che, anche intervenendo per eliminare eventuali decisioni discriminatorie più prossime, diventi difficile o quasi impossibile risalire indietro fino a quelle più distanti, a loro volta, magari, basate su decisioni del passato ugualmente discriminatorie.

D'altronde, gli algoritmi funzionano partendo da una preselezione di dati basati sullo storico e producono calcoli statistici. La stessa etimologia della parola "algoritmo" rimanda a "stato, situazione o condizione di una cosa"[6] per questo è stato osservato che "this reliance on past practices or assessments may be based on exclusion and prejudice and lead to unfair discrimination"[7] .

La decisione presa statisticamente, anche sulla base di un algoritmo perfettamente funzionante, potrebbe non risultare corretta, soprattutto in relazione al singolo caso, dato che la statistica forni-

[4] P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in *Consulta online*, 2020, pp. 1-19.

[5] Si veda S. TOMMASI, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, cit., pp. 112-119.

[6] G. CAPORALE, *Corso di statistica teorico-pratica*, Napoli, 1976.

[7] G. SARTOR, *Artificial Intelligence: Challenges for EU Citizens and Consumers. Briefing. Requested by the IMCO committee*, 2019, pp. 1-7, disponibile *online*.

sce delle indicazioni tanto più attendibili se calibrate su un effetto complessivo e non isolato[8].

La ricostruzione di tendenze predittivamente rilevanti avviene a partire dalle occorrenze empiriche esistenti. I sistemi algoritmici hanno la tendenza a "codificare" il passato, ingabbiando soluzioni e predizioni all'interno di "scatole" di dati forniti dai trascorsi storici elaborati attraverso la lente delle logiche che hanno accompagnato la programmazione del sistema. Ciò significa, in altre parole, che una determinata situazione tende a essere cristallizzata nel processo prognostico, influenzandone i risultati ed orientando, in modo più o meno importante, le decisioni prese a valle della valutazione automatizzata[9].

Ne consegue che i sistemi di intelligenza artificiale possono essere discriminatori non perché il sistema sia di per sé "cattivo", ma perché eredita comportamenti sbagliati che poi ripete. Gli algoritmi, infatti, funzionano secondo la logica *garbage in – garbage out*, per cui dati incongrui, inesatti o non aggiornati non possono che produrre risultati decisionali inaffidabili, creando delle vere e proprie trappole, spesso per lo più invisibili. Anche da comportamenti assolutamente innocenti e ordinari possono essere dedotte connessioni sorprendentemente precise su preferenze e attitudini[10].

Si è avvertito, con un paragone suggestivo, che «algorithms are a lot like magical illusions. At first they appear to be nothing short

[8] Insegnano gli statistici che: «il calcolo delle probabilità, e la statistica a mezzo del calcolo delle probabilità, anche se applicati a masse di casi, non possono mai portare a conclusioni sicure, ma solo a conclusioni probabili. Possono legittimare dei dubbi più o meno forti - e questa è certamente una funzione utile - ma non possono mai scioglierli in modo definitivo. Possono fornire non "testi di significatività", ma "elementi di sospetto"» così C. GINI, *I pericoli della Statistica*, cit., p. 39.

[9] G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza. Politica del diritto*, 2019, pp. 199- 236.

[10] E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation,* in *Nuove leg. civ. comm.*, 2018, pp. 1209-1235.

of wizardry, but as soon as you know how the trick is done, the mystery evaporates»[11].

Nella realtà si è già disegnato un quadro preoccupante di quelli che sono i casi di discriminazione algoritmica che si sono verificati mediante l'utilizzo di sistemi di intelligenza artificiale in diversi settori. Studi di estrazione di testo, ad esempio, hanno dimostrato l'associazione di determinate parole con stereotipi diffusi di genere e di razza[12].

È lungo questa linea direttrice, pertanto, che si svilupperà il presente capitolo, non prima però di aver delineato l'attuale quadro giuridico che regola il divieto di discriminazione in ambito internazionale ed europeo.

2. Il divieto di discriminazione nel diritto internazionale

In aggiunta ai meccanismi elaborati all'interno di diversi contesti regionali, tra cui quelli europei che si esamineranno a breve[13], il principio di non discriminazione, quale declinazione del più generale principio di uguaglianza[14], è contemplato in diversi strumenti di protezione dei diritti umani in ambito internazionale[15].

Nella specie, ai sensi di quanto dispone la Carta delle Nazioni Unite[16] all'interno dell'articolo 55, il «rispetto e l'osservanza universale dei diritti dell'uomo e delle libertà fondamentali per tutti, sen-

[11] H. FRY, *Don't Believe the Algorithm*, in *The Wall Street Journal*, Sept. 5, 2018, disponibile *online*.

[12] A. CALISKAN, J. BRYSON, A. NARAYANAN, *Semantics derived automatically from language corpora contain human-like biases. Science*, 2017, pp. 183-186.

[13] Si veda *infra, in questo capitolo,* par. 2.2.

[14] Cfr. G. TESAURO, *Eguaglianza e legalità nel diritto comunitario [Relazione presentata al Convegno dell'Associazione italiana dei Costituzionalisti, Trieste, 17-19 dicembre 1998*], in *Il diritto dell'Unione europea*, 1999, pp. 1-19.

[15] Si vedano *ex multis* M. BARBERA, *Principio di eguaglianza e divieti di discriminazione*, in M. Barbera, A. Guariso (a cura di), *La tutela antidiscriminatoria. Fonti, strumenti, interpreti,* Torino, 2019, p. 5 ss.

[16] Carta delle Nazioni Unite adottata a San Francisco il 26 giugno 1945.

za distinzione di razza, sesso, lingua o religione» rientra tra i compiti fondamentali dell'organizzazione.

La Dichiarazione universale dei diritti dell'uomo contiene diverse disposizioni in tema di non discriminazione. In particolare, all'interno dell'articolo 2 è contenuta una previsione generale che stabilisce il diritto di ciascun individuo a vedersi riconosciuti e garantiti tutti i diritti e le libertà enunciati nella Dichiarazione, senza distinzione alcuna[17]. La previsione è altresì completata da quanto dispone l'articolo 7, che riconosce l'uguaglianza di tutti dinanzi alla legge senza distinzione alcuna e il diritto a ricevere eguale tutela contro ogni discriminazione ma anche contro qualsiasi incitamento alla discriminazione.

Norme analoghe sono presenti anche in ulteriori atti, quali il Patto internazionale sui diritti civili e politici[18], il Patto internazionale sui diritti economici, sociali e culturali[19] ma anche in accordi più specifici.

[17] L'articolo 2 recita «tutti i diritti e tutte le libertà enunciate nella presente Dichiarazione, senza distinzione alcuna, per ragioni di razza, di colore, di sesso, di lingua, di religione, di opinione politica o di altro genere, di origine nazionale o sociale, di ricchezza, di nascita o di altra condizione. Nessuna distinzione sarà inoltre stabilita sulla base dello statuto politico, giuridico o internazionale del paese o del territorio cui una persona appartiene, sia indipendente, o sottoposto ad amministrazione fiduciaria o non autonomo, o soggetto a qualsiasi limitazione di sovranità».

[18] Patto internazionale sui diritti civili e politici, adottato dall'Assemblea Generale delle Nazioni Unite il 16 dicembre 1966, entrato in vigore il 23 marzo 1976, all'articolo 26 si prevede che «tutti gli individui sono eguali dinanzi alla legge e hanno diritto, senza alcuna discriminazione, ad una eguale tutela da parte della legge. A questo riguardo, la legge deve proibire qualsiasi discriminazione e garantire a tutti gli individui una tutela eguale ed effettiva contro ogni discriminazione, sia essa fondata sulla razza, il colore, il sesso, la lingua, la religione, l'opinione politica o qualsiasi altra opinione, l'origine nazionale o sociale, la condizione economica, la nascita o qualsiasi altra condizione».

[19] Patto internazionale sui diritti economici, sociali e culturali, adottato dall'Assemblea Generale delle Nazioni Unite il 16 dicembre 1966, entrato in vigore il 3 gennaio 1976 che all'articolo 2 chiarisce che «Gli Stati parti del presente Patto si impegnano a garantire che i diritti in esso enunciati verranno esercitati senza discriminazione alcuna, sia essa fondata sulla razza, il colore, il sesso, la lingua, la religione, l'opinione politica o qualsiasi altra opinione, l'origine nazionale o sociale, la condizione economica, la nascita o qualsiasi altra condizione».

Considerato che il divieto di discriminazione nasce, in origine, per proteggere i gruppi di minoranze lasciati senza adeguata tutela, non sorprende che il primo Trattato delle Nazioni Unite su questo tema abbia riguardato proprio le discriminazioni in ragione della razza[20].

In seguito, nel 1979, è stata approvata la Convenzione sull'eliminazione di ogni forma di discriminazione contro le donne[21] mentre, nel 1989, è stata la volta della Convenzione sui diritti del fanciullo[22]. A seguire, più di recente, è stata approvata la Convenzione sui diritti delle persone con disabilità[23].

Tutti questi atti sono tesi a tutelare soggetti o categorie deboli da possibili forme di discriminazione.

Chiaramente, anche il mercato del lavoro è un terreno molto delicato all'interno del quale è particolarmente facile riscontrare casi di trattamenti ingiustificatamente discriminatori a carico dei lavoratori. A motivo di ciò, in molti degli atti in questo settore si ritrova un'enunciazione comune che obbliga gli Stati contraenti a garantire e rispettare i diritti dei lavoratori senza distinzione alcuna[24].

[20] Convenzione internazionale sull'eliminazione di ogni forma di discriminazione razziale (ICERD), aperta alle firme e ratificata dall'Assemblea Generale il 21 dicembre 1965 entrata in vigore il 4 gennaio 1969. La Convenzione definisce discriminazione razziale «ogni distinzione, esclusione, limitazione o preferenza basata sulla razza, il colore della pelle, la discendenza o l'origine nazionale o etnica, che abbia lo scopo o l'effetto di annullare o compromettere il riconoscimento, il godimento o l'esercizio, in condizioni di parità, dei diritti umani e delle libertà fondamentali in campo politico, economico, sociale e culturale o in ogni altro ambito della vita pubblica". L'articolo 2 proibisce la discriminazione razziale e obbliga le parti "a continuare, con tutti i mezzi adeguati e senza indugio, una politica tendente ad eliminare ogni forma di discriminazione razziale" e a "favorire l'intesa tra tutte le razze».

[21] La Convenzione CEDAW, ripropone la stessa definizione di "discriminazione" introdotta precedentemente dall'IRCED. Nell'ambito di entrambe le convenzioni è stata prevista la creazione di un comitato di controllo.

[22] Convenzione internazionale sui diritti dell'infanzia e dell'adolescenza (1989) Adottata dall'Assemblea Generale delle Nazioni Unite con Risoluzione 44/25 del 20 novembre 1989 ed entrata in vigore il 2 settembre 1990.

[23] Adottata dall'Assemblea Generale delle Nazioni Unite con Risoluzione 61/106 del 13 dicembre 2006 ed entrata in vigore il 3 maggio 2008.

[24] «Come quella di sesso, di razza, di colore, di lingua, di religione o di con-

Tra gli strumenti di *soft law* in materia di non discriminazione meritano inoltre di essere ricordate: la Dichiarazione sulla razza e il pregiudizio razziale del 1978, la Dichiarazione sull'eliminazione di ogni forma di intolleranza e di discriminazione basata sulla religione o le convinzioni personali del 1981, la Dichiarazione sui diritti delle persone appartenenti a minoranze nazionali o etniche, religiose e linguistiche del 1992, e la Dichiarazione sui diritti delle popolazioni indigene del 2007.

Sebbene si tratti di testi non vincolanti, tutti contengono importanti principi volti a supportare la lotta contro le discriminazioni.

Vale la pena sottolineare, che tutti gli Stati membri dell'Unione europea sono attualmente parti contraenti di molte delle convenzioni appena ricordate.

2.1. Segue. *Il divieto di discriminazione nel sistema del Consiglio d'Europa*

Anche all'interno del sistema del Consiglio d'Europa vi sono diversi testi che contemplano un generale divieto di discriminazione[25].

vinzione, di opinione politica o di altro tipo, di origine nazionale, etnica o sociale, di nazionalità, di età, di posizione economica, di proprietà, di stato civile, di nascita o di altra condizione». Così recita l'art. 7 della Convenzione internazionale sulla protezione dei diritti dei lavoratori migranti e dei membri delle loro famiglie, Adottata dall'Assemblea Generale delle Nazioni Unite con risoluzione 45/158 del 18 dicembre 1990 ed entrata in vigore il 1° luglio 2003.

[25] M. BALBONI (a cura di), *The ECHR and the Principle of Non-discrimination*, in *La Ricerca del Diritto nella Comunità internazionale*, Napoli, 2017, p. 20 ss.; A. SACCUCCI, *Profili di tutela dei diritti umani tra Nazioni Unite e Consiglio d'Europa*, Padova, 2005, p. 180 ss. e spec. p. 189; E. CARPANO, *État de droit et droits européens. L'évolution du modèle de l' État de droit dans la cadre de l'européanisazion des systèmes juridiques*, Paris-Budapest-Torino, 2005, p. 437. Nello specifico, sul tema della revisione della Carta sociale europea, si veda F. OLIVERI, *La Carta sociale europea tra enunciazione dei diritti, meccanismi di controllo e applicazione nelle corti nazionali. La lunga marcia verso l'effettività*, in *Rivista del Diritto della Sicurezza Sociale*, n. 3, 2008, pp. 509-539.

Ovviamente, per cominciare, la Convenzione europea dei diritti dell'uomo che, all'articolo 14, garantisce la parità di trattamento nel godimento dei diritti senza nessuna discriminazione[26].

Il protocollo XII del 2000 alla CEDU, inoltre, amplia la portata del divieto di discriminazione, alla parità di trattamento nel godimento di ogni diritto, compresi quelli previsti dalle legislazioni nazionali[27].

Chiaramente, la tutela apprestata tanto dall'articolo 14, quanto dal protocollo n. XII, resta confinata nell'ambito del sistema CEDU ed è invocabile solo in relazione al godimento di altri diritti fondamentali tutelati[28]. Secondo quanto più volte chiarito dalla

[26] Articolo 14: «Il godimento dei diritti e delle libertà riconosciuti nella presente Convenzione deve essere assicurato senza nessuna discriminazione, in particolare quelle fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o quelle di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione».

[27] L'articolo 1 dispone che «Il godimento di ogni diritto disposto da una legge sarà garantito senza alcuna discriminazione per motivi di sesso, razza, colore, lingua, religione, opinione politica o altra opinione, origine nazionale o sociale, associazione ad una minoranza nazionale, proprietà, nascita o ogni altra condizione». All'interno della relazione esplicativa, Protocollo n. 12 alla convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (STE n. 177), relazione esplicativa, punto 22, viene chiarito che la tutela si estende a situazioni che comportano delle discriminazioni: «i) nel godimento di ogni diritto specificamente riconosciuto a una persona dal diritto nazionale; ii) nel godimento di ogni diritto derivante da un chiaro obbligo di un'autorità pubblica in forza del diritto nazionale, cioè nel caso in cui, ai sensi del diritto nazionale, tale autorità sia tenuta a comportarsi in un determinato modo; iii) da parte di un'autorità pubblica nell'esercizio del potere di discrezionalità (per esempio, la concessione di determinati sussidi); iv) mediante altre azioni od omissioni da parte di un'autorità pubblica (per esempio, il comportamento dei funzionari responsabili dell'applicazione della legge quando intervengono per sedare una sommossa)». Sempre nella relazione esplicativa, cit., punto 28, viene evidenziato che sebbene l'effetto della tutela dovrebbe essere di tipo verticale, cioè a garantire la tutela dei singoli contro le discriminazioni delle autorità pubbliche, in qualche modo riguarda anche i rapporti orizzontali tra privati che di norma rientrano nel campo delle normative nazionali.

[28] Si veda per alcune riflessioni di ordine generale il commento di U. VILLANI, *Il Protocollo n. 14 alla Convenzione europea dei diritti dell'uomo,* in *La Comunità internazionale*, 2004, p. 487.

Corte stessa, infatti, l'articolo 14 non ha un'esistenza indipendente, in quanto vale unicamente per «il godimento dei diritti e delle libertà» sanciti dalla Convenzione. Motivo per cui, le doglianze mosse sotto il profilo dell'articolo 14, generalmente, andrebbero formulate in combinato disposto con le altre norme che, all'interno della Convenzione, disciplinano diritti sostanziali.

Nonostante tale orientamento, v'è da dire che la Corte EDU, per non sminuire la portata e l'efficacia dell'articolo 14 e del principio di non discriminazione, si è spesso trovata a precisare che quest'ultimo può essere invocato anche in mancanza di una specifica violazione delle norme convenzionali a carattere sostanziale e che, in tale misura, possiede una portata autonoma, sebbene non possa trovare applicazione se i fatti della controversia non abbiano almeno ad oggetto uno o più diritti sostanziali tutelati dalla Convenzione[29].

D'altronde, la giurisprudenza della Corte EDU ha mostrato nel tempo una tendenza all'interpretazione estensiva per tutti i diritti tutelati all'interno della Convenzione e non solo con riferimento alla portata materiale ma anche per ciò che riguarda i profili della competenza giurisdizionale.

A tale ultimo riguardo, infatti, l'articolo 1 stabilisce che ogni persona soggetta alla giurisdizione di uno Stato membro, possa godere dei diritti sanciti dalla stessa. Ne consegue, secondo la formula particolarmente ampia di tale articolo e nel rispetto dello spirito che ha dato origine alla CEDU, che l'applicazione *ratione loci* è assicurata in modo aperto e onnicomprensivo, posto che per godere dei diritti sanciti dalla Convenzione è sufficiente trovarsi nella giurisdizione di uno qualsiasi degli Stati contraenti. La nozione di giurisdizione è stata oggetto di interpretazione ulteriormente estensiva da parte della Corte EDU che, nel corso del tempo, ha ampliato le

[29] *Ex multis,* Corte EDU, 7 gennaio 2014, *Cusan e Fazzo contro Italia*, § 54; ID., 7 febbraio 2013, *Fabris contro Francia*, § 47; ID., 22 marzo 2012, *Konstantin Markin contro Russia*, § 124; ID., 20 giugno 2006, *Zarb Adami contro Malta*, § 42; ID., 27 marzo 1998, *Petrovic contro Austria*, § 22; ID., 21 febbraio 1997, *Van Raalte contro Paesi Bassi*, § 33.

maglie delle tutele garantite dalla Convenzione[30], incrementando la portata dei diritti in essa sanciti.

L'altro testo generale di riferimento all'interno del sistema del Consiglio d'Europa a cui è affidata la tutela dei diritti fondamentali è la Carta Sociale Europea[31], sottoposta a revisione completa nel 1996[32]. A differenza della precedente versione del 1961[33], la nuova

[30] Nell'applicazione dell'articolo 14 la Corte EDU ha fornito un'interpretazione estensiva dei diritti sanciti dalla CEDU: in primo luogo, ha precisato che i ricorsi basati sull'articolo 14 possono essere esaminati in relazione a un diritto sostanziale, ancorché non sussista un'effettiva violazione del diritto sostanziale di per sé considerato (Cfr., ad esempio, Corte EDU, *Sommerfeld c. Germania* [GC], n. 31871/96, 8 luglio 2003. Cfr., ad esempio, Id., A.*H. e a. c. Russia*, n. 6033/13 e 15 altre istanze, 17 gennaio 2017, punto 380 e ss.); in secondo luogo, ha affermato che la portata di una doglianza per discriminazione può ricadere nell'ambito di un determinato diritto, ancorché la fattispecie non verta di per sé su di uno specifico diritto sancito dalla CEDU. In questi casi è sufficiente che la fattispecie sia genericamente ricollegabile ad aspetti protetti dalla Convenzione Corte EDU, *Zarb Adami c. Malta*, n. 17209/02, 20 giugno 2006; Corte EDU, *Khamtokhu e Aksenchik c. Russia* [GC], nn. 60367/08 e 961/11, 24 gennaio 2017, punto 58.

[31] Consiglio d'Europa, Carta sociale europea, STCE n. 163, Strasburgo, 3 maggio 1996. La Carta presenta una struttura articolata in 6 parti: la I e la II enunciano rispettivamente i diritti, che costituiscono gli obiettivi da raggiungere, e le obbligazioni corrispondenti, che lo Stato si impegna a rispettare al fine di conferire effettività alle situazioni giuridiche. La III indica gli impegni che gli Stati contraenti devono necessariamente accettare come vincolanti; la IV appresta la disciplina sulle procedure di controllo sull'attuazione dei diritti e rinvia al Protocollo che istituisce il sistema dei reclami collettivi; la V contiene un'importante clausola generale di non discriminazione (art. E), una nuova procedura di emendamento (art. J) e disposizioni relative agli strumenti di attuazione a livello nazionale dei diritti economici e sociali (con leggi, regolamenti, accordi di categoria e ogni altro mezzo appropriato); la VI stabilisce il regime giuridico della Carta riveduta (firma, ratifica, adesione, entrata in vigore ecc.).

[32] La versione del 1996 della Carta sociale europea prevede il diritto alla parità di trattamento in materia di lavoro e professione, senza discriminazioni basate sul sesso. Ulteriori tutele contro la discriminazione sono previste dalla Convenzione quadro per la protezione delle minoranze nazionali, dalla Convenzione del CDE sulla lotta contro la tratta degli esseri umani e dalla Convenzione del CDE sull'accesso ai documenti ufficiali; dal protocollo addizionale alla Convenzione sulla criminalità informatica.

[33] Consiglio d'Europa, Carta sociale europea, STCE n. 35, Torino, 18 ottobre 1961.

stesura contiene un articolo E[34], che ricorda molto nella formulazione e nei contenuti l'articolo 14 della CEDU, e che, proprio come quest'ultimo, vieta esplicitamente ogni forma di discriminazione, a prescindere dalle situazioni di partenenza e dalle appartenenze[35].

In un'ottica più settoriale, sempre in seno al sistema del Consiglio d'Europa, ulteriori tutele contro la discriminazione sono previste nella Convenzione quadro per la protezione delle minoranze nazionali[36], nella Convenzione sulla lotta contro la tratta degli esseri umani[37] e nella Convenzione sull'accesso ai documenti ufficiali[38].

Un divieto di discriminazione è altresì previsto nel Protocollo alla Convenzione sulla criminalità informatica[39] e nella Convenzione di Istanbul sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica[40].

La circostanza che una previsione in tema di non discriminazio-

[34] Articolo E - *Non discriminazione* «Il godimento dei diritti riconosciuti nella presente Carta deve essere garantito senza qualsiasi distinzione basata in particolare sulla razza, il colore della pelle, il sesso, la lingua, la religione, le opinioni politiche o ogni altra opinione, l'ascendenza nazionale o l'origine sociale, la salute, l'appartenenza ad una minoranza nazionale, la nascita o ogni altra situazione».

[35] La Carta, come noto, è suscettibile di creare soltanto obbligazioni per gli Stati, mentre spetta ai singoli legislatori adottare norme interne che possano garantire quegli stessi diritti. Per alcune considerazioni si vedano G. GORI, *Domestic Enforcement of the European Social Charter: The Way Forward*, in G. De Burca, B. De Witte, *Social rights in Europe*, New York, 2005, p. 70-88, spec. p. 76; C. BENELHOCINE, *La charte sociale européenne*, Editions du Conseil de l'Europe, 2011, p. 53-62.

[36] Consiglio d'Europa, *Convenzione quadro per la protezione delle minoranze nazionali (FCNM), STCE* n. 157, 1995. Cfr. articoli 4, 6, paragrafo 2, e 9.

[37] Consiglio d'Europa, *Convenzione sulla lotta contro la tratta di esseri umani, STCE n. 197,* 2005. Cfr. articolo 2, paragrafo 1.

[38] Consiglio d'Europa, convenzione sull'accesso ai documenti ufficiali, STCE n. 205, 2009. Cfr. articolo 2, paragrafo 1.

[39] Consiglio d'Europa, *Protocollo aggiuntivo alla convenzione sulla criminalità informatica relativo alla criminalizzazione degli atti di natura razzista e xenofoba commessi attraverso l'uso di sistemi informatici*, *STE 189*. Cfr. articolo 3, paragrafo 1.

[40] Consiglio d'Europa, *Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, STCE n. 210*, 2011. Cfr. articolo 4.

ne sia inserita in pressocché tutti gli atti che compongono il sistema di tutele delineato all'interno del Consiglio d'Europa dimostra che il principio di non discriminazione rappresenta un elemento primario e costituisce un presupposto necessario per assicurare un'adeguata protezione della persona e, soprattutto, garantire il godimento di tutti gli altri diritti connessi e collegati previsti, a diversi livelli, nel sistema governato dalla CEDU.

2.2. Segue. *Le norme che regolano il principio di non discriminazione nell'Unione europea*

L'azione europea volta a garantire l'uguaglianza e la non discriminazione tra le persone vanta una lunga tradizione[41]. Il processo che ha visto emergere tali diritti non ha però seguito il consueto *iter* della positivizzazione in una norma generale e la successiva declinazione in casi specifici, ma ha subito piuttosto un processo inverso, che si potrebbe definire dal "particolare al generale".

Il Trattato istitutivo CEE[42] prevedeva, all'articolo 119[43], un divieto di discriminazione per nazionalità strumentale a garantire la libera circolazione all'interno del mercato unico. In aggiunta, su insistente richiesta della Francia, che voleva evitare fenomeni di *dumping* sul mercato del lavoro, è stato introdotto uno specifico obbligo di parità retributiva tra uomo e donna[44].

[41] M. BELL, *Anti-discrimination law and the European Union*, Oxford, 2002, p. 43.

[42] V. G. GAJA, A. ADINOLFI, *Introduzione al diritto dell'Unione europea*, cit., spec. cap. I par. 1 e cap. VI par. 3; TESAURO G., *Manuale di diritto dell'Unione europea*, spec. p. 15 ss. e p. 123 ss.

[43] Nonostante la vocazione evidentemente mercantilistica della norma se n'è parlato come di una «oasi sociale» v. J. CRUZ VILLALON, *Lo sviluppo della tutela antidiscriminatoria nel diritto comunitario*, in *Giornale di diritto del lavoro e di relazioni industriali,* 2003, n. 99-100, p. 353. L'A. si riferisce ai divieti di discriminazione salariale in ragione del sesso e della discriminazione a motivo della nazionalità definendole le due uniche "oasi" di socialità nell'ambito della dimensione sociale europea. Si veda altresì M. ROCCELLA, T. TREU, *Diritto del lavoro della Comunità Europea*, Padova, 2002, pp. 203-204.

[44] M. MILITELLO, *Principio di uguaglianza e di non discriminazione tra Costituzione italiana e Carta dei diritti fondamentali dell'Unione Europea* (*artt. 3 Cost.;*

Nonostante lo scopo evidentemente limitato di tale previsione e la connotazione marcatamente economica, è stato osservato che l'articolo 119 ha svolto una funzione «fortemente costituzionale»[45].

Occorre rilevare che, anche in questo caso, l'opera interpretativa della Corte di giustizia ha giocato un ruolo fondamentale[46] precedendo, accompagnando e, all'occorrenza, indirizzando gli interventi del legislatore europeo, riconducibili, nelle primissime fasi, eminentemente al settore giuslavoratistico, con le direttive degli anni '70 sull'attuazione della parità di trattamento con riferimento alla retribuzione, alle condizioni di lavoro e ai regimi di sicurezza sociale.

In seguito, già con il Trattato di Amsterdam, sono stati forniti all'Unione europea nuovi strumenti per realizzare azioni contro qualunque discriminazione basata sul sesso, la razza e l'origine etnica, la religione, le convinzioni, la disabilità, l'età e l'orientamento sessuale.

L'inserimento all'interno del trattato dell'articolo 13 (ora articolo 19 TFUE)[47] e, dal punto di vista del diritto derivato, l'adozione

art. 20 e art. 21 Carta di Nizza), in *Biblioteca '20 Maggio'*, 1, 2010, p. 140, e spec. pp. 160-161, originariamente pubblicato come WP C.S.D.L.E. "Massimo D'Antona". INT – 77/2010.

[45] Cfr. S. SCIARRA, *Integrazione dinamica tra fonti nazionali e comunitarie: il caso del lavoro notturno delle donne*, in *Il diritto del lavoro*, 1995, p. 153; C. BARNARD, *The economic objectivs of art. 119*, in T. Hervey, O'Keeffe (a cura di), *Sex Equality Law in European Union*, 1996, Wiley, 1996, p. 321 ss.

[46] Si veda per tutti la posizione assunta dalla Corte di Giustizia nella sentenza Mangold. In tale occasione la Corte con riferimento alla discriminazione per età ha affermato che «Il principio di non discriminazione in ragione dell'età deve pertanto essere considerato un principio generale del diritto comunitario […]» (punto 75 della sentenza CGCE del 22 novembre 2005, C-144/04, *Werner Mangold c. Rüdiger Helm*). Da questa affermazione, non nuova per la verità, la Corte ne ha fatto discendere una conseguenza inedita per la quale i divieti di discriminazione, in quanto specificazione di un principio di eguaglianza che esiste indipendentemente dalla normazione secondaria, vivono di una vita propria che prescinde dai comportamenti degli Stati e dall'assetto presente e futuro delle competenze sovranazionali. Cfr. in dottrina M. BARBERA, *Il nuovo diritto antidiscriminatorio: innovazione e continuità,* in M. Barbera (a cura di), *Il nuovo diritto antidiscriminatorio*, Milano, 2002, p. XLIII.

[47] L'articolo 13 sta che «fatte salve le altre disposizioni del presente trattato e

delle direttive 78/2000/Ce[48], 43/2000/Ce[49] e 2004/113/CE[50], hanno segnato un punto di svolta per il riconoscimento di un generale divieto di discriminazione all'interno dell'ordinamento europeo.

La novità dell'articolo 13, rispetto agli articoli 12 e 119 (ora articoli 18 e 157 TFUE), risiede nel fatto che, al contrario delle precedenti previsioni, strettamente funzionali alla creazione del merca-

nell'ambito delle competenze da esso conferite alla Comunità, il Consiglio, deliberando all'unanimità su proposta della Commissione e previa consultazione del Parlamento europeo, può prendere i provvedimenti opportuni per combattere le discriminazioni fondate sul sesso, la razza o l'origine etnica, la religione o le convinzioni personali, gli handicap, l'età o le tendenze sessuali». Come osservato in dottrina in questo articolo sarebbe contenuto un nuovo principio generale che «supera di gran lunga i confini del vecchio divieto di discriminazione fondato sulla nazionalità […]», cfr. L. ANGELINI, *A proposito di diritti sociali e principio di uguaglianza nella Carta dei diritti fondamentali dell'Unione Europea,* in *Giornale di diritto del lavoro e di relazioni industriali,* 2001, pp. 636-637.

[48] Direttiva 2000/78/CE del Consiglio, del 27 novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro Gazzetta ufficiale n. L 303 del 02/12/2000. Si veda, sul punto, in dottrina M. BONINI BARALDI, *La pensione di reversibilità al convivente dello stesso sesso: prima applicazione della direttiva 2000/78/CE in materia di discriminazione basata sull'orientamento sessuale*, in *Famiglia e diritto*, n. 7/2008, p. 660 ss.; G. PICARELLA, *Le discriminazioni fondate sull'orientamento sessuale nella giurisprudenza della Corte di Giustizia: dal caso P. alla sentenza Romer*, in *Rivista Italiana del Diritto del Lavoro*, n. 4/2011, p. 1325 ss. e S. NINATTI, *Il caso Romer: limiti di materia, principio di uguaglianza o tutela di diritti?*, in *Quaderni costituzionali*, n. 3/2011, p. 693 ss.

[49] Direttiva 2000/43/CE del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica, in GUCE L 180/22 del 19.7.2000.

[50] Direttiva 2004/113/CE del Consiglio del 13 dicembre 2004 che attua il principio della parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e la loro fornitura in GUUE L 373/37 del 21/12/2004. In dottrina si vedano i contributi di P. CHIECO, *Le nuove direttive comunitarie sul divieto di discriminazione*, in *Rivista Italiana di Diritto del Lavoro,* 2002, pp. 75-117; M. VIZIOLI, *Il diritto comunitario tra principio di non discriminazione e tutela delle differenze*, in *Il diritto del mercato del lavoro*, n. 3/2004, p. 953 ss., e, per una analisi delle misure assunte con riferimento ai diversi profili di discriminazione, cfr. M. BARBERA (a cura di), *Il nuovo diritto antidiscriminatorio. Il quadro comunitario e nazionale*, Milano, 2007.

to unico, la nuova disposizione, sebbene priva di efficacia diretta[51], come si legge nei preamboli di entrambe le direttive[52], ha inteso dare effettiva attuazione ai principi di libertà, democrazia e rispetto dei diritti fondamentali così come sanciti all'interno delle Costituzioni dei singoli Stati membri[53]. L'articolo 13 ha, pertanto, rappresentato un'apertura dell'ordinamento europeo al principio di eguaglianza ed è stato adottato al dichiarato scopo di avvicinare l'Europa ai cittadini, attraverso il rafforzamento degli strumenti in dotazione alla Comunità per promuovere e garantire i diritti fondamentali[54].

A partire dal settore giuslavoristico e previdenziale si è dunque assistito ad una lenta e progressiva estensione anche ad altri ambiti, sino ad arrivare ad una esplicita e generale affermazione all'interno dei trattati[55].

[51] La diretta applicabilità del principio della parità di trattamento retributiva tra uomo e donna, è arrivata a seguito della sentenza della Corte di Giustizia del 8 aprile 1976 in C–43/75 *Defrenne* che ha fatto da apripista rispetto al riconoscimento dell'efficacia diretta verticale ma anche orizzontale di tale principio, cfr. M. BARBERA, *Discriminazioni ed eguaglianza nel rapporto di lavoro*, Milano, 1991, p. 34 ss.

[52] Nei preamboli delle direttive all'interno del considerando n. 1) si legge: «Conformemente all'art. 6 del Trattato sull'Unione europea, l'Unione europea si fonda sui principi di libertà, democrazia, rispetto dei diritti umani e delle libertà fondamentali e dello Stato di diritto, principi che sono comuni a tutti gli Stati membri e rispetta i diritti fondamentali quali sono garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e quali risultano dalle tradizioni costituzionali comuni degli Stati membri, in quanto principi generali del diritto comunitario».

[53] Cfr. M. BELL, *The new article 13 EC Treaty: a sound basis for European anti – discrimination law?,* in *Maastricht Journal of European and comparative law*, 1999, n. 1, p. 6.

[54] L. WADDINGTON, *Testing the limits of the EC Treaty article on non-discrimination*, in *Industrial Law Journal*, 1998, n. 1, p. 134.

[55] Già nel preambolo del TUE si legge che gli Stati membri si ispirano alle eredità culturali, religiose e umanistiche dell'Europa, da cui si sono sviluppati i valori universali dei diritti inviolabili e inalienabili della persona, della libertà, della democrazia, dell'uguaglianza e dello Stato di diritto. Viene enunciato il rispetto dei principi della libertà, della democrazia, l'osservanza dei diritti dell'uomo e delle libertà fondamentali nonché dello Stato di diritto. Viene altresì confermato

Nel 2009, in particolare, il Trattato di Lisbona ha introdotto una clausola orizzontale volta a integrare la lotta contro le discriminazioni in tutte le politiche e le azioni dell'Unione (articolo 10 TFUE), con la previsione di una procedura legislativa speciale, che prevede il voto all'unanimità in seno al Consiglio previa approvazione del Parlamento europeo.

Ad oggi, guardando ai trattati, in tema di non discriminazione, particolare rilievo assume l'articolo 2 TUE, secondo cui l'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello stato di diritto e dei diritti umani, compresi i diritti delle persone appartenenti a minoranze: valori ritenuti ormai comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini. Ancora più puntualmente, in tema di non discriminazione, il successivo articolo 3 (3) dispone che l'Unione combatte l'esclusione sociale e le discriminazioni, promuove la giustizia e la protezione sociale nonché la parità tra donne e uomini.

Il divieto di discriminazione inteso, anche in questo caso, come manifestazione del più generale principio di eguaglianza, costituisce al momento presente, un caposaldo dell'ordinamento dell'Unione

il rispetto dei diritti sociali definiti all'interno della Carta sociale europea firmata a Torino il 18 ottobre 1961 e della Carta comunitaria dei diritti sociali fondamentali dei lavoratori del 1989. Queste carte, pertanto, unitamente ai principi da esse richiamati, entrano a pieno titolo nell'*acquis* comunitario nonostante l'assenza di forza vincolante. Per ciò che riguarda i Trattati, particolare rilievo assume l'articolo 2 TUE, in forza del quale l'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e dei diritti umani, compresi i diritti delle persone appartenenti a minoranze: valori ritenuti ormai comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini; e, ancora più puntualmente in tema di non discriminazione, il successivo articolo 3 (3), secondo cui «l'Unione combatte l'esclusione sociale e le discriminazioni e promuove la giustizia e la protezione sociale, la parità tra donne e uomini, la solidarietà tra le generazioni, la tutela dei diritti del minore, la coesione economica, sociale e territoriale, e la solidarietà tra gli Stati membri».

europea[56] finalizzato a garantire la parità di trattamento e la non discriminazione a diversi livelli.

Secondo una costante giurisprudenza della Corte di giustizia[57], il principio di non discriminazione, che taglia trasversalmente l'intero ordinamento sovranazionale, rappresenta, insieme al novero dei diritti fondamentali ormai codificati e spesso di ispirazione costituzionale, parte integrante dei principi generali del diritto dell'Unione. Per questo, nell'assumere le proprie decisioni, la Corte si è sempre dimostrata molto attenta nel trattare le tradizioni costituzionali comuni agli Stati membri, nonché nell'uniformarsi alle indicazioni fornite dagli strumenti internazionali relativi alla tutela dei diritti dell'uomo a cui gli Stati membri hanno cooperato o aderito[58].

Inoltre, come noto, in virtù del ricordato valore di fonte primaria riconosciuto alla Carta di Nizza a seguito dell'entrata in vigore del Trattato di Lisbona, del principio di efficacia diretta del diritto dell'Unione europea negli Stati membri[59] e del ruolo ormai riconosciuto anche alle norme della CEDU[60], in pratica, i giudici interni si trovano a dover applicare le tutele previste in tema di non discriminazione, tanto dal diritto dell'Unione quanto dalla Convenzione europea dei diritti dell'uomo, anche nell'ambito di giudizi interni, e

[56] Così si è espressa più volte la Corte di giustizia si vedano a titolo esemplificativo CGUE, cause riunite 117-76 e 16-77, *Albert Ruckdeschel & Co. e Hansa-Lagerhaus Ströh & Co. c. Hauptzollamt Hamburg-St. Annen; Diamalt AG c. Hauptzollamt Itzehoe*, 19 ottobre 1977; CGUE, causa 283/83, *Firma A. Racke c. Hauptzollamt Mainz*, 13 novembre 1984; CGUE, C-292/97, *Kjell Karlsson e a.,* 13 aprile 2000.

[57] Ben riassunta nelle sentenze *Internationale Handelsgesellschaft*, 11/70, EU:C:1970:114, punto 4, e *Nold/Commissione*, 4/73, EU:C:1974:51, punto 13.

[58] Corte di giustizia dell'Unione europea (Seduta Plenaria), parere 2/13, del 18 dicembre 2014, ECLI:EU:C:2014:2454.2, punto 37.

[59] Cfr. *ex multis* CGUE, *Mangold c. Rüdiger Helm,* C-144/04; ID., *Kücükdeveci c. Swedex GmbH & Co., C-555/07;* ID., *Rasmussen c. Dansk Industries*, C-441/14, ID., *Seda Kücükdeveci/Swedex GmbH & Co. KG* [Grande Sezione], C-555/07, 19 gennaio 2010, in *Racc.* dove la Corte evidenzia come il principio di non discriminazione in base all'età "debba essere considerato un principio generale del diritto dell'Unione al quale la direttiva 78/2000 da espressione concreta".

[60] V. *supra*, in questo capitolo, par. 2.1.

ciò a prescindere dal fatto che le parti del procedimento vi facciano o meno riferimento.

A seguito del ricordato assetto delineato dal Trattato di Lisbona, un'altra fonte normativa fondamentale da considerare quando si discute di non discriminazione, è certamente la Carta di Nizza[61], con i suoi articoli 20 e 21[62].

Quest'ultima disposizione vieta la discriminazione fondata, "in particolare", sul sesso, la razza, il colore della pelle, l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione, le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, gli handicap, l'età, le tendenze sessuali, oltre a quella fondata sulla cittadinanza.

A questa disposizione, che rappresenta la garanzia fondamentale che tutela la dignità della persona indipendentemente dalle diverse caratteristiche personali, è stata attribuita, grazie all'inciso "in particolare", una portata ancora più estesa, poiché consentirebbe di realizzare un ampliamento «di tipo universalistico della tutela antidiscriminatoria»[63].

V'è però da dire che, nonostante le molteplici iniziative ricordate, ad oggi il quadro normativo europeo in tema di non discriminazione non appare completo. Sebbene, infatti, l'Unione abbia giocato un ruolo significativo rispetto all'azione demandata agli Stati membri nell'attuare e tutelare i principi di uguaglianza e non di-

[61] Spiegazioni relative alla Carta dei Diritti fondamentali, doc. 2007/C 303/02, pubblicato nella Gazzetta ufficiale dell'Unione europea del 14 dicembre 2007. Si veda in dottrina, *ex multis*, O. POLLICINO, V. SCIARABBA, *La Carta di Nizza oggi, tra "sdoganamento giurisprudenziale" e Trattato di Lisbona*, in *Diritto Pubblico Comparato e Europeo*, 2008, pp. 101-120.

[62] Si vedano in dottrina i contributi di C. FAVILLI, *La non discriminazione nell'Unione europea*, Bologna, 2008, p. 25 ss.; F. CASOLARI, *Commento agli art. 20 e 21 della Carta dei diritti fondamentali dell'Unione europea*, in Pocar, F., Baruffi, M.C., *Commentario breve ai trattati dell'Unione europea*, II ed., 2011, Padova, pp. 1719-1729; G. BIAGIONI, I. CASTANGIA (a cura di), *Il principio di non discriminazione nell'Unione europea*, Napoli, 2011, p. 167 ss.

[63] L. CURCIO, A. GUARISO, *Articolo 21. Non discriminazione*, in G. Bisogni, G. Bronzini, V. Piccone (a cura di), *La Carta dei diritti dell'Unione Europea. Casi e materiali*, Taranto, 2009, p. 257.

scriminazione e abbia svolto un'importante funzione di impulso e di guida, ad oggi manca ancora una normativa unitaria.

La Commissione si era già mossa in questo senso oltre dieci anni fa con una proposta di direttiva[64] che aveva l'obiettivo di rinnovare l'impegno a rafforzare la lotta contro la discriminazione e a consolidare gli strumenti di promozione attiva dell'uguaglianza e delle pari opportunità[65]. Tale normativa, però, stenta a vedere la luce.

A questo punto, delineato brevemente il fondamento giuridico del divieto di discriminazione a livello internazionale ed europeo, si può ora passare all'analisi dei profili di rischio che l'imporsi sulla scena dell'intelligenza artificiale sta ponendo anche in tema di non discriminazione.

3. *Bias* e *math washing*: l'apparente neutralità e i rischi di discriminazione legati all'utilizzo di algoritmi

Uno dei dibattiti principali attorno ai rischi che l'intelligenza artificiale può generare sui diritti fondamentali oltre che, come già evidenziato, sul tema della tutela dei dati[66], è incentrato sul rispetto del principio di eguaglianza e sui potenziali risultati discriminatori[67] a cui l'utilizzo di algoritmi potrebbe condurre[68].

[64] Proposta di direttiva del Consiglio recante applicazione del principio di parità di trattamento fra le persone indipendentemente dalla religione o le convinzioni personali, la disabilità, l'età o l'orientamento sessuale, COM (2008) 426 definitivo.

[65] In tal senso il contenuto della Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni "Non discriminazione e pari opportunità: Un impegno rinnovato" del 2 luglio 2008, COM (2008) 420 definitivo, che accompagna la proposta di direttiva citata alla nota 37.

[66] Vedi *supra* cap. III.

[67] L. NAUDTS, *AI en algoritmische categorisatie: gelijkheid en non-discriminatie*, in Jan De Bruyne, Nicolas Bouteca (eds.) *Artificiële intelligentie en maatschappij*, Oud-Turnhout/'s-Hertogenbosch, 2021, pp. 223–247.

[68] Per un approfondimento sulla genesi e sullo sviluppo della tutela antidiscriminatoria nelle esperienze americana ed europea si veda L. GIACOMELLI, *Ri-*

Come si avrà modo di sottolineare, tutti i profili oggetto di analisi, seppur diversamente delineati, rimandano unitariamente a possibili rischi di trattamenti ingiustificatamente diversi riconducibili a razza, nazionalità, credenze religiose, opinioni politiche, etnia, genere, sesso, stato di salute, tratti somatici e convinzioni personali.

È stato osservato che eventuali esiti discriminatori potrebbero concretizzarsi in due momenti diversi dello sviluppo del sistema[69].

Un primo momento è quello che, normalmente, inizia con la fase di acquisizione dei dati, seguita dalla rielaborazione, dalla selezione delle caratteristiche, dal *training* e dall'applicazione del modello di elaborazione programmato. La discriminazione, in questo caso, potrebbe realizzarsi proprio nel primissimo stadio di acquisizione dati, qualora il sistema venga alimentato con informazioni incomplete, parziali o distorte. Ciò conduce normalmente a due risultati, entrambi potenzialmente discriminatori, una falsa rappresentazione della realtà, che conduce ad effettuare scelte non corrette, e una discriminazione strutturale, insita nel processo di assunzione della decisione[70]. Peraltro, come già evidenziato[71], quando si tratta di intelligenza artificiale il modello etico da implementare è scelto *a priori* da chi sviluppa, o più precisamente è dettato dalla morale pubblica corrente e, dunque, il sistema deve essere settato in modo da assecondare le opinioni della società contemporanea, anche se queste dovessero essere "indirettamente" o "velatamente" discriminatorie e sessiste.

Un secondo momento è quello della classificazione. Si tratta dello stadio in cui vengono selezionate, tra le tante possibili, le caratteristiche dei soggetti coinvolti (ad esempio sesso, razza, religione, orientamento sessuale). In questo processo di selezione, qualora

pensare l'uguaglianza. Gli effetti collaterali della tutela antidiscriminatoria, Torino, 2018, p. 198 ss.

[69] C. DAELMAN, *AI through a human rights lens. The role of human rights in fulfilling AI's potential*, in J. De Bruyne, C. Vanleenhove (eds), *Artificial Intelligence and the Law*, Cambridge, 2021, p. 140 ss.

[70] M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. Ebers, S. Navas Navarro (a cura di), *Algorithms and Law*, Cambridge, 2019, p. 49 ss.

[71] Si veda *supra* cap. IV, par. 6.

vengano privilegiate determinate informazioni a discapito di altre, potrebbero verificarsi dei *bias* a danno di talune categorie di individui.

Invero, all'interno dei grandi *database* che introitano dati, si operano categorizzazioni spesso in maniera non visibile.

Ne sono un esempio gli Stati Uniti, dove il sistema *Fico score,* un algoritmo che valuta il rischio economico e che è diventato un punto riferimento nel mondo del credito al consumo, valuta per ciascun individuo l'affidabilità e i rischi connessi nel caso di eventuale accesso al credito. In questo caso, si tratta peraltro di un *software* pubblico, ma gli istituti di credito spesso ne utilizzano di altre tipologie che lavorano per gli stessi obiettivi ma in modo del tutto silente e opaco, con rischi di distorsioni delle informazioni e di risultati iniqui ancora più seri.

In sintesi, questi sistemi effettuano delle accurate profilazioni degli individui interessati, ma anche delle loro famiglie, raccogliendo e correlando dati (c.d. *data mining*) per stabilire i livelli di indebitamento, le abitudini di vita e di consumo, le preferenze, la situazione bancaria e, addirittura, quella giudiziaria.

L'insieme di questi dati e i loro collegamenti consentono di tratteggiare "profili umani"[72] sempre più dettagliati.

I dati così elaborati vengono poi rivenduti per consentire alle aziende di predire i comportamenti degli individui, intesi come "consumatori", al fine di inviare pubblicità dedicata. Tali classificazioni sono sempre più dettagliate e, soprattutto, sono delineate all'insaputa degli interessati che si trovato così, del tutto inconsapevolmente e al di fuori di qualsiasi tipo di supervisione pubblica, ad essere classificati come "clienti non affidabili", oppure come soggetti con un "profilo sanitario rischioso" o con "reddito in calo" *et similia*[73].

In altre parole, aggregando i dati, viene costruita una sorta di identità digitale del soggetto. In questo modo ne viene altresì creata

[72] In realtà non solo umani. A quanto pare il riconoscimento facciale verrà utilizzato anche sui ratti.

[73] Si veda L. GIACOMELLI, *Big Brother is "gendering" you*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., pp. 208-209.

una rappresentazione virtuale che, tuttavia, potrebbe non risultare corretta o sufficientemente accurata e potrebbe non corrispondere al dato di realtà, già a partire dal genere (ad esempio un soggetto, sulla base dei dati acquisiti, potrebbe essere categorizzato come di sesso femminile o maschile nel mondo digitale, ma essere del genere opposto nella realtà).

Come è stato osservato, ciò che viene categorizzata e, di conseguenza, discriminata, è la "persona digitale", risultato di una composizione e decomposizione dei propri dati, in un continuo processo di integrazione e disintegrazione. Pur essendo vero, il problema basilare è che gli effetti di eventuali comportamenti discriminatori non ricadono sul soggetto digitale ma su quello reale[74].

[74] Si veda D. LYON, *Surveillance Society. Monitoring Everyday Life*, in *Open University Press*, 2001, disponibile online. L'A. sostiene che non solo viviamo in una società digitale ma anche in una società della sorveglianza. V. anche S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Bari, 2014, p. 20 ss. In questo caso l'A. evidenzia la necessità di una "cittadinanza digitale" che tuteli il soggetto che accede alla rete e il suo "corpo elettronico", che garantisca la cancellazione dei propri dati personali e il 'nuovo' "diritto all'oblio". La Corte di giustizia ha riconosciuto e tutelato il diritto all'oblio e, con due note sentenze del 2019, ha fissato i limiti alla "deindicizzazione" dei contenuti digitali, CGUE, 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd*; 13 maggio 2014, C-131/12, *Google Spain*; 06 ottobre 2015, C-362/14, *Schrems (Facebook);* 24 settembre 2019, C-507/17, *Google CNIL*; 03 ottobre 2019, C18/18, *Glawischnig-Piesczek*. Si veda per alcune indicazioni di ordine generale WP ART. 29, *Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12*, 26 novembre 2014, disponibili *online*. In dottrina, *ex multis*, O. POLLICINO, *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it,* n. 19, 2019, p. 2 ss.; F. PIZZETTI, *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il 'Velo di Maya'*, in G. Resta, Zeno-Zencovich (a cura di), *Il Diritto all'oblio su internet dopo il caso Google Spain*, Roma, 2015, p. 255 ss. e M. SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, p.123; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, fasc. 2, p. 440; AA.VV., *Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997*, E. Gabrielli (a cura di), Napoli, 1999, p. 10 ss.; S. NIGER, *Il diritto*

4. Discriminazione basata sull'etnia: Il caso degli Uyghur

Il diffondersi delle nuove tecnologie ha messo in mano ai "potenti del mondo" nuovi strumenti repressivi con un potenziale lesivo oggettivamente preoccupante.

In un recente scritto Darren Byler[75], affrontando il tema delle nuove forme di repressione attuate mediante l'utilizzo delle attuali tecnologie, ha esaminato il caso cinese e le discriminazioni perpetrate nella regione autonoma dello Xinjiang ai danni di minoranze etniche e religiose e, in particolare, degli Uyghur[76].

Tale minoranza, essendo percepita dal governo cinese come una minaccia nazionalista, sarebbe sistematicamente sottoposta ad indottrinamento politico, oppressione religiosa, restrizioni alla libertà personale, di movimento e a detenzioni di massa.

Il controllo su tale minoranza sarebbe attuato proprio mediante l'impiego di sistemi di intelligenza artificiale, specialmente attraver-

all'oblio, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale,* Padova, 2007, p. 59 ss.; T. AULETTA, *Diritto alla riservatezza e* "droit à l'oubli", in G. Alpa, M. Bessone, L. Boneschi e G. Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, p. 127 ss.; G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, p. 801 ss.; S. MORELLI, *voce Oblio (diritto all')*, in *Enc. dir. agg.*, VI, Milano, 2002, p. 851 ss.; G. FINOCCHIARO, *La memoria della Rete e il diritto all'oblio*, Anno XXVI, fasc. 3, p. 391 ss.; M. MEZZANOTTE, *Il Diritto all'oblio, Contributo all'analisi della privacy storica*, Napoli, 2009, p. 26 e 81 ss. Per un'idea di come sia stato recepito il diritto all'oblio in Italia R. LANZO, M. GIORDANO, *Diritto all'oblio e motori di ricerca: Il diritto di essere dimenticati. I casi decisi dal garante,* Milano, 2021, p. 22 ss. e sia altresì consentito di rinviare a C. GRIECO, *L'attuazione in Italia del diritto all'oblio*, in *Il Mercato Unico Digitale*, (a cura di) Gianluca Contaldi, *Diritto, Mercato e Tecnologia, numero speciale 2017, Atti del Convegno*, pp. 161-188.

[75] D. BYLER, *In the Camps: Life in China's High-Tech Penal Colony*, London, 2022, p. 20 ss.; ID., *Terror Capitalism Uyghur Dispossession and Masculinity in a Chinese City*, Durham, 2021, p. 10 ss.

[76] Si tratta di una minoranza turcofona residente in Cina che parla una propria lingua e professa la religione islamica sunnita. Si veda, al riguardo, HUMAN RIGHTS WATCH, *China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App*, 1 maggio 2019, disponibile online e B. DARREN, *China's hi-tech war on its Muslim minority*, *Guardian,* 11 aprile 2019, disponibile *online*.

so tecnologie di riconoscimento facciale, utilizzate sempre più frequentemente per monitorare gli Uyghur, facilitandone in modo esponenziale l'identificazione e il tracciamento[77].

Numerosi parlamenti di diversi Paesi nel mondo[78] hanno denunciato tale stato di cose, accusando il regime di Pechino di genocidio[79]. Le stime più recenti parlano di circa un milione di uiguri rinchiusi in "campi di rieducazione"[80].

Quello in corso in Cina è stato definito come l'esempio più 'avanzato' (se così si può definire) di utilizzazione delle tecnologie dell'intelligenza artificiale a fini di profilazione razziale e religiosa[81].

[77] C. DAELMAN, *AI through a Human Rights Lens. The Role of Human Rights in Fulfilling AI's Potential*, in Jan De Bruyne Cedric Vanleenhove (eds.) *Artificial Intelligence and the Law*, Cambridge, 2021, p. 141 ss.

[78] Una posizione particolarmente severa è stata assunta dagli Stati Uniti nel delicato contesto della guerra commerciale che ha contrapposto USA e Cina a partire dal 2019. Il presidente Biden nel dicembre del 2021 ha firmato *l'Uyghur Forced Labor Prevention Act* (UFLPA). Tale norma, al momento un *unicum* nel panorama internazionale, impone al governo degli Stati Uniti di monitorare le eventuali violazioni dei diritti delle minoranze e punirne i responsabili con appropriate sanzioni. È inoltre prevista la nomina di un coordinatore speciale per lo Xinjiang presso il Dipartimento di Stato e un'azione dell'FBI rispetto alle eventuali minacce e violazioni di diritti commesse nei confronti di cittadini statunitensi di origine uigura, nel contesto di una politica cinese che il testo stesso della norma statunitense definisce "orwelliana". Si aggiunge a queste misure una serie di attività di monitoraggio e produzione di rapporti che trova fondamento in altre leggi vigenti negli Stati Uniti in materia di tutela delle minoranze religiose e che hanno ispirato anche numerosi paesi europei. Chiaramente, tale presa di posizione non è passata inosservata. La Cina ha dichiarato di "opporsi fermamente" al provvedimento e che esso costituisce una "flagrante interferenza negli affari interni della Cina". Sempre nel 2021 è stato approvato il *China Technology Transfer Control Act* che, se approvato, imporrebbe pesanti restrizioni all'*export* di tecnologia utilizzata nelle attività di sorveglianza da parte del governo cinese.

[79] Si veda il rapporto redatto dal OHCHR *"Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China"* e la risposta della Cina alle accuse entrambi i testi sono disponibili *online*.

[80] Human Rights Watch, *China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App*, 1° Maggio 2019, approfondimenti disponibili *online*.

[81] Ci si riferisce agli esperti che hanno redatto il *Report on International Religious Freedom: China – Xinjiang*, pubblicato nel settembre 2019 dalla *US Com-*

Secondo gli ultimi rapporti[82], infatti, il governo cinese utilizzerebbe diverse applicazioni di intelligenza artificiale, in particolare quelle di riconoscimento facciale, per consentire alle autorità di identificare, profilare e tracciare gli spostamenti degli uiguri. I dati raccolti, mediante l'utilizzo di questi sistemi, vengono combinati tra loro per fornire alle autorità un'idea dettagliata degli aspetti della vita dei soggetti profilati[83] quali: occupazione, scuola, negozi frequentati, abitudini di vita, spostamenti, preferenze e residenza.

Pratiche tipiche della religione islamica, quali l'ora di preghiera, l'insegnamento della religione o, anche semplicemente, avere parenti all'estero, sono considerati indicatori di pericolosità sociale e possono condurre addirittura alla deportazione forzata in strutture che sono chiamate dalle autorità cinesi "campi di rieducazione" dove, oltre alla già intollerabile e inaccettabile privazione della libertà personale, si sospetta che vengano altresì praticati, in maniera abituale, trattamenti inumani e degradanti, torture e violenze di ogni tipo.

In un caso come quello appena esaminato, è indubbio che siano proprio i sistemi di intelligenza artificiale i mezzi che rendono possibile la messa in atto, da parte del governo cinese, di queste politiche oppressive e discriminatorie su larga scala. Senza questi sistemi, la possibilità di localizzare, seguire e profilare minoranze risulterebbe di certo più difficoltosa e molto meno pervasiva, seppur non del tutto esclusa, e la portata della violazione dei diritti fondamentali a danno degli Uyghur, risulterebbe, almeno nella pratica, meno lesiva.

Questo esempio dimostra in tutta la sua drammaticità la portata

mission on International Religious Freedom. All'interno viene denunciata l'istallazione di milioni di telecamere in ogni zona del paese per controllare le aree pubbliche, i programmi speciali di sorveglianza Sharp Eyes e Skynet, la creazione di un *database* nazionale con il Dna dei cittadini cinesi, la cura particolare dedicata ai residenti dello Xinjiang (in maggioranza uiguri) di cui sono stati raccolti, dopo accurati esami medici, tracce ematiche, immagine dell'iride, impronte digitali.

[82] HUMAN RIGHTS WATCH, *China's Algorithims of Repression Reverse Enginnering a Xinjiang Police mass Surveillance App*, cit., p. 1.

[83] B. DARREN, *China's hi-tech war on its Muslim minority*, in *The Guardian*, 11 aprile 2019, pp. 13-28, disponibile *online*.

distruttiva che questi sistemi possono avere se, in assenza di un'adeguata regolamentazione che ne disciplini compiutamente lo sviluppo e, soprattutto, le possibilità e i limiti di impiego, dovessero finire in mani sbagliate.

Peraltro la Cina sta continuando a muoversi in una direzione preoccupante.

Di recente, infatti, le autorità di Pechino hanno reso noto di aver approvato gli indirizzi per le aziende operanti nel settore dell'*hi-tech*. Nella specie, la *Cyberspace Administration of China* (CAC), ovvero l'agenzia di sicurezza cinese che si occupa della regolamentazione, censura e supervisione di Internet, ha presentato un progetto di legge[84], ora aperto alla raccolta di osservazioni e commenti, contenente una serie di regole che disciplinano l'utilizzo dei nuovi prodotti di intelligenza artificiale sviluppati in Cina. Tra le prescrizioni si legge che tali tecnologie dovranno rispettare "i valori fondamentali del socialismo" ma anche la moralità pubblica e l'ordine pubblico.

Pertanto, le aziende, che intendano sviluppare o commercializzare in Cina tecnologie di intelligenza artificiale, dovranno sottoporre i loro prodotti a una verifica di sicurezza governativa prima di poterli commercializzare. Le *chatbot* dovranno verificare l'identità degli utenti e i loro creatori e, a quanto si legge, saranno obbligati a garantire che i contenuti serviti dall'intelligenza artificiale siano veritieri e non discriminatori. Sarà vietato diffondere contenuti

[84] Il testo è disponibile sul sito dell'autorità all'indirizzo http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm. In particolare, all'interno dell'articolo 4 del progetto, si legge: «The provision of generative artificial intelligence products or services shall comply with the requirements of laws and regulations, respect social morality, public order and good customs, and meet the following requirements: 1) The content generated by generative artificial intelligence should reflect the core values of socialism, and must not contain subversion of state power, overthrow of the socialist system, incitement to split the country, undermine national unity, promote terrorism, extremism, and promote ethnic hatred and ethnic discrimination, violence, obscene and pornographic information, false information, and content that may disrupt economic and social order».

ritenuti in grado di sovvertire il potere dello Stato o di sostenere il rovesciamento del sistema politico comunista del Paese.

Il progetto di legge ha già suscitato delle reazioni, soprattutto nelle organizzazioni che si occupano della tutela dei diritti umani, poiché le nuove linee guida sembrerebbero rappresentare il segno più evidente della volontà delle autorità cinesi di estendere il proprio apparato di censura *online* al mondo emergente dell'intelligenza artificiale generativa.

In particolare, secondo Michael Caster, responsabile del programma digitale per l'Asia di Article 19, un'organizzazione per i diritti umani che si occupa di libertà di espressione online in Cina, «il Partito utilizzerà le nuove linee guida sull'intelligenza artificiale generativa per svolgere la stessa funzione di censura, sorveglianza e manipolazione delle informazioni che ha cercato di giustificare con altre leggi e regolamenti»[85].

Nel frattempo, la Cina ha licenziato un *software* di intelligenza artificiale generativa SenseTime (in pratica un'alternativa all'americana ChatGPT) mentre il gigante della tecnologia Alibaba ha annunciato l'intenzione di lanciare sul mercato il proprio prodotto, anch'esso in stile ChatGpt, che si chiamerà Tongyi Qianwen.

Le autorità di regolamentazione cinesi non hanno lesinato le loro preoccupazioni per le potenziali interferenze politiche attribuite alle *chatbot* di intelligenza artificiale prodotte negli Stati Uniti. Lo scorso febbraio, le cinesi Tencent e Ant Group avrebbero bloccato gli utenti che cercavano di accedere a ChatGPT poiché, secondo le autorità di regolamentazione, potrebbe essere usato per "diffondere false informazioni" e alcune delle risposte fornite da ChatGPT sono state percepite dalle autorità cinesi come "coerenti con la propaganda politica del governo statunitense"[86].

Di contro, le autorità statunitensi stanno esprimendo preoccupazioni analoghe sui modelli di intelligenza artificiale sviluppati da Pechino. Il repubblicano Mike Gallagher, nel corso di un convegno sul tema dell'intelligenza artificiale, ha descritto i modelli di intelli-

[85] L'intervista si può leggere al seguente link https://gizmodo.com/ai-china-regulations-free-speech-baidu-ernie-chatgpt-1850329689.

[86] *Ibidem*.

genza artificiale cinesi come armi che i funzionari governativi potrebbero usare per perfezionare uno "stato di sorveglianza tecnototalitario orwelliano". Mentre l'ex amministratore delegato di *Google*, Eric Schmidt, ha affermato che gli Stati Uniti devono fare tutto il necessario ("whatever it takes") per vincere la gara a colpi di intelligenza artificiale contro la Cina[87].

La polarizzazione del dibattito, così come della sfida tecnologica ed economica in atto tra Cina e Stati Uniti, dalla quale peraltro l'Europa è completamente esclusa, dovrebbe preoccupare. In primo luogo perché, come già osservato nei paragrafi precedenti, le tecnologie di intelligenza artificiale, per poter essere utilizzate al fine di migliorare il benessere sociale collettivo, dovrebbero essere scevre da qualsiasi implicazione politica e dovrebbero focalizzarsi unicamente sulla strada migliore per assicurare un sano e proficuo progresso tecnologico. In secondo luogo in quanto, per assicurare il rispetto dei diritti fondamentali degli individui, le tecnologie di intelligenza artificiale, anche generativa, devono applicare il più possibile modelli neutrali per evitare rischi di potenziali discriminazioni.

Al momento, però, visto quanto sta accadendo alla minoranza degli Uyghur e considerato il tenore delle nuove linee guida cinesi, aumenta ragionevolmente le preoccupazioni che le autorità di Pechino vogliano utilizzare le tecnologie di intelligenza artificiale per salvaguardare il regime e continuare le repressioni a danno delle minoranze, facendo dell'intelligenza artificiale uno strumento politico.

5. Discriminazione basata sul genere con particolare riguardo all'accesso al mercato del lavoro e all'istruzione

L'intelligenza artificiale sta trasformando, sotto diversi profili, anche il mercato del lavoro. Questa ondata di automazione è caratterizzata dalla crescente capacità delle macchine di svolgere nuove mansioni, non più solo quelle caratterizzate da un alto grado di

[87] *Ibidem*.

standardizzazione e ripetitività, ma anche dall'impiego di algoritmi nei processi di selezione del personale, nelle valutazioni delle *performance* e nella rilevazione delle presenze.

Sfortunatamente, si è notato che spesso, anche in questo settore, l'impiego di sistemi di intelligenza artificiale può condurre a risultati discriminatori.

Ad esempio, si è visto che i pregiudizi di genere sono spesso incorporati nella progettazione di sistemi di intelligenza artificiale poiché tendono a riflettere e, addirittura, ad amplificare i punti di vista e i pregiudizi personali di coloro che sviluppano queste tecnologie.

Pregiudizio nella progettazione significa che la stessa modalità operativa predefinita dei sistemi di intelligenza artificiale risulta discriminatoria, escludente o sessista.

Ora, chiaramente, mentre un minimo margine di errore nella classificazione potrebbe anche considerarsi accettabile, un vero e proprio *bias* nella progettazione si traduce in una discriminazione a carico di alcuni gruppi demografici, come le donne, rispetto alle quali si è visto che il livello di errore è spesso più alto rispetto a quello a carico di altri gruppi[88]. Questo si verifica quando la progettazione di nuovi algoritmi di apprendimento automatico si basa su insiemi di dati incompleti ma anche quando i programmi di addestramento e le tecniche di analisi risultano distorte[89].

Quando siffatti sistemi sono incorporati negli strumenti di gestione della forza lavoro possono portare ad esiti discriminatori ed escludenti.

In realtà, questi effetti discriminatori possono aversi già nella fase iniziale di accesso al mercato del lavoro e, in particolare, nella fase del *recruiting*.

I motori di ricerca giocano un ruolo importante quando un candidato si mette alla ricerca di una nuova posizione lavorativa.

[88] J. FEAST, *4 Ways to Address Gender Bias in AI*, in *Harvard Business Review*, 2019, disponibile *online*.

[89] Si veda la compiuta analisi effettuata su questo tema dallo EUROPEAN INSTITUTE FOR GENDER EQUALITY, *Artifcial intelligence, platform work and gender equality*, 2021, disponibile *online.*

Sfortunatamente, è stato rilevato che in fase di *screening* delle candidature, gli algoritmi, applicando protocolli di *machine learning*, tendono ad assimilare e replicare i pregiudizi umani[90].

La conseguenza è che il motore di ricerca tende a mostrare annunci per posizioni più appetibili e meglio remunerate con più frequenza a candidati di sesso maschile che di sesso femminile, rischiando così di andare ad amplificare l'annoso, ormai quasi strutturale, problema del *gender gap* nei salari[91].

Casi di discriminazione possono aversi anche in fase di gestione organizzativa della prestazione lavorativa. Anche in questo ambito, gli algoritmi hanno mostrato delle criticità importanti.

Un caso recentemente esaminato dal Tribunale di Bologna, con l'ordinanza del 31 dicembre 2020[92], ha posto in luce tutti i limiti che gli algoritmi possono presentare nella gestione del rapporto lavorativo. In questa occasione, in particolare, è stato esaminato il funzionamento dell'algoritmo *Frank*, utilizzato dalla società *Deliveroo,* a causa dei rischi di discriminazione insiti nella programmazio-

[90] Gli algoritmi utilizzati da Amazon per scansionare curricula e *cover letters* mostrano di discriminare le donne. Si veda J. DASTIN, *Amazon scraps secret AI recruiting tool that showed bias against women*, in *Reuters*, 10 ottobre 2018, disponibile online.

[91] In Italia il problema è particolarmente accentuato. La fotografia occupazionale restituisce un'immagine sconfortante. Si è notato che nonostante rendimenti scolastici più alti, percorsi di laurea più brevi e votazioni più alte, le laureate italiane fanno molta più fatica a trovare lavoro rispetto ai colleghi uomini e guadagnano in media il 20% in meno. Con il Covid-19 la forbice è addirittura cresciuta. Cfr. E. BRUNO, *Gender gap: le donne guadagnano il 20% in meno degli uomini*, in *IlSole24Ore*, 28 gennaio 2022, disponibile *online* e D. AMIT, D. ANUPAM, *Automated Experiments on a Ad Privacy Settings a Tale of Opacity, Choice and Discrimination*, in *Proceeding on Privacy Enhancing Technologies*, 2015, pp. 105-106 e K. YORDANOVA, *AI is a Girl's Best Friend? A gender-based analysis of the legal and ethical challenge of AI systems*, in *Global Wo-men Hub Blog*, 2020-11, disponibile *online*.

[92] Tribunale di Bologna, Ord. del 31 dicembre 2020, consultabile *online*. Per un commento M. BORZAGA, M. MAZZETTI, *Discriminazioni algoritmiche e tutela dei lavoratori: riflessioni a partire dall'Ordinanza del Tribunale di Bologna del 31 dicembre 2020*, in *BioLaw*, 2022, 1, pp. 225-50, disponibile *online*.

ne e la minaccia ai diritti dei lavoratori che lo stesso è potenzialmente in grado di generare.

In sintesi, il sistema utilizzato da *Deliveroo* funziona attribuendo a ciascun *rider* un punteggio sulla base di due indicatori: affidabilità e partecipazione. Il primo viene calcolato sulla base dei *logs*, ovvero quei *file* di sistema utilizzati per tenere traccia degli accessi di ciascun *rider* all'interno della piattaforma di prenotazione dei turni messa a disposizione dall'azienda. Il sistema è programmato per tenere in considerazione unicamente gli accessi effettuati almeno quindici minuti prima del turno prenotato nella zona geografica di competenza del *rider*. Il secondo indicatore viene calcolato tenendo in considerazione la maggiore disponibilità dei *riders* a lavorare negli orari in cui la richiesta da parte dell'utenza di consegne a domicilio risulta più alta.

Combinando i due indicatori, l'algoritmo elabora per ciascun *rider* una statistica sulla base della quale gli viene attribuito un punteggio che, come chiarito dal tribunale di Bologna, costituisce "elemento di preferenza per le sessioni di prenotazione successive".

In un'ottica di premialità, il sistema così impostato consente ai *riders* con un punteggio più alto di prenotare in via prioritaria le sessioni di consegne che però, di conseguenza, risulteranno man mano non più disponibili per i *riders* con punteggi inferiori.

Se fin qui non si evidenziano particolari criticità nel funzionamento dell'algoritmo, considerando che in pratica è stata "tradotta in linguaggio di programmazione" la maggiore disponibilità in termini di tempo del lavoratore da dedicare all'attività lavorativa e, dunque, la possibilità di contare su una presenza più o meno costante nelle fasce orarie più critiche, il problema si pone in un momento successivo che attiene proprio alla gestione del lavoro e al riconoscimento dei diritti individuali.

L'algoritmo nell'elaborazione del punteggio, infatti, tiene in considerazione, tra i fattori che comportano un trattamento deteriore per il lavoratore, la mancata cancellazione del turno almeno ventiquattrore prima dell'inizio dello stesso, senza però prendere in considerazione le motivazioni per cui il *rider* non ha partecipato al turno in precedenza prenotato.

Come puntualmente rilevato dal Tribunale di Bologna, «in tutti

questi casi il *rider* vede penalizzate le sue statistiche indipendentemente dalla giustificazione della sua condotta e ciò per la semplice motivazione, espressamente riconosciuta da Deliveroo, che la piattaforma non conosce e non vuole conoscere i motivi per cui il *rider* cancella la sua prenotazione»[93].

Il problema, secondo il Tribunale, risiede proprio nell'indiscriminata mancata considerazione dei motivi che hanno determinato, tanto l'anullamento del turno precedentemente prenotato quanto l'eventuale cancellazione tardivo dello stesso. Secondo il giudice di merito, il fatto che a diverse situazioni sia riservato lo stesso trattamento determina una forma di discriminazione indiretta, che pone «una determinata categoria di lavoratori (quelli partecipanti ad iniziative sindacali di astensione dal lavoro) in una posizione di potenziale particolare svantaggio»[94].

In un simile sistema, dunque, l'elemento di discriminazione è rinvenibile nel fatto che qualora un *rider* aderisca ad uno sciopero, o non possa partecipare ad un turno di lavoro a causa di motivazioni legittime, non necessariamente annunciate o annunciabili con un preavviso di ventiquattrore, – si pensi ad una malattia, un incidente, impellenti esigenze familiari o di accudimento di minori –, rischia di veder peggiorare le sue statistiche e di perdere la posizione eventualmente raggiunta con conseguente – ingiustificato – aggravamento della sua posizione lavorativa.

L'ordinanza rileva correttamente un carattere discriminatorio nella condotta datoriale poiché, da un lato, il sistema adottato dava «applicazione ad una disposizione apparentemente neutra (la normativa contrattuale sulla cancellazione anticipata delle sessioni prenotate)» idonea a mettere «una determinata categoria di lavoratori (quelli partecipanti ad iniziative sindacali di astensione del lavoro) in una posizione di potenziale particolare svantaggio»; dall'altro, secondo il giudice di merito, la società convenuta non avrebbe assolto adeguatamente l'onere probatorio, non dimostrando la sussi-

[93] Tribunale di Bologna, Ord. del 31 dicembre 2020, cit., pag. 16 ss.
[94] *Ibidem.*

stenza di una finalità legittima e il carattere di appropriatezza e necessità dei mezzi impiegati nella gestione del rapporto di lavoro[95].

Questo caso dimostra chiaramente come anche da una mera omissione – come nel caso di specie la mancata considerazione della motivazione a causa della quale vi sia stata una tardiva cancellazione del turno oltre le previste ventiquattrore da parte del *rider* – si possano generare delle conseguenze negative a cascata che non consentono di garantire un'adeguata tutela della dignità e dei diritti dei lavoratori. Tali effetti, se non adeguatamente previsti, ponderati e gestiti possono portare a derive molto pericolose.

Per ciò che attiene alla tutela del diritto al lavoro vi è un altro profilo da considerare, ovvero quello di un contesto lavorativo tecnologico sempre più automatizzato.

A questo riguardo si prospetta la necessità di tutelare i lavoratori sotto un duplice profilo. Da una parte, dal rischio di esclusione e isolamento, nel caso di sostituzione da parte di nuove macchine in grado di svolgere determinate mansioni in tempi minori e in maniera più efficiente. Dall'altra parte, da tutti quei casi in cui, pur rimanendo nella quota occupazionale, i lavoratori si trovino a subire la supremazia delle macchine. In altre parole, si deve evitare non solo il diniego del diritto al lavoro[96], ma anche la discriminazione a dan-

[95] Ai sensi dell'art. 3, co. 6, d.lgs. n. 216/03. Si veda in dottrina l'esame del caso di M. PERUZZI, *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *LLI*, Vol. 7, No. 1, 2021, p. I-50.

[96] Proprio su questo punto, un gruppo di parlamentari europei sta ragionando su come diminuire i danni che la diffusione dei *robot* potrebbe causare e ha presentato alla Commissione europea un *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) Committee on Legal Affairs Rapporteur: Mady Delvaux (Initiative – Rule 46 of the Rules of Procedure).* Nella bozza, che dovrà poi essere vagliata dal Parlamento, sono evidenziate le sfide legali ed etiche che l'umanità dovrà affrontare con lo sviluppo dell'intelligenza artificiale e della robotica. In ballo ci sarebe "la sopravvivenza della specie". Il punto che ha fatto più discutere nella relazione è il passo in cui si chiede alla Commissione Europea di "creare nuove tasse per i proprietari di *robot* che devono contribuire alla previdenza sociale". La misura sarebbe pensata per proteggere gli esseri umani dalla disoccupazione crescente in settori sempre più automatizzati.

no dei lavoratori e a favore delle macchine, che ne causerebbe un'evidente lesione della dignità umana.

D'altronde, seppure probabilmente anche per mancanza di una visione completa delle opportunità insite nello sviluppo di sistemi di intelligenza artificiale, anche dal lato di impiego delle risorse, questo è uno dei fattori che maggiormente spaventa, man mano che la tecnologia continua ad avanzare[97]. La paura di essere sostituiti dalle nuove tecnologie è protagonista, anche perché continua a registrarsi e, anzi, si sta aggravando ulteriormente, un disallineamento tra istruzione, formazione e mercato del lavoro. La mancanza generalizzata di competenze nel digitale pesa sui lavoratori e sulla produttività, posto che molte aziende faticano considerevolmente a reperire sul mercato le professionalità di cui hanno bisogno[98].

[97] In realtà, l'intelligenza artificiale, seppure porterà la tecnologia a sostituire lavori a bassa specializzazione, contribuirà a creare nuovi posti di lavoro. È stato stimato che tra il 2020 e il 2022 si creeranno oltre sei milioni di nuove opportunità lavorative grazie all'automazione e altre applicazioni tecnologiche. Si veda lo studio del World Economic Forum, *Jobs of Tomorrow – Mapping Opportunity in the New Economy*, gennaio 2020, disponibile *online*.

[98] Qualcosa in Italia si sta muovendo in questo senso. Nell'ambito del PNRR è stato attivato il programma Italia digitale 2026, che contiene l'azione Competenze digitali con l'obiettivo di «colmare il gap di competenze digitali, con almeno il 70% della popolazione che sia digitalmente abile entro il 2026». Le informazioni sono disponibili nell'apposita sezione del sito del Dipartimento per l'Innovazione tecnologica e la transizione digitale (https://innovazione.gov.it/). Una delle iniziative strategiche è *Repubblica digitale*, descritta sulla pagina dedicata come «l'iniziativa strategica nazionale, promossa dal Ministro per l'innovazione tecnologica e la transizione digitale e coordinata dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio, che ha l'obiettivo di ridurre il divario digitale e promuovere l'educazione sulle tecnologie del futuro, supportando il processo di sviluppo del Paese». Sono previste quattro linee di intervento: la prima in tema di «Istruzione e Formazione Superiore – per lo sviluppo delle competenze digitali all'interno dei cicli d'istruzione»; la seconda riguarda «Il potenziamento e lo sviluppo delle competenze digitali della forza lavoro, sia nel settore privato che nel settore pubblico»; la terza tocca il tema dello «Sviluppo di competenze specialistiche ICT per nuovi mercati e nuovi posti di lavoro»; mentre la quarta è specificamente dedicata ai «Cittadini – per sviluppare le competenze digitali necessarie a esercitare i diritti di cittadinanza e la partecipazione consapevole alla vita democratica». I dettagli del programma sono disponibili sul sito del

In quest'ottica, servirebbe uno sforzo di medio lungo periodo, a diversi livelli, al fine di adeguare i programmi di istruzione, l'offerta di corsi formativi e professionalizzanti, considerato che lo sviluppo tecnologico non esaurisce la sua influenza nelle cosiddette materie STEM[99] ma ormai interessa tutti i settori disciplinari[100], non ultimi quelli umanistici.

Un aspetto strettamente collegato al precedente e propedeutico all'inserimento nel mercato del lavoro, è quello dell'acceso all'istruzione. Anche in quest'ultimo caso si sono registrati dei problemi quando per la selezione sono stati impiegati algoritmi[101].

Sono molte le università, particolarmente quelle statunitensi, che hanno iniziato ad impiegare algoritmi deterministici per gestire i processi di ammissione degli studenti. In questo caso, l'utilizzo di tali tecnologie può portare alla violazione del principio della parità di accesso all'istruzione. Tali sistemi, nella maggior parte dei casi, sono sviluppati su misura per soddisfare le preferenze della scuola e, per questo motivo, possono presentare alcune problematiche che potrebbero condurre a risultati discriminatori.

Ne è un esempio l'uso di dati storici, appartenenti a studenti precedentemente ammessi, per strutturare il modello. Molte delle università più prestigiose, infatti, sono storicamente frequentate da studenti di sesso maschile, bianchi e benestanti. Ciò avviene, in particolare, nelle università statunitensi, alcune delle quali notoriamente molto costose, dove i sistemi algoritmici di scelta vengono addestrati fornendo dati di precedenti studenti che, nella maggior parte

ministero https://repubblicadigitale.innovazione.gov.it/. Sul problema del *digital divide* si veda altresì il *report* di *AI4Belgium*, disponibile *online* e, in dottrina, per un'indagine generale si vedano i contributi di L. SARTORI, *Il divario digitale. Internet e le nuove disuguaglianze sociali*, Bologna, 2006, pp. 208 e ID., *Il digital divide*, Bologna, 2006, p. 20 ss. e J. VAN DIJK, *The digital divide*, Cambridge, 2020, p. 40 ss.

[99] STEM è l'acronimo di *Science Technology Engineering Mathematics*.

[100] Si vedano le riflessioni di I. TUOMI, *The Impact of Artificial Intelligence on Learning, Teching and Education, Policies for the future*, JRC Science for Policy Report, p. 27 ss. disponibile *online*.

[101] Il diritto all'istruzione trova tutela sia nella Carta di Nizza sia nella CEDU all'interno dell'art. 14.

dei casi, rispondono alle menzionate caratteristiche[102]. Qualsiasi modello algoritmico che utilizzi questi dati, rischia di perpetuare le tendenze del passato così come, applicando moduli di *machine learning*, i pregiudizi di sistema.

Questo potrebbe portare a università che utilizzano processi di selezione intrinsecamente discriminatori presentati però come obiettivi[103].

È evidente quindi, anche in questo caso, l'importanza di addestrare gli algoritmi con impostazioni corrette, dati accurati e completi per evitare, il più possibile, simili conseguenze pregiudizievoli.

Se l'intelligenza artificiale viene utilizzata per tracciare e prevedere il rendimento degli studenti, in modo tale da limitare la possibilità di studiare certe materie o di avere accesso a certe opportunità educative, il diritto all'istruzione rischia di essere messo seriamente a rischio.

Considerato poi che sempre più spesso sistemi di misurazione delle potenzialità e di predizione delle possibilità di successo vengono utilizzati anche su bambini, il rischio è che vengano limitate le opportunità per i ragazzi in età sempre più giovane, soprattutto nei confronti di quelli provenienti da contesti svantaggiati. Normalmente, infatti, gli studenti che crescono in realtà sociali complesse tendono ad avere esiti scolastici più negativi. Ne consegue che, se venisse utilizzato unicamente questo parametro, il rischio potrebbe essere quello di rafforzare le disuguaglianze educative esistenti e non dare pari opportunità a giovani che, seppur con minori possibilità economiche e con alle spalle situazioni sociali e familiari più sfidanti, vorrebbero impegnarsi per raggiungere il successo accademico e professionale.

V'è da dire però che, anche in questo caso, non tutto è negativo. Anche nel settore dell'istruzione, infatti, sono state evidenziate concrete potenzialità e sono emersi diversi possibili aspetti positivi derivanti dall'introduzione di tecnologie di intelligenza artificiale.

[102] Accessnow, *Human Rights in the age of artificial intelligence,* cit., p. 27.

[103] Si vedano le considerazioni di C. O'NEIL, *Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy*, New York, 2016, pp. 50-67.

Nella specie, si è visto che l'utilizzo di tali sistemi può migliorare i processi educativi non solo nelle classi ma anche ad un livello più alto che interessa la stessa programmazione didattica[104]. Strumenti di intelligenza artificiale potrebbero consentire agli studenti di personalizzare l'apprendimento, gestendo meglio le materie di studio e le tempistiche, adeguandole ai propri ritmi[105].

Nondimeno, occorre un governo di tali misure e una programmazione che introduca l'intelligenza artificiale nelle scuole in modo graduale e strutturato. L'obiettivo deve essere supportare l'apprendimento senza però azzerare la capacità critica e di analisi degli studenti. In altre parole, l'intelligenza artificiale non dovrebbe, come avvenuto nel ricordato caso di ChatGPT, essere utilizzata come mezzo "per fare di meno" bensì come strumento che potrebbe consentire di fare meglio in minor tempo, in altre parole, di ottimizzare il tempo da dedicare allo studio rendendolo più efficiente e produttivo.

6. Discriminazioni basate sulla razza: il rischio di procedure elettorali inique e la pratica del *Gerrymandering,* la valutazione del rischio di recidiva penale e i pericoli evidenziati nell'utilizzo dell'algoritmo COMPAS

I sistemi di intelligenza artificiale possono perpetuare e, addirittura, amplificare situazioni discriminatorie basate sulla razza.

[104] Si veda, al riguardo, OECD, *Directorate for Education and Skills, Trustworthy artificial intelligence (AI) in education: promises and challenge*, 6 aprile 2020, pp. 7-8, disponibile *online*.

[105] L'effetto positivo derivante dall'impiego di algoritmi nel settore dell'istruzione è stato dimostrato ad esempio nel programma di matematica *Teach to One*. Tale programma fornisce istruzioni che sono adattate alle abilità dei discendenti attraverso l'analisi delle del loro livello di partenza, proprio mediante l'utilizzo di algoritmi. Si veda per maggiori informazioni il sito dedicato. I. TUOMI, *The Impact of Artificial Intelligence on Learning, Teching and Education,* cit., p. 27 ss. Per alcune considerazioni ulteriori su tale punto si vedano altresì le conclusioni del presente lavoro.

Ne è un esempio il c.d. *Gerrymandering*[106]. Si tratta di una pratica molto preoccupante e rischiosa, per la stessa salvaguardia della democrazia partecipativa, che viene utilizzata per condizionare l'esito delle elezioni, al fine di assicurare a un partito o a uno specifico candidato di aggiudicarsi un numero di seggi maggiore rispetto a quello che normalmente avrebbe potuto ottenere affidandosi unicamente al voto popolare.

Tale pratica, finalizzata appunto a favorire un partito o un candidato specifico, viene normalmente messa in atto intervenendo *ad hoc* sul disegno dei distretti elettorali (c.d. *apportionment*) in modo da crearne alcuni sovrappopolati da elettori che sostengono un determinato partito o uno specifico candidato e altri in cui gli elettori sono dispersi tra più distretti, in modo che non abbiano alcun peso significativo in nessuno di essi.

Negli Stati Uniti, dove in effetti questa pratica è nata, è ammesso il *Gerrymandering* politico ma non quello razziale (c.d. *racial Gerrymandering*)[107].

[106] Per garantire pari opportunità ai candidati, i confini dei collegi elettorali dovrebbero essere stabiliti nella maniera più neutrale possibile. Quando invece i confini sono tracciati appositamente per favorire uno dei partiti in lizza, si usa il termine di *Gerrymandering*, coniato per antonomasia con riferimento a E. Gerry (governatore del Massachusetts all'inizio dell'Ottocento). Quest'ultimo, sapendo che all'interno d'una certa regione (dipartimento o stato), c'erano settori della popolazione (ben localizzabili) favorevoli a un partito o ad una specifica figura politica (ad esempio, seguendo le dicotomie centro/periferia, giovani/vecchi, ceto basso/ceto medio o alto), disegnò un nuovo collegio elettorale con confini particolarmente tortuosi, per incorporarvi parti della popolazione a lui favorevoli ed escludendo porzioni a lui sfavorevoli, al fine di garantire una possibile rielezione. Le linee di tale collegio erano così irregolari e tortuose, da farlo sembrare a forma di salamandra (da qui la seconda parte del termine dalla parola "*salamander*"). Una tecnica di *Gerrymandering* consiste nell'unire artificiosamente porzioni di territorio lontane geograficamente ma coese ideologicamente. Un'altra tecnica prevede l'abbinamento di quartieri urbani e periferie rurali (distribuendo il voto cittadino su più collegi) o, al contrario, isolare il capoluogo dalle periferie. Quando invece si attribuiscono seggi ai collegi senza proporzione con la consistenza demografica si parla più precisamente di *malapportioning*. Si veda Voce dedicata al *Gerrymandering* nell'enciclopedia Treccani, su *Treccani.it.* e in dottrina D. FISICHELLA, *Elezioni e democrazia. Un'analisi comparata*, Bologna, 2008, p. 131 ss.

[107] Negli Stati Uniti il *Gerrymandering* politico ovvero quella pratica che con-

È però evidente che l'intelligenza può elevare la pratica del *Gerrymandering* ad un livello superiore[108], sia in positivo sia in negativo. Gli algoritmi, infatti, possono essere facilmente utilizzati per creare mappe elettorali più eque, ma possono anche essere utilizzati per l'esatto opposto, ovvero per perpetuare discriminazioni razziali se i dati utilizzati per addestrare i modelli vengono raccolti in modo non equo oppure se i modelli vengono progettati in modo non imparziale.

Purtroppo, sebbene il *Gerrymandering* razziale sia vietato, non è inconsueto che casi del genere arrivino all'esame dei tribunali statunitensi[109]. Il rischio è che le applicazioni di intelligenza artificiale vengano impiegate per aggirare facilmente il divieto, utilizzando

siste nella manipolazione dei confini dei distretti elettorali per favorire un determinato partito è ammesso (così si è espressa anche la Suprema Corte degli Stati Uniti nel caso *Gill v. Whitford*, Supreme Court of the United States, 18 giugno 2018). Ciò che, al contrario, non è ammesso è il *Gerrymandering* razziale ovvero quella pratica che consiste nel manipolare i confini dei distretti elettorali al fine di sotto rappresentare determinate minoranze razziali (Corte Suprema degli Stati Uniti, *Cooper v. Harris*, 22 maggio 2017). Si veda per una compiuta spiegazione del fenomeno P. ANDREW, *Gerrymandering, explained*, in *Vox*, 9 maggio 2019, disponibile *online*.

[108] E. JORDAN, *How Computers turned Gerrymandering Into a Science*, in *New York Times*, 6 ottobre 2017, disponibile *online*.

[109] In realtà nonostante il divieto, la Corte suprema americana si è dovuta spesso misurare con problematiche di tipo razziale in ambito elettorale. In particolare, nella decisione resa nel caso *Bethune-Hill v. Virginia State Bd. of Elections*, 1° marzo 2017, la Corte è stata chiamata ad affrontare proprio questo tema e, in particolare, il disegno dei collegi elettorali nello Stato della Virginia di cui si era lamentato il carattere discriminatorio, in quanto sarebbe stato deliberatamente volto a favorire certe candidature a discapito di altre, in base a considerazioni di ordine razziale. Più precisamente, il contenzioso era stato originato dal ricorso con cui alcuni elettori avevano denunciato la violazione della *Equal Protection Clause* del Quattordicesimo Emendamento, da parte dalla previsione legislativa che – all'indomani del censimento del 2010 ed in vista dell'elezione dei "grandi elettori" nei dodici collegi elettorali dello Stato della Virginia – aveva stabilito che, in ciascuno, almeno il 55% della popolazione votante avrebbe dovuto essere di colore (cd. BVAP: *black voting-age population*). La Corte, in questa occasione, così come in altre precedentemente, ha evidenziato sul punto che «The Equal Protection Clause prohibits a State, without sufficient justification, from "separat[ing] its citizens into different voting districts on the basis of race».

l'affiliazione politica come *proxy* della razza e che la creazione di questo tipo di correlazione porti comunque ad una discriminazione, seppure in maniera indiretta.

Un secondo aspetto che merita di essere approfondito è l'impiego, ormai molto diffuso, di algoritmi predittivi in campo giudiziario, e, in particolare, l'utilizzo di sistemi algoritmici per la valutazione della recidiva in ambito penale.

Anche in questo campo, i risultati più preoccupanti arrivano da oltre oceano.

Nel sistema giudiziario americano, così come in quello canadese, si utilizzano già da tempo dei *software* utili a calcolare la percentuale di rischio di recidiva degli imputati e dei condannati per precedenti reati. Tali sistemi di *risk assessment* vengono utilizzati, sia per determinare le misure cautelari in corso di processo da applicare all'imputato sia, nell'ambito di alcune giurisdizioni[110], per determinare la pena finale e le eventuali circostanze aggravanti[111].

Ciò è quanto è accaduto nell'ambito di uno di questi processi, il molto discusso caso *Loomis* deciso dalla Corte Suprema del Wisconsin nel 2016[112].

Loomis, arrestato nel 2013 per ricettazione e resistenza a pubblico ufficiale, all'esito del processo era stato condannato ad una pena particolarmente severa, pari a sei anni di reclusione. La particolarità è da ravvisare nel fatto che l'ammontare di tale pena era stato in parte determinato tenendo in considerazione l'alto punteg-

[110] Ci si riferisce in particolare a: Arizona, Colorado, Delaware, Kentucky, Louisiana, Oklahoma, Virginia, Washington e Wisconsin.

[111] Si veda per un commento G.M. RUOTOLO, *Imparzialità e indipendenza dei giudici, intelligenza artificiale, diritto internazionale,* in S. CAFARO (a cura di), *Beni e valori comuni nella dimensione internazionale e sovranazionale – Atti del XXV Convegno annuale della Società italiana di Diritto internazionale e di Diritto dell'Unione europea (SIDI)*, Lecce, 24 e 25 settembre 2021, Napoli, 2022, p. 357 ss.

[112] *State v. Loomis, 881 N.W.2d 749 (Wisc. 2016)* nel quale la Corte Suprema del Wisconsin ha stabilito che l'impiego di algoritmi predittivi per la valutazione del rischio di recidiva non viola il diritto dell'imputato ad un equo processo. Per un commento S. CARRER, *Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in *Giurisprudenza Penale Web*, 2019, 4.

gio attribuito all'imputato da uno dei sistemi algoritmici predittivi del rischio di recidiva più diffusi[113], denominato COMPAS[114] (*Correctional Offender Management Profiling for Alternative Sanctions*).

La sentenza veniva impugnata da *Loomis,* il quale sosteneva che l'utilizzo da parte della Corte di un algoritmo predittivo per elaborare la sentenza di condanna si ponesse in contrasto con le garanzie processuali e il diritto di difesa dell'imputato[115]. *Loomis* sosteneva, in particolare, che COMPAS fosse un algoritmo proprietario il cui meccanismo di funzionamento non era stato reso noto dalla società proprietaria, in quanto tutelato da segreto industriale. Ne consegue che, secondo il ricorrente, non c'era modo di verificare se il pun-

[113] L. GIACOMELLI, *Big Brother is "gendering" you*, cit., pp. 218-219.

[114] COMPAS è uno degli algoritmi processuali maggiormente applicati, seppure in via sperimentale, negli Stati Uniti. Il brevetto è di proprietà di una società americana, la *Northpointe Inc*., ed inizialmente è stato sperimentato in un ristretto numero di corti di merito al fine di valutare, su una base statistica, la probabilità di recidiva dell'imputato al fine di quantificare la pena e le eventuali misure restrittive della libertà. Terminata la fase sperimentale, oggi il suo utilizzo è stato autorizzato ufficialmente da diversi Stati americani. L'algoritmo si basa su una serie di dati concernenti il passato, anche criminale, del soggetto le condizioni socio economiche e personali dell'imputato oltre a 137 domande a risposta vincolata. L'algoritmo elaborando tali dati calcola il rischio di recidiva su tre livelli *low, medium and high*. Il problema che è stato evidenziato è che, trattandosi di un algoritmo tutelato da brevetto, la modalità di funzionamento e le metodologie utilizzate per calcolare i rischi di recidiva non sono state rese note ai giudici. Ne consegue che risulta praticamente impossibile verificare in concreto la correttezza del calcolo effettuato dal *software* né capire fino in fondo il ragionamento utilizzato dal sistema. COMPAS processa tutte le informazioni inserite le suddivide in 12 sezioni: *current charges; criminal history; non-compliance; family criminality; peers; substance abuse; residence stability; social environment; education; vocation; leisure recreation; social isolation; criminal personality; anger and criminal attitudes*. Si vedano le riflessioni di T. BRENNAN, W. DIETERICH, B. EHRET, *Evaluating the predictive validity of the COMPAS risk and needs assessment system*, in *Crim. Just. Behav*., 2009, p. 21.

[115] Il ricorrente aveva sostenuto la violazione della *due process clause* prevista dal XIV Emendamento che prevede «[*omissis*] nor shall any State deprive any person of life, liberty or property, without due process of law, nor deny to any person within its jurisdiction the equal protection of the laws».

teggio elaborato a suo carico potesse effettivamente considerarsi il risultato di un processo oggettivo, imparziale e corretto. Inoltre, nell'impugnativa *Loomis* sosteneva altresì la non imparzialità dell'algoritmo posto che, seppur programmato per elaborare dati di *input* imparziali, si era mostrato particolarmente punitivo e severo nei confronti di soggetti di genere maschile e di razza non bianca.

Chiamata a risolvere il caso, la Corte Suprema, pur pronunciandosi a favore dell'utilizzabilità di algoritmi finalizzati a calcolare il rischio di recidiva penale, in questa occasione, ha altresì chiarito che il punteggio derivante dal calcolo algoritmico non può essere l'unico parametro tenuto in considerazione per assumere la decisione finale e che il giudice conserva sempre la propria discrezionalità. La Corte ha poi aggiunto, respingendo, in modo per la verità criticabile, le argomentazioni del ricorrente, che il fatto di tenere in considerazione anche altri fattori, quali il genere e la razza, sortirebbe esattamente l'effetto opposto rispetto a quanto sostenuto dall'imputato. La Corte, dunque, pur essendo consapevole dei rischi che si celano dietro all'utilizzo di tali algoritmi in giudizio, ha ritenuto che l'obbligo di motivazione e il divieto di fondare la decisione solo sul punteggio calcolato dall'algoritmo siano parametri sufficienti a salvaguardare i diritti di difesa e fondamentali dell'imputato[116].

Rendere noto il funzionamento dell'algoritmo appare, tuttavia, un requisito imprescindibile per poter garantire un corretto contraddittorio tra le parti, a maggior ragione in ambito penale, dove la parità processuale tra accusa e difesa, particolarmente nelle fasi delle indagini e in quella probatoria, non sempre sono effettivamente assicurate.

[116] In senso fermamente contrario all'utilizzo di algoritmi in ambito processuale K. FREEMAN, *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis*, in N.C. J.L. & Tech., 2016, 18, p. 75 ss., disponibile *online*. L'A. sostiene che perchè l'utilizzo di tali algoritmi sia effettivamente rispettoso dei diritti processuali, l'algoritmo dovrebbe diventare uno strumento *open source*, il cui buon funzionamento dovrebbe essere verificato da un supervisore terzo e imparziale. Inoltre, la difesa dovrebbe poterne analizzare il funzionamento per poter valutare la correttezza del punteggio elaborato a carico del proprio assistito.

La particolarità del caso *Loomis*, si evidenzia nel fatto che per la prima volta un algoritmo per il calcolo della recidiva sia stato utilizzato in fase di cognizione e il punteggio elaborato sia stato utilizzato pienamente come fonte di prova per elaborare la sentenza finale di condanna. Ne consegue che, salvo intervento contrario da parte della Corte Suprema federale, questa pronuncia, di fatto, apre alla possibilità di utilizzare simili algoritmi anche in ambito giudiziario e penale.

Tale scelta appare però criticabile. Allo stato attuale, infatti, manca una normativa chiara sullo sviluppo di tali sistemi oltre che un'adeguata e approfondita conoscenza dei meccanismi di funzionamento, inclusi quelli opachi, tali da consentirne indiscriminatamente l'utilizzo in contesti in cui in gioco vi è la libertà personale degli individui. Ad oggi, le garanzie e le tutele per gli imputati, di fronte all'utilizzo di tali sistemi, appaiono obiettivamente insufficienti. In primo luogo, perché continua a permanere un'opacità di fondo nel funzionamento di tali tecnologie e, di conseguenza, una difficoltà intrinseca di comprensione profonda, necessaria per valutare se effettivamente il ragionamento utilizzato dall'algoritmo, per elaborare un determinato risultato, sia o meno corretto e, soprattutto, se risulti, anche solo indirettamente, discriminatorio. In secondo luogo, si pone un problema di bilanciamento tra il diritto delle aziende proprietarie di tali sistemi a proteggere il segreto industriale e il diritto dell'imputato a conoscere appieno il funzionamento dell'algoritmo che ha calcolato l'ammontare della pena che gli verrà comminata, oltre ai parametri e al ragionamento che hanno condotto ad una determinata sentenza (a maggior ragione se di condanna).

La tutela della prima esigenza impedisce di rendere noto il funzionamento dell'algoritmo ma porta con sé inevitabilmente insufficienti tutele per l'imputato, soprattutto se per giudicarlo ciò che "decide l'algoritmo" assume un peso specifico troppo rilevante nella dialettica processuale e nelle ragioni che hanno condotto il giudice ad assumere una decisione e a redigere, di conseguenza, una determinata motivazione[117].

Questo è un tema che dovrà essere affrontato a livello normati-

[117] Così L. GIACOMELLI, *Big Brother is "gendering" you*, cit., p. 220.

vo, al fine di evitare che la giurisprudenza dei singoli Stati, in assenza di un quadro normativo chiaro, in una spinta interpretativa, crei una prassi, che poi verrà magari seguita da altre corti, e che metta a rischio la stessa libertà personale degli individui[118].

7. Discriminazioni basate su religione, credenze e opinioni politiche

L'intelligenza artificiale può altresì creare discriminazioni sulla base di credenze religiose e opinioni politiche.

Ne sono un esempio, di certo non virtuoso, i colossi come Facebook, in cui l'algoritmo di visualizzazione delle notizie mostrava agli utenti contenuti polarizzati e dannosi, selezionati in base alle loro preferenze politiche, e Google, che è stato accusato di discriminazione nella pubblicità *online*, poiché proponeva annunci diversi agli utenti in base alla razza, al genere e all'orientamento sessuale[119].

[118] Si veda anche HUMAN RIGHTS COMMITTEE, *General Comment No. 32, Article 14: Right to equality before courts and tribunals and to a fair trial*, U.N. Doc. CCPR/C/GC/32 (2007) e, in dottrina, le considerazioni di S. GLESS, *AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials*, in *Georgetown Journal of International Law*, 2020, vol. 51, n. 2, pp. 195-253; J. LARSON, L. ANGWIN, S. MATTU, L. KIRCHNER, *Machine Bias. There's Software Used Across the Country to Predict Future Criminals. And it's Biased against Blacks, ProPublica*, 23 maggio 2016, disponibile *online*. Si vedano altresì i contributi di A. COWGER, *The Threats of of Algorithms and AI to Civil Rights, Legal Remedies, and American Jurisprudence: One Nation Under Algorithms*, 2020, Lanham, p. 276 e ss.; M. CAIANELLO, *Potenzialità e rischi derivanti dall'interazione tra I.A. e giustizia penale preventiva*, in U. Ruffolo (A cura di), *XXVI Lezioni di Diritto dell'Intelligenza artificiale*, cit., p. 206 e ss., e anche L. FREEMAN, *Digital Evidence and War Crimes Prosecutions*: *The Impact of Digital Technologies and International Criminal Investigations and Trials,* in *Fordham International Law Journal*, 2018, 41, 2, p. 283 ss.; O. LYNSKY, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing*, in *International Journal of Law in Context*, 2019, pp. 162-176.

[119] Ad esempio, gli algoritmi di riconoscimento delle immagini di Google hanno erroneamente categorizzato due persone di colore ritratte in una foto per due gorilla, si veda J. VINCENT, *Google 'Fixed' its Racist Algorithm by Removing*

Nell'ambito della tutela delle opinioni politiche e delle convinzioni personali, alcuni rischi sono legati ad un utilizzo di sistemi di intelligenza artificiale per la diffusione di notizie false[120] e per alterare la creazione e la formulazione delle informazioni e l'accesso alle stesse.

La sorveglianza basata sull'intelligenza artificiale potrebbe, infatti, pregiudicare la partecipazione politica se utilizzata per identificare e scoraggiare determinati gruppi dal recarsi al voto o per influenzarne la preferenza[121]. Se comportamenti del genere si dovessero ripetere con frequenza, questo potrebbe dare origine ad un *loop* negativo di sfiducia nella legittimazione dell'azione politica e nell'utilità stessa di un caposaldo fondamentale della democrazia partecipativa[122], ovvero il diritto di voto[123].

Peraltro sistemi di intelligenza artificiale potrebbero essere utilizzati addirittura per diffondere in modo intenzionale delle notizie che, creando disinformazione, finiscono per generare odio sociale,

Gorillas from its Image-Labeling Tech, The Verge, 12 Gennaio 2018, disponibile *online* e si vedano altresì le riflessioni di L. HARDESTY, *Study finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems. Examination of Facial-Analysis Software Shows Error Rate of 0.8 Percent for Light-Skinned Men, 34.7 Percent for Dark-Skinned Women*, in *MIT News*, disponibile *online*.

[120] Si veda sul punto G.M. RUOTOLO, *Social Networks: Libertà d'opinione, fake news e hate speech,* in *Scritti di diritto internazionale ed europeo dei dati*, 2021, Bari, 2021, p. 229.

[121] È quanto accaduto ad esempio nelle elezioni presidenziali del 2016 negli Stati Uniti dove l'utilizzo di algoritmi sui *social* ha contribuito alla diffusione di notizie false a sfavore della Clinton e a favore di Trump. Alcuni quotidiani hanno denunciato che anche il coinvolgimento di *trolls* russi abbia contribuito ad influenzare l'esito delle elezioni presidenziali americane.

[122] Si veda su questo specifico aspetto G. MORGESE, *Principio e strumenti della democrazia partecipativa nell'Unione europea*, in E. Triggiani (a cura di), *Le nuove frontiere della cittadinanza europea*, Bari, 2011, p. 37 ss.

[123] Per un esame approfondito dei rischi che l'utilizzo di sistemi di intelligenza artificiale potrebbe comportare sulla tutela dei diritti collettivi si veda C. SCHEPISI, *Diritti fondamentali, principi democratici e rule of law: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, in A. Paino, F. Donati, A. Perrucci (a cura di), cit., p. 203 e ID., *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in Quaderni AISDUE, Atti convegni AISDUE, n. 16, 28, 2022, p. 330 ss.

escalation di violenza, episodi di razzismo o addirittura conflitti armati[124].

Una notizia falsa che circola all'interno di un "quartiere" ha conseguenze negative, seppur potenzialmente gravi, certamente circoscritte. Una notizia falsa in mano ad un sistema di intelligenza artificiale può diventare virale nel giro di pochi minuti e raggiungere i quattro angoli del mondo nello stesso esiguo lasso temporale. La portata negativa può diventare ancor più devastante, tenendo in considerazione le intenzioni malevoli di chi l'ha creata *ad hoc*.

I sistemi di riconoscimento biometrico potrebbero sfociare in pratiche di sorveglianza di massa con il rischio di scivolare nell'autoritarismo[125] e in forme di controllo generalizzate finalizzate a controllare proteste e manifestazioni ed ostacolare la libertà di associazione, di aggregazione pacifica e finanche di pensiero.

La costante sensazione di controllo potrebbe inoltre scoraggiare i cittadini dall'esprimere liberamente le loro idee, andando così a minare anni di faticose conquiste, in termini di libertà di pensiero e libera espressione dello stesso.

In tale prospettiva appare assolutamente cruciale che le aziende che utilizzano tecnologie di intelligenza artificiale siano assolutamente trasparenti sulle modalità con cui vengono utilizzati i dati degli utenti e che adottino tutte le misure necessarie per prevenire questo tipo di discriminazioni nei loro sistemi.

8. I rischi di discriminazione insiti negli algoritmi vision del genere *"unsupervised"*

A differenza del più conosciuto e utilizzato apprendimento supervisionato, l'apprendimento *"unsupervised"* si verifica quando i dati di *input* utilizzati per addestrare gli algoritmi non sono etichet-

[124] K. SCHOORS, *Ai en digitale dictatuur,* in J. De Bruyne, N. Bouteca (a cura di), *Artificiële intelligentie en maatschppij*, Turnhout, 2021, p. 20 ss.

[125] Si vedano le riflessioni di C. SCHEPISI, *Diritti fondamentali, principi democratici e rule of law: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, cit., p. 203 ss.

tati o non hanno un corrispondente valore di *output* ed è lo stesso algoritmo, attraverso moduli di *machine learning*, ad identificare eventuali relazioni esistenti tra gli stessi[126].

L'utilizzo di tali tipologie di modelli è adatto a cercare relazioni nascoste nei dati che sfuggono all'osservazione, magari perché oscurate da altre informazioni oppure perché la quantità di dati è talmente grande da non poter essere osservata facilmente senza un ausilio computazionale.

Questi modelli di apprendimento riescono a realizzare operazioni molto più complesse rispetto a quelle del caso supervisionato, proprio perché sono in grado di apprendere direttamente dai dati senza il bisogno di un *dataset* di addestramento[127]. La funzione di questi algoritmi è quella di estrarre, da un *database,* le relazioni e le somiglianze esistenti tra i dati in esso contenuti. In questa famiglia, vi rientrano, ad esempio, gli algoritmi utilizzati per individuare interessi comuni tra gli utenti, per inviare promozioni mirate ed efficaci (*targeted marketing*). Sono algoritmi che non fanno predizioni (come i loro gemelli *supervised*), ma che tentano di estrarre caratteristiche (*features*) da immensi *dataset* allo scopo di suddividere i dati in gruppi affini per una o più caratteristiche; oppure che hanno

[126] Gli algoritmi di apprendimento non supervisionato possono essere essenzialmente ricondotti alla seguenti categorie: Algoritmi di *clustering*: i dati di *input* sono raggruppati in diversi *cluster* in base alla similarità delle loro caratteristiche; Algoritmi associativi: consentono di associare le variabili in grandi *database* secondo relazioni predefinite; Algoritmi di riduzione della dimensionalità: in presenza di un numero elevato di dati di *input* permettono di estrarre le caratteristiche più importanti o di ricombinare i dati di partenza per ottenere componenti separate.

[127] La funzione di questi algoritmi è quella di estrarre da un data base le relazioni e le somiglianze esistenti tra i dati in esso contenuti. In questa famiglia, vi rientrano ad esempio gli algoritmi utilizzati per individuare interessi comuni tra gli utenti, per inviare promozioni mirate ed efficaci *(targeted marketing).* Sono algoritmi che non fanno predizioni (come i loro gemelli "*supervised*"), ma che tentano di estrarre caratteristiche (*features*) da immensi *data set* allo scopo di suddividere i dati in gruppi affini per una o più caratteristiche; oppure che hanno l'obiettivo di individuare certe correlazioni tra i dati per definire, a sua volta, regole generali ricorrenti.

l'obiettivo di individuare certe correlazioni tra i dati per definire regole generali ricorrenti.

Queste attività di *clustering* o di associazione hanno forti implicazioni etiche, poiché dividere, estrarre, associare, sono tutte attività che suggeriscono un processo di categorizzazione dei dati da cui, per ovvi motivi, possono emergere pregiudizi o stereotipi, che riflettono sentimenti o pensieri ricorrenti all'interno di un gruppo o di una determinata società.

In un recente studio[128], in cui sono stati esaminati per la prima volta modelli di rappresentazione dell'immagine del genere *unsupervised*, è stato dimostrato che tali modelli apprendono automaticamente e incorporano pregiudizi sociali che potrebbero avere effetti dannosi proprio dal momento che nessuna categoria o etichetta viene utilizzata nella fase di *training* dell'algoritmo[129].

Nel corso di questo studio, a partire dallo IAT, ovvero il *test* utilizzato per misurare i *bias* negli algoritmi di elaborazione del linguaggio naturale (NLP) sono stati sviluppati degli IEAT (*Image Embedding Association Test*). Si tratta del primo metodo utilizzato per rilevare e quantificare i *social bias* appresi da immagini non etichettate applicando lo stesso meccanismo di rilevamento utilizzato per riconoscere *bias* all'interno delle parole, anche alle immagini.

Per la fase di *training*, gli studiosi hanno utilizzato ImageNet 2012, uno dei *database* più diffusi contenente immagini selezionate estratte dal *web*, scegliendo come modelli per la rappresentazione dell'immagine, Sim-CLRv2 e iGPT, quest'ultimo divenuto particolarmente noto in quanto si tratta del primo modello in grado di completare immagini ritagliate o parziali.

Gli studiosi hanno voluto utilizzare il cosiddetto approccio *Transfer Learning*, che consiste appunto nell'utilizzare modelli algoritmici di avanguardia che vengono preliminarmente addestrati su

[128] Lo studio è stato condotto da Ryan Steed (Carnegie Mellon University) e Aylin Caliskan (George Washington University) dal titolo *Image Representations Learned With Unsupervised Pre-Training Contain Human-like Biases*, in *arXiv:2010.15052 [cs.CY]*, 27 gennaio 2021, disponibile *online*.

[129] Lo studio è stato esaminato da A. BALDRATI, *Se l'algoritmo diventa lo specchio dei nostri stereotipi: uno studio,* in *Agenda Digitale,* 26 febbraio 2021, disponibile *online*.

set di dati di grandi dimensioni, così da ridurre esponenzialmente i costi della fase di *training* prima del *fine tuning*, ovvero quella fase di messa a punto del modello per adattarlo alle esigenze e ai compiti specifici di un determinato scenario applicativo.

Sono stati riprodotti due tipologie di test: il *Valence test*, in cui due concetti e/o elementi sono testati per associazione con immagini piacevoli (*pleasant*), quindi di alta valenza, oppure sgradevoli (*unpleasant*), cioè di bassa valenza[130] e lo *Stereotype test*, attraverso il quale due concetti sono testati associandoli ad una coppia di attributi stereotipati[131].

In particolare, durante lo studio, sono stati applicati otto dei pregiudizi sociali più diffusi, da quelli innocui, se applicati a categorie come insetti e fiori, a quelli potenzialmente dannosi, come razza e genere, ma anche peso e disabilità.

Purtroppo lo studio ha restituito risultati preoccupanti. Nel *test* di valenza, entrambi i modelli hanno mostrato un *bias* significativo quando è stata misurata l'associazione tra immagini di cittadini americani di origini arabe, con i parametri *pleasant* e *unpleasant*, registrando una forte propensione dell'algoritmo a collegarli al concetto di non piacevolezza.

Inoltre nel test *Gender-Career* è stato dimostrato che l'algoritmo tende a collegare molto più spesso la categoria "maschio" con attributi legati alla carriera come "*business*" e "ufficio" e la categoria "femmina" con prerogative che rimandano al concetto di famiglia come "bambini" o "casa".

Il modello iGPT ha poi mostrato un *bias* nell'associare le persone magre con il concetto di piacevolezza e le persone in sovrappasso con il concetto opposto e, nel caso dell'*Intersectional bias*, ovvero quei casi in cui il *bias* prende vita dall'intersezione di più caratteristiche e identità personali, il modello iGPT generalmente ha mostrato una valenza positiva verso i bianchi e una tendenzialmente negativa verso le persone di colore. Nondimeno, tra tutti i *test* effettuati il disvalore più grande è stato registrato fra uomini bianchi e

[130] Ad esempio "sole" e "pioggia" potrebbero essere associati ad immagini che esprimono rispettivamente un senso di piacevolezza o non piacevolezza.

[131] Ad esempio "uomo/donna", "carriera/famiglia".

donne di colore, quest'ultime associate ad una valenza molto negativa rispetto agli uomini bianchi associati, al contrario, a valutazioni molto positive.

Questo studio, di certo significativo, dimostra con allarmante chiarezza come il problema non sia effettivamente solo la tecnologia ma il fatto che è la struttura sociale a dover essere corretta. In questi casi, infatti, i *bias* e le possibili discriminazioni discendenti non sono affatto legate ad opacità di fondo dei processi decisionali algoritmici ma, semplicemente, vengono riproposte in modo fedele le tipologie di immagini che è possibile rinvenire sul *web*, che altro non è che lo specchio delle società. Non è un caso che le categorie all'interno di ImageNet mostrino una disparità nella rappresentanza di alcuni generi o razze.

Queste disparità creano favoritismi verso una data categoria, dando vita alla gran parte dei *bias* esistenti, poi assorbiti dagli algoritmi stessi. È indubbio, infatti, che i modelli *unsupervised* siano influenzati dalla collocazione abituale di certi gruppi sociali in determinati contesti.

In definitiva questo studio ha dimostrato che se da una parte il *Transfer Learning* permette di contenere i costi della fase di *training* degli algoritmi, dall'altra, l'uso incauto di tali modelli algoritmici può condurre, ovviamente, a risultati gravi perché può amplificare esponenzialmente la portata discriminatoria dei pregiudizi e degli stereotipi della società[132].

Occorre dunque utilizzare questi modelli in modo consapevole, prendendo coscienza del fatto che seppur la tecnologia, di per sé, potrebbe essere neutrale, potrebbe essere la società in cui opera a non esserlo, quindi occorre intervenire per "correggere" i dati, adottando l'auspicato approccio *by design,* in modo che l'elabo-

[132] Nel corso dello studio i ricercatori hanno selezionato cinque volti artificiali di aspetto maschile ed altrettanti di aspetto femminile. Dopo aver ritagliato i volti all'altezza del collo, è stato chiesto al modello iGPT di completare ogni immagine in otto versioni diverse. Nel 52,5% dei casi l'algoritmo ha scelto di vestire l'uomo con un abito mentre la donna, nel 42,5% dei casi, è stata rappresentata con un *bikini* o con una scollatura.

razione algoritmica restituisca risultati il più possibile scevri da stereotipi o da pregiudizi sociali.

9. Conclusioni

Quello dell'intelligenza artificiale è un settore complesso e contraddittorio. Basti riflettere sul fatto che nonostante la diffidenza verso queste tecnologie, i timori che possano superare le abilità umane e, dunque, sostituire i lavoratori, quando si pensa alle macchine l'associazione immediata che la mente restituisce è: affidabilità. Se il risultato è generato da un algoritmo si tende a darne per scontata la sua esattezza.

Nondimeno quanto sin qui esaminato ha posto in luce tutti i limiti, non solo di una simile (fallace) impostazione di pensiero, ma anche di queste stesse tecnologie.

In parte perché, come evidenziato, il modello etico che la macchina è destinata a replicare (potenzialmente all'infinito) è impresso dall'uomo. Come detto, questi sistemi sono programmati per compiacere e assecondare una certa "sensibilità" pubblica. Il caso cinese esaminato, sotto diversi punti di vista, è emblematico. Imporre all'intelligenza artificiale il rispetto di valori socialisti, ovviamente, significa obbligare gli sviluppatori, che implementano i sistemi, ad inserire negli stessi un'impronta che sia idonea a soddisfare tale richiesta e a consentire il rispetto di un simile obbligo. Con buona pace della neutralità dell'algoritmo. Un simile sistema non potrebbe, evidentemente, trovare applicazione in nessun ordinamento occidentale perché, diversamente, restituirebbe dei risultati non in linea con il sentire comune, ma nemmeno in qualsiasi paese che vanti una tradizione socio culturale rispettosa del libero pensiero, anche dal punto di vista politico.

Considerato, pertanto, che il sistema valoriale recepito dall'algoritmo è quello imperante nella comunità in cui dovrà operare, è anche destinato a replicarne le discriminazioni, dirette o indirette, esplicite o celate che siano. L'opacità di questi sistemi e l'impossibilità di un controllo umano *in itinere*, eventualmente pronto ad intervenire per "correggere" correlazioni statistiche non

corrette perché magari slegate dal significato o dal contesto, certamente aggravano il problema.

CONCLUSIONI

SOMMARIO: 1. Prime considerazioni. – 2. Il ruolo del legislatore europeo nel governo dell'intelligenza artificiale. – 3. La tenuta dell'attuale assetto normativo in tema di diritti fondamentali dinanzi al prepotente imporsi sulla scena dell'intelligenza artificiale. Sono necessari nuovi diritti "digitali"? – 4. L'intelligenza artificiale come possibile strumento per la promozione dei diritti fondamentali.

1. Prime considerazioni

L'analisi condotta nelle pagine che precedono ha consentito di mettere in luce una serie di problematiche giuridiche che le istituzioni sovranazionali dovranno considerare con attenzione, se vorranno tentare di dare all'Unione europea un suo ruolo e, perché no, una sua centralità nel panorama mondiale di regolamentazione dell'intelligenza artificiale.

Nel corso del presente scritto ci si è soffermati sui possibili rischi che potrebbero profilarsi per gli utenti *online* in ragione dell'impiego di sistemi di intelligenza artificiale, anche alla luce della regolamentazione contenuta all'interno della nuova proposta di regolamento presentata dalla Commissione europea. Nella specie, l'analisi ha preso in considerazione i profili della tutela dei dati personali e delle discriminazioni, dirette e indirette, che tali sistemi potrebbero generare. Si è proceduto poi ad una disamina dell'attuale impianto di tutela dei diritti fondamentali, così come delineato dalla Carta di Nizza, dalla CEDU ma anche dal GDPR, per tentare di valutarne la resilienza dinanzi alla prepotente diffusione di tali nuove tecnologie, che lavorano mediante l'impiego di algoritmi sempre più sofisticati.

Si è ritenuto opportuno iniziare, discostandosi momentaneamente dal campo strettamente giuridico, delineando un quadro generale volto ad introdurre il tema dell'intelligenza artificiale, chiarendo, innanzitutto, di cosa si tratti, analizzandone i progressi nel corso del tempo e descrivendo il processo attraverso il quale gli al-

goritmi sono arrivati oggi ad applicare meccanismi di apprendimento automatico che sollevano molti dubbi ed interrogativi a causa dell'opacità che spesso caratterizza il loro funzionamento.

Nel valutare positivamente o negativamente l'intelligenza artificiale, si è anche evidenziato che non se ne può trascurare il potenziale nell'ottica di affrontare in modo efficiente, se non addirittura risolutivo, alcune delle urgenti sfide dei tempi moderni, da cui dipende la stessa sopravvivenza del genere umano. L'ottimizzazione dell'efficienza energetica, la lotta al cambiamento climatico, la fame nel mondo, la soluzione ad alcune malattie mediante l'impiego di algoritmi predittivi, la gestione e l'ottimizzazione delle risorse naturali, la conservazione della biodiversità, sono questioni che attendono risposte, che non possono più essere procrastinate. In questa direzione, i primi dati hanno dimostrato che i sistemi algoritmici possono essere utilmente impiegati in diversi campi con risultati apprezzabili.

Nondimeno, dall'analisi svolta all'interno dei capitoli IV e V, è purtroppo altresì emerso che queste nuove tecnologie pongono delle problematiche rilevanti in tema di tutela dei diritti fondamentali degli individui. Si pensi ai risultati che si sono esaminati in conseguenza dell'applicazione di algoritmi nei settori giudiziario o lavorativo, al caso COMPAS o Deliveroo, di come tali tecnologie abbiano dimostrato di incamerare i pregiudizi umani e di restituire risultati a contenuto discriminatorio, anche in assenza di una reale consapevolezza da parte degli sviluppatori.

I profili esaminati rendono legittimo ritenere che, principalmente in virtù dello sviluppo rapidissimo che stanno avendo queste tecnologie e degli impieghi già in atto nei settori più diversi, deve considerarsi ampiamente iniziato, e probabilmente già parzialmente trascorso[1], il tempo in cui le istituzioni europee dovrebbero intervenire per regolamentare e governare questo settore in modo che sia garantita una sufficiente tutela dei diritti fondamentali degli individui. Parte della dottrina, in modo condivisibile, ha evidenziato

[1] Sul ritardo nell'adozione del regolamento si veda v. M.R. CARBONE, *Regolamento europeo sull'intelligenza artificiale in ritardo*, ecco perché, in *Agenda Digitale*, 22 febbraio 2022, disponibile *online*.

che sarebbe necessario «interiorizzare i valori tutelati del diritto costituzionale nelle macchine» e che occorrerebbe intervenire «quando scienziati e tecnologi sono ancora in formazione per spiegare il valore di principii quali la "*privacy by design*" oppure il principio della "comprensibilità" degli algoritmi predittivi»[2].

Il problema è anche da rinvenirsi, come evidenziato all'interno del capitolo V del presente scritto esaminando il caso cinese o la risposta statunitense, che la corsa all'intelligenza artificiale sembra assumere sempre di più connotati politici e i contorni di una "corsa all'armamento digitale". Il rischio è che, così come nell'ambito dei conflitti armati in cui i diritti dei singoli passano inesorabilmente in secondo piano, la corsa alla supremazia digitale "lasci indietro gli individui". L'attenzione per la prospettiva competitiva ed economica, di cui Cina e Stati Uniti sono i principali fautori, attualmente supera, di gran lunga, quella per la tutela dei diritti degli individui. Questo può tradursi in un rischio importante per gli esaminati sistemi di salvaguardia dei diritti fondamentali, la cui tenuta sarà messa a dura prova.

Eppure, l'analisi svolta all'interno dei capitoli II e III, nel delineare il quadro normativo in materia di intelligenza artificiale in prospettiva europea, ha fatto emergere una visione delle istituzioni sovranazionali parzialmente differente da quella sostenuta dai due ricordati *competitors* internazionali.

Come si è evidenziato, infatti, la proposta di regolamento, ma anche gli atti precedenti, pongono fortemente l'accento sulla creazione di un "ecosistema di fiducia" e di un'intelligenza artificiale etica e antropocentrica. L'Europa sta dimostrando, almeno sulla carta, di voler adottare una visione differente da quella proposta da Cina e Stati Uniti. È indubbio, infatti, che non voglia perdere la sfida in termini di competitività sui mercati mondiali, ma è altresì ve-

[2] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista internazionale di filosofia del diritto,* 1, 2019, p. 87 ss. e spec. p. 103. Gli A. evidenziano che «[d]al momento che la tecnologia è sempre più integrata con la vita delle persone, occorre che valori come la dignità e la libertà della persona stessa divengano parte integrante della formazione di coloro che poi lavoreranno a quelle tecnologie. Di qui il ruolo delle agenzie formative ovvero delle associazioni professionali o accademiche».

ro, che non sembra disposta a pagare, come prezzo, il sacrificio dei diritti fondamentali. Occorrerà vedere se poi, alla prova dei fatti, nella scelta tra attrarre investimenti o tutelare gli individui, le istituzioni saranno in grado di mantenere la posizione garantista inizialmente prospettata e, soprattutto, se questa verrà mantenuta nel testo definitivo del regolamento, una volta che sarà adottato.

A tale riguardo, occorre porre in evidenza che la presente analisi, pur avendo tentato uno sforzo ricostruttivo dell'attuale panorama normativo in tema di intelligenza artificiale e delle applicazioni più diffuse e avendo tenuto conto delle attese prossime evoluzioni, non può avere alcuna pretesa di completezza. Il fatto che non sia ancora giunto al termine l'*iter* legislativo della proposta di regolamento sull'intelligenza artificiale lascia aperti ancora molti interrogativi che richiederebbero ulteriori riflessioni, ma le cui risposte dipendono in maniera sostanziale dalla posizione che il legislatore europeo deciderà di adottare.

Nondimeno, ciò che è emerso con evidenza, sulla base di questa iniziale analisi svolta, è che quello dell'intelligenza artificiale, dei *Big Data* e dell'*Internet of Things,* sono temi che non possono essere settorializzati o circoscritti. Al contrario, per tentare di garantire una certa protezione agli individui, particolarmente al cospetto dei colossi del digitale, la sfida deve necessariamente essere affrontata su un livello territoriale e normativo che sia il più vasto possibile, anche in considerazione della crescente smaterializzazione e deterritorializzazione dei rapporti giuridici[3]. Come è stato osservato trattando all'interno del capitolo IV dei possibili profili di interferenza e di coordinamento con il GDPR, è la natura stessa del fenomeno dell'intelligenza artificiale, così come lo era stato, anni prima, quello della *privacy*, a richiedere un livello di normazione di tipo europeo[4].

[3] Di «questione eminentemente transnazionale, e come tale difficilmente ricomponibile ricorrendo alla tradizione giuridica singolo-nazionale», parla A. VENANZONI, *Intersezioni costituzionali – Internet e Intelligenze Artificiali tra ordine spontaneo, natura delle cose digitale e garanzia dei diritti fondamentali*, in *Forum di Quaderni Costituzionali*, 27 aprile 2018, p. 4.

[4] C. BERGONZINI, *"Prova a prendermi". Ecosistema digitale e consapevolezza degli utenti: uno spazio per la regolazione nazionale?*, in *Osservatoriosullefonti.it*, 2, 2022, p. 17 ss. e anche in G. Di Cosimo (a cura di), *Processi democratici e tecnolo-*

Posto quanto sopra, di seguito si riporteranno alcune riflessioni conclusive in aggiunta a quanto già evidenziato nei paragrafi che precedono.

Ci si soffermerà in particolare su tre punti: un primo aspetto riguarderà il ruolo che ci si può ragionevolmente attendere da parte del legislatore europeo nel governo dell'intelligenza artificiale e i possibili profili di criticità che potrebbero emergere (e che in parte sono già emersi nell'esaminata proposta di regolamento); in secondo luogo, saranno svolte alcune riflessioni sulla tenuta dell'esaminato assetto normativo in tema di diritti fondamentali dinanzi al prepotente imporsi sulla scena dei nuovi sistemi algoritmici e se siano o meno necessari nuovi diritti digitali a tutela degli utenti *online* e, da ultimo, si svilupperanno alcune considerazioni volte a capire se sia ragionevole ipotizzare che i sistemi di intelligenza artificiale possano essere utilizzati come strumento per promuovere la tutela dei diritti fondamentali e, in caso di risposta affermativa, in che termini.

2. Il ruolo del legislatore europeo nel governo dell'intelligenza artificiale

Seppur raccogliendo dati ancora incompleti derivanti da quelle che potremmo definire sporadiche applicazioni rispetto alle potenzialità di tali tecnologie – l'esame che precede ha posto in evidenza, con sufficiente chiarezza, che i sistemi di intelligenza artificiale sono in grado di generare rischi significativi per gli utenti *online*, soprattutto per quanto riguarda la tutela della *privacy* e le possibili discriminazioni.

Di fronte ad un simile scenario, riflettendo sul ruolo a cui è chiamato il legislatore europeo, non pare né prudente né tantomeno ragionevole pensare di agire *a posteriori,* andando ad intervenire su prassi commerciali ormai consolidate. Il rischio sarebbe quello di generare delle «bolle giuridiche»[5]. D'altra parte, i risultati discen-

gie digitali, in *Osservatorio sulle Fonti, Collana di Studio*, Torino, 2023, p. 91 ss.

[5] Ovvero quel fenomeno che tende a verificarsi quando gli operatori econo-

denti dalle prime applicazioni di sistemi algoritmici, quantomeno nei diversi settori che sono stati presi in esame nel corso del presente scritto, particolarmente all'interno dei capitoli IV e V, offrono al legislatore europeo elementi assai significativi, seppure certamente ancora parziali, che suggeriscono la necessità che l'Unione europea si doti, il prima possibile, di una normativa chiara e sufficientemente garantista in materia. Diversamente, oltre alla minaccia per la tutela dei diritti individuali, si rischierebbe, come avvenuto con il GDPR, di ingenerare una gran confusione negli operatori del settore che, nel dubbio di trovarsi nella condizione di non saper più distinguere ciò che è lecito da ciò che non lo è, decidano semplicemente di non investire in un settore in cui i possibili rischi superino di gran lunga le potenzialità di generare profitti. Sfortunatamente, nel campo dell'innovazione tecnologica, tra i più competitivi e dispendiosi in termini di risorse, gli investimenti privati in ricerca e sviluppo – effettuati perlopiù dalle *Big Tech* – risultano vitali per la crescita del settore ed è indubbio che un clima di incertezza giuridica rappresenti un forte disincentivo in tal senso. Di contro, se ci si pone dal punto di vista della prospettiva considerata nella presente analisi, ovvero quella individuale e, particolarmente, della tutela dei diritti fondamentali degli utenti *online*, sono proprio le *Big Tech* a dover essere "controllate" con particolare attenzione, sia per l'enorme potenziale lesivo, in termini di bacino di utenza, che le loro azioni potrebbero generare, sia perché, essendo tanto forti da un punto di vista economico, mere sanzioni pecuniarie, come quelle che si è visto essere previste all'interno della proposta di regolamento sull'intelligenza artificiale, potrebbero non rivelarsi un rimedio sufficiente. Sarebbe forse più opportuno inserire, in aggiunta alla sanzione pecuniaria, dei veri e propri divieti assoluti di utilizzo dei sistemi di cui dovesse venire accertato un potenziale lesivo, a cui dovrebbe seguire una segnalazione specifica del relativo codice algoritmico all'interno di elenchi dedicati da condividere con le

mici investono nello sfruttamento economico di una nuova risorsa in un contesto di incertezza e ignoranza sulle implicazioni legali delle attività innovative cfr. M. GIRAUDO, *On legal bubbles: some thoughts on legal shockwaves at the core of the digital economy,* in *Journal of Institutional Economics,* 2022, 18, pp. 587-604.

singole autorità nazionali, il cui ruolo nelle procedure di verifica e controllo dovrebbe essere maggiormente esteso ed incisivo.

Se le *Big Tech* mirano a sottrarre i sistemi di intelligenza artificiale alle regole, il legislatore europeo deve muoversi esattamente nella direzione contraria, imponendo una normativa chiara e rigorosa. È stato ipotizzato in dottrina, che sarebbe opportuno, a margine dell'approccio *risk-based*, prevedere un sistema di «illegalità di *default*» per i sistemi di intelligenza artificiale, ovvero un modello *ex ante* in cui siano gli sviluppatori ad avere l'onere di dimostrare che la loro tecnologia non risulti discriminatoria, manipolativa, ingiusta, imprecisa e persegua finalità legittime. In altre parole, un modello di pre-approvazione che preveda, però, una presunzione di illegalità e un'inversione dell'onere della prova[6]. La proposta non appare tuttavia convincente, non tanto per i contenuti, che appaiono, seppur difficilmente realizzabili su larga scala, condivisibili, ma quanto per l'impatto che una simile impostazione potrebbe generare, particolarmente per ciò che riguarda la presunzione di illegalità. Come diffusamente osservato, infatti, in tutti gli atti delle istituzioni sovranazionali presi in esame all'interno dei capitoli II e III, viene costantemente evidenziato che l'obiettivo finale che deve raggiungersi è quello di creare, intorno all'intelligenza artificiale, "un ecosistema di fiducia". Non pare possa considerarsi adatta allo scopo una regolamentazione che ponga su questi sistemi una presunzione di illegalità. Considerato che si ritiene che l'unico ragionevole obiettivo a cui dovrebbe tendersi sia quello di assicurare, nella massima estensione possibile, la "neutralità" del sistema, sarebbe più utile, tentare di implementare un *test standard* o una serie di *test* il più possibile completa, da utilizzare per saggiare la neutralità dell'algoritmo sotto diversi profili e subordinarne la commercializzazione al conseguimento di un esito positivo.

[6] G. MALGIERI, F. A. PASQUALE, *From Transparency to Justification: Toward Ex Ante Accountability for AI*, May 3, 2022, *Brooklyn Law School, Legal Studies Paper No. 712, Brussels Privacy Hub Working Paper, No. 33*, consultabile *online* e D. TAFANI, *"Automaticamente illegali". Una proposta per i sistemi di intelligenza artificiale,* in *Bollettino telematico di filosofia politica*, 7 novembre 2022, consultabile *online*.

Si potrebbero utilizzare allo scopo, i ricordati spazi di sperimentazione, che si sono esaminati nell'affrontare, all'interno del capitolo IV, il tema del coordinamento tra la proposta di regolamento e il GDPR, nell'ambito dei quali far confluire e collaborare, esponenti delle aziende del settore, esperti in tema di digitale e intelligenza artificiale ma anche rappresentanti delle istituzioni.

Per ciò che riguarda l'esaminata proposta di regolamento, dall'analisi condotta è emerso che sono ancora molti gli interrogativi a cui il legislatore europeo dovrà dare risposta, auspicabilmente, all'interno del testo definitivo che licenzierà al termine di questo lungo periodo di gestazione.

Nella specie, nella prospettiva di garantire un'adeguata tutela della *privacy* degli utenti *online*, all'interno del capitolo IV, si sono evidenziate alcune difficoltà di coordinamento tra l'attuale proposta di regolamento sull'intelligenza artificiale e il GDPR, che potrebbero minarne l'effettività.

Un primo aspetto problematico riguarda proprio il profilo del consenso.

Si è detto, infatti, che le fasi della raccolta e del trattamento non sono regolamentati nella proposta e che, pertanto, la disciplina andrà ricercata altrove e, nella specie, all'interno del GDPR. Tuttavia, come sottolineato, sembrerebbe esservi un'incompatibilità, difficilmente conciliabile, tra la logica sottesa alla prestazione del consenso, delineata dal regolamento, e le stesse modalità di funzionamento dei sistemi di intelligenza artificiale.

Secondo le disposizioni del GDPR, infatti, è previsto che l'interessato abbia sempre il controllo sui propri dati e gli venga garantita, in qualsiasi momento, la possibilità di esercitare i propri diritti, così come conferiti dalla normativa. In questa prospettiva, nel corso della presente disamina, ci si è chiesti come una simile impostazione possa conciliarsi con le modalità di trattamento multiplo e automatizzato utilizzate, nella maggior dei casi, dai sistemi di intelligenza artificiale. Il rischio concreto individuato, qualora la logica del consenso, nei termini oggi conosciuti, venga applicata, senza i necessari adattamenti, anche ai sistemi di intelligenza artificiale, è che questo stesso consenso, già oggi così sottovalutato, apra o, quantomeno, consenta l'utilizzo dei dati per il perseguimento di fi-

nalità che non saranno immediatamente, ma neppure facilmente, comprensibili per gli utenti.

D'altra parte, anche la circostanza che il GDPR imponga al titolare, l'obbligo di limitazione del trattamento, se non per finalità determinate, o l'acquisizione di una nuova manifestazione positiva di volontà ogni qualvolta la raccolta dati si discosti, in maniera oggettiva o soggettiva, dalle finalità iniziali sulla base delle quali erano stati legittimamente raccolti, si è visto che, dal punto di vista del coordinamento con la proposta di regolamento sull'intelligenza artificiale, pone un ulteriore profilo di criticità.

Nel caso, infatti, dei trattamenti multipli processati dai sistemi di intelligenza artificiale l'onere per il titolare del trattamento (laddove individuabile) di notifica nel caso di modifica o di esercizio dei diritti dell'interessato diventerebbe insostenibile e si ricadrebbe nell'alveo dell'eccezione per eccessiva onerosità contemplata all'interno dell'articolo 19 del GDPR, con conseguente indiretta deresponsabilizzazione dei produttori.

Il profilo del diritto alla spiegazione e della trasparenza, affrontato proprio all'interno del paragrafo 4 del capitolo del IV dove si è trattato anche delle decisioni totalmente automatizzate, pone problemi ancora più seri, posto che dubbi analoghi si erano posti già con riferimento al GDPR e non sono stati (ancora) risolti dal legislatore europeo. Si ricorderà, infatti, che l'articolo 22, nel disciplinare il diritto dell'interessato a non essere sottoposto ad una decisione discendente da un processo totalmente automatizzato, non include anche un vero e proprio diritto alla spiegazione. L'unica espressa menzione in tal senso si ritrova, all'interno del considerando 71 che però, chiaramente, non ha portata precettiva ma piuttosto interpretativa. Un simile stato di cose, come già avvenuto nel caso del GDPR ma in misura ancora più grave se visto nella prospettiva del funzionamento dei sistemi algoritmici, è destinato a generare incertezza giuridica e, soprattutto, una normativa così congeniata non risulta sufficientemente protettiva per gli utenti *online*. Purtroppo, tale lacuna non è stata colmata, almeno non in maniera definitiva ed esaustiva, neppure all'interno della proposta di regolamento sull'intelligenza artificiale. All'articolo 10, infatti, il legislatore si è limitato a prevedere laconicamente che i dati di addestra-

mento debbano soddisfare determinati requisiti e che, dunque, debbano essere pertinenti, rappresentativi, esenti da errori e completi. Una risposta, seppure parziale, si può rinvenire all'interno dell'articolo 13, paragrafo 1, della proposta che parla di sistemi "sufficientemente trasparenti". Il problema è che la norma si riferisce solo ai sistemi ad alto rischio. Sarebbe quantomai opportuno estendere tale requisito a tutti i sistemi di intelligenza artificiale, se del caso specificando che tale obbligo si estende, *a fortiori*, ai sistemi ad alto rischio, prevedendo altresì misure progressivamente sanzionatorie a seconda che l'obbligo di trasparenza venga violato con riferimento a sistemi ad alto rischio o a medio e basso rischio.

Diversamente, come già osservato, il "diritto" alla spiegazione rischia di diventare un concetto assai fumoso se riferito ai sistemi di intelligenza artificiale, posto che, come più volte evidenziato nell'ambito della presente analisi, gli algoritmi sono spesso, per definizione, opachi. Peraltro, l'obbligo dovrebbe essere previsto in maniera particolarmente incisiva, poiché un diritto alla spiegazione, che si limiti ad obbligare l'operatore economico a rendere nota la logica che si cela dietro il funzionamento di un determinato algoritmo, potrebbe risultare insufficiente ad assicurare il livello di tutela dell'utente auspicato.

Anche per ciò che riguarda la corretta identificazione dei soggetti responsabili, potrebbero profilarsi delle criticità nel coordinamento tra i due atti. Le norme del GDPR e quelle contenute all'interno della proposta di regolamento, infatti, si indirizzano a destinatari differenti. Mentre quest'ultima impone dei comportamenti agli sviluppatori e ai fornitori di sistemi di intelligenza artificiale, gli obblighi previsti dal GDPR sono per lo più posti a carico del titolare del trattamento.

È proprio il profilo dell'individuazione del soggetto responsabile che deve essere chiarito, al fine di consentire agli utilizzatori finali di non trovarsi in balia del sistema senza avere cognizione precisa del riparto di responsabilità e di chi sia il soggetto a cui rivolgersi per esercitare i propri diritti e presentare eventuali reclami. Nel caso del GDPR si prevede che il titolare del trattamento venga individuato in modo esplicito in un soggetto unitario. L'esatto opposto avviene nel caso di sistemi di intelligenza artificiale, che spesso im-

plicano l'intervento di più soggetti a diversi livelli, circostanza che implica che la raccolta dei dati possa avvenire anche con strumenti diversi, non necessariamente assoggettati a gestione unitaria. La pluralità di soggetti e la difficoltà di individuare quelli direttamente responsabili, a cui legittimamente rivolgere eventuali reclami, può compromettere l'effettività della tutela per l'utente, che molto più facilmente, in una situazione di ambiguità, sarà propenso ad abbandonare eventuali contestazioni.

Ciò posto, come dovrebbe attribuirsi la responsabilità in questi casi? L'ipotesi proposta potrebbe essere quella di prevedere una sorta di responsabilità oggettiva e cumulativa da attribuirsi a carico di uno solo dei soggetti coinvolti, applicando un criterio di prevalenza, qualitativa o quantitativa – soluzione che però appare macchinosa da attuare nella pratica – diversamente, si potrebbe prevedere una responsabilità generalizzata di tutti i soggetti coinvolti, a vario titolo, nello sviluppo e produzione (con l'unica esclusione del soggetto che si occupa della mera commercializzazione e che confida nella liceità del prodotto). Tale soluzione certamente più agevole da realizzare, appare anche meno equa dal punto di vista di produttori e sviluppatori, il cui coinvolgimento nel processo di sviluppo, difficilmente avrà un peso specifico equivalente. L'alternativa è quella di rassegnarsi all'idea di avere più soggetti responsabili andando, in definitiva, ad aggravare la posizione di tutela dell'utilizzatore finale.

Occorrerà effettuare una scelta tra le posizioni in gioco per decidere quale "aggravare", effettuando un attento bilanciamento tra rischi e opportunità per ciascuno dei profili interessati.

Alla luce delle molteplici ed eterogenee criticità rilevate, considerato che, come detto, i dati costituiscono il principale nutrimento dei sistemi di intelligenza artificiale, se davvero si vuole assicurare un'adeguata tutela degli utenti *online* e garantire altresì un esatto coordinamento, tra l'attuale disciplina sulla protezione dei dati personali e la futura regolamentazione sull'intelligenza artificiale, è necessario uno sforzo aggiuntivo di sistematizzazione da parte delle istituzioni europee.

Le criticità sopra rilevate appaiono ancora più serie se guardate attraverso la lente della non discriminazione.

Se, infatti, si parte dall'assunto, ormai verificato, che i dati costituiscono il principale nutrimento dei sistemi di intelligenza artificiale, ci si scontra inevitabilmente con la circostanza che tali dati possano restituire, a seconda di come vengono combinati, risultati direttamente o indirettamente discriminatori.

Sebbene, infatti, l'articolo 9 del GDPR vieti di trattare dati particolari, che sono chiaramente quelli che più facilmente potrebbero condurre a conseguenze discriminatorie, tale divieto potrebbe non risultare sufficiente se applicato al settore dell'intelligenza artificiale.

In primo luogo, perché attraverso tale divieto ci si pone al riparo, unicamente, dalle discriminazioni di tipo diretto e non anche da quelle indirette. Questo, nel settore dell'intelligenza artificiale, particolarmente alla luce delle criticità emerse analizzando, all'interno del capitolo V, alcune applicazioni pratiche di tali sistemi, appare obiettivamente una tutela insufficiente. Come evidenziato in maniera diffusa, infatti, nel caso degli algoritmi il problema non si esaurisce nella lettura di *input* e *output* ma di tutto ciò che avviene nello spazio ricompreso tra questi due momenti, posto che spesso tali sistemi operano mediante correlazioni e non applicando un nesso di causalità. Pertanto, è stato visto che anche dati apparentemente neutrali, se combinati, potrebbero restituire risultati discriminatori creando un impatto negativo su determinate categorie di individui. Il problema è che gli eventuali pregiudizi recepiti dall'algoritmo e i processi di stratificazione dei dati, potenzialmente, potrebbero portare a perpetrare una distorsione all'infinito e a non consentire più, almeno non agevolmente, di individuare il momento esatto in cui il "cortocircuito" si è verificato.

Per evitare questi problemi, dal lato dei dati è cruciale quelli utilizzati per addestrare i modelli siano privi di pregiudizi razziali e che gli sviluppatori tengano conto delle questioni di equità e di giustizia sociale nel *design* e nell'utilizzo dei modelli da implementare. Per raggiungere tale scopo potrebbe aiutare moltissimo una maggiore diversità nei gruppi che sviluppano gli algoritmi, in modo che le differenze nelle prospettive di coloro che lavorano alla programmazione aiutino ad adottare pratiche progettuali inclusive, a sviluppare strutture algoritmiche *by design* capaci di superare anche i

pregiudizi che emergono dal modello etico imperante all'interno di una determinata realtà e, in generale, ad utilizzare dati di addestramento ampi e diversificati. Su tale ultimo aspetto vale tuttavia la pena di evidenziare che, ponendosi in una prospettiva inversa, più ampia è la mole di dati che gli algoritmi potranno processare, più intenso sarà il sacrificio richiesto agli utilizzatori in termini di cessione di informazioni e di compressione della propria sfera della *privacy*.

Sarebbe importante e opportuna l'implementazione di misure per monitorare e valutare continuamente l'equità di tali sistemi. In particolare, occorrerebbe prevedere una procedura di valutazione dell'impatto degli algoritmi su diverse categorie di persone e la creazione di meccanismi di trasparenza per consentire ai consumatori di comprendere come vengono utilizzati i loro dati. Sebbene, come evidenziato, l'articolo 13 della proposta di regolamento preveda qualcosa di simile, è comunque necessario, alla luce delle lacune evidenziate in tema di trasparenza e diritto alla spiegazione, un intervento del legislatore europeo utile a circoscriverne, in maniera più puntuale, i confini per non rischiare di lasciare zone d'ombra in cui gli operatori economici possano rifugiarsi per sottrarsi ai propri obblighi.

D'altronde, se il presupposto su cui si concorda è che l'intelligenza artificiale debba essere una tecnologia utile a migliorare la vita delle persone, la discriminazione, diretta o indiretta che sia, deve considerarsi semplicemente inaccettabile. Deve essere una preoccupazione costante del legislatore sovranazionale e, a cascata, anche di quelli nazionali, ma anche degli sviluppatori che dovrebbero essere adeguatamente sensibilizzati sul tema, grazie ad una normativa che risulti efficacemente ed effettivamente protettiva per gli individui e sufficientemente chiara da garantire la necessaria certezza giuridica e non lasciare aperti troppi spazi all'interpretazione o all'iniziativa individuale che, in questi casi, genererebbe solo una grande confusione.

Inoltre, per evitare il ripetersi di risultati come ad esempio quelli discendenti dagli esaminati casi Deliveroo, Loomis o legati all'utilizzo dei sistemi algoritmici come Fisco e COMPAS, è importante che le tecnologie di intelligenza artificiale non siano utilizzate,

almeno non in via esclusiva, per prendere decisioni che possano avere conseguenze negative sugli individui, come l'accesso al credito o all'occupazione. In questi casi, è necessario garantire che i soggetti coinvolti abbiano la possibilità di contestare in modo semplice e diretto le decisioni e che sia sempre garantita una sufficiente trasparenza rispetto al ragionamento algoritmico impiegato.

Ultimamente poi, il diffondersi dell'intelligenza artificiale generativa, come nell'esaminato caso di ChatGPT[7], ha portato i termini della questione ad un livello superiore, e pone il legislatore europeo dinanzi a problematiche nuove, di cui dovrà necessariamente tenere conto nell'elaborazione del testo finale del regolamento (come, d'altronde, già sottolineato dal Parlamento europeo negli emendamenti presentati).

Come facilmente prevedibile questi *tools* stanno riscuotendo un enorme successo tra gli utenti, soprattutto tra le giovani generazioni, ma anche in questo caso, sono già emersi dei profili preoccupanti.

In primo luogo, il rischio di appiattimento cognitivo e di intorpidimento intellettivo. Poter utilizzare un sistema in grado di svolgere compiti che, diversamente, richiederebbero molto tempo e sforzo rappresenta ovviamente una possibilità particolarmente allettante, che tuttavia potrebbe condurre, nel lungo periodo, ad un impoverimento cognitivo. Di contro però, se tali sistemi dovessero essere utilizzati per svolgere compiti meccanici, particolarmente energivori ma intellettualmente poco stimolanti, come ad esempio l'associazione di grandi quantità di dati o calcoli particolarmente complessi, rimarrebbe più tempo da dedicare allo studio, alla ricerca e, in generale, alle attività creative. Ecco dunque che il legislatore europeo è chiamato ad adottare una disciplina che sia in grado di bilanciare questi due aspetti, ovvero garantire l'utilizzo di tali sistemi in modo da non perderne i vantaggi ma non consentire lo sviluppo di una generazione priva di capacità di analisi e acritica.

Un ulteriore problema che si pone, con crescente preoccupazione, è che trattandosi spesso di *tools* disponibili *open source*, hanno iniziato ad essere attenzionati con crescente interesse da cyber-

[7] Si veda *supra* capitolo IV, par. 6.

criminali per la scrittura di codice di intrusione malevolo per sferrare attacchi *hacker,* anche su larga scala, con conseguenze che potrebbero risultare gravissime, a carico di individui, ma anche di società e governi. L'aspetto ancora più grave è che rischia di infoltire le fila dei cybercriminali includendo quei soggetti che, pur avendo un intento criminale, mancavano di particolari competenze informatiche che ora, grazie a questi sistemi, possono tentare di acquisire in modo facile e gratuito[8].

Sono stati denunciati anche i primi casi di "dipendenza"[9] da questi sistemi, ed è stato evidenziato che il rischio legato all'utilizzo potrebbe essere quello di «una grande solitudine che evolve nell'angoscia»[10].

Peraltro, occorre anche considerare che l'a-territorialità che caratterizza queste tecnologie pone al legislatore europeo una sfida ulteriore. Si ricorderà, ad esempio, quanto trattato proprio con riferimento al caso ChatGPT. Recentemente il Garante privacy era intervenuto imponendo il blocco del servizio per gli utenti italiani avendo rilevato delle criticità per ciò che riguarda la base giuridica del trattamento dati, la titolarità, l'esercizio dei diritti ma anche la

[8] In un recente articolo del Sole24Ore, Paolo Dal Checco, tra i più noti informatici forensi in Italia, ha evidenziato che «L'AI e in particolare ChatGpt facilitano le cose ai cybercriminali. Il *bot* di OpenAI una cosa fa di sicuro molto bene ed è proprio scrivere codice». I ricercatori di *Check Point Research* (CPR) hanno segnalato almeno tre casi in cui cybercriminali mostrano, in *forum underground*, come hanno sfruttato l'intelligenza artificiale di ChatGpt per scopi malevoli, l'articolo è disponibile *online*.

[9] Nel film del 2015, *Ex Machina*, di Alex Garland, il protagonista si fa sedurre da un androide (a cui gli autori fanno assumere sembianze e caratteristiche femminili) al punto da perdere la vita, non potendo credere che dietro le parole dolci ed empatiche che gli rivolge, non vi siano sentimenti reali.

[10] Il Fatto Quotidiano ha recentemente riportato una testimonianza S. GRIGGIO, *ChatGtp ti ruba la vita, è come una droga. Per colpa sua ho perso amici e fidanzata e ho avuto una crisi d'astinenza*, in *Il Fatto Quotidiano*, 10 maggio 2023. All'interno dell'articolo Federico Tonioni, psichiatra e psicoterapeuta, fondatore del primo ambulatorio in Italia sulla dipendenza da Internet, chiarisce che «una personalità narcisistica, posta davanti a un'intelligenza artificiale avanzata, può sentirsi perfettamente a proprio agio, come fosse davanti a uno specchio. Ma il rischio è quello di una grande solitudine che evolve nell'angoscia».

verifica della minore età dei fruitori del servizio. Nonostante OpenAI si sia conformata all'obbligo imposto, la delimitazione territoriale non ha assolutamente impedito agli interessati, *medio tempore*, di poterlo utilizzare. È risultato semplicissimo, anche per gli utenti meno esperti, aggirare i limiti imposti dalla territorialità. È stato sufficiente, infatti, utilizzare un banale server *proxy* (ovvero un *server* che si interpone nel normale flusso di comunicazione tra il *client* e i *server* dei servizi *web*) o una VPN (*Virtual Private Network*) su cui far transitare la richiesta, per collegarsi al di fuori dell'Italia, eludendo completamente il limite della territorialità[11].

Quello di riuscire ad assicurare, anche nel difficile mondo del digitale, l'effettività di specifici provvedimenti sanzionatori eventualmente adottati, rappresenta è un punto cruciale che il legislatore europeo non può assolutamente sottovalutare se davvero si vuole arrivare a creare un "ecosistema di fiducia" nell'intelligenza artificiale da parte dei cittadini.

3. La tenuta dell'attuale assetto normativo in tema di diritti fondamentali dinanzi al prepotente imporsi sulla scena dell'intelligenza artificiale. Sono necessari nuovi diritti "digitali"?

In tema di tutela dei diritti fondamentali e con particolare riferimento alla *privacy* e alla non discriminazione, il nodo da sciogliere riguarda la necessità di capire se l'attuale quadro normativo sia o meno in grado di raccogliere e affrontare positivamente le nuove sfide che il massiccio ricorso a strumenti regolati dall'intelligenza artificiale sta ponendo con intensità e livelli di complessità sempre crescenti.

Si è visto, esaminando nel corso del presente scritto i risultati

[11] Sia consentito rinviare a C. GRIECO, *Ancora sul diritto all'oblio: la Corte di giustizia si pronuncia sull'obbligo di deindicizzazione di contenuti nel caso in cui contengano informazioni inesatte*, in Osservatorio sulla Corte di giustizia dell'Unione europea n.1/2023, *Ordine internazionale e diritti umani*, (2023), pp. 199-206, dove analoghe considerazioni sono state svolte in tema di diritto all'oblio.

delle prime applicazioni pratiche di sistemi algoritmici in vari settori, che l'uso crescente dell'automazione e del processo decisionale algoritmico, in tutte le sfere della vita pubblica e privata, potrebbe minacciare di alterare il concetto stesso di "diritti fondamentali" che agiscono come 'difese' contro l'ingerenza statale.

La tradizionale asimmetria di potere e informazione tra le strutture statali e gli esseri umani si sta spostando verso un'asimmetria di potere e informazione tra gli operatori di algoritmi e coloro che ne sono governati[12].

Occorre capire se dalla rivoluzione digitale in atto il delineato sistema di tutela dei diritti fondamentali, particolarmente in ambito europeo, ne uscirà rafforzato o, al contrario, indebolito.

L'interrogativo appare legittimo, anche alla luce del fatto che la maggior parte dei diritti tutelati dalla Carta di Nizza così come dalla CEDU, come si è visto all'interno del capitolo III esaminando anche la giurisprudenza delle due Corti[13], non rivestono carattere assoluto. Questo comporta che la compressione dei diritti, seppure al ricorrere di condizioni legittime, è in una certa misura, lecita. Come si è visto all'interno dello stesso capitolo, la stessa Corte di giustizia, in più occasioni, ha chiarito che qualsiasi compressione all'esercizio dei diritti e delle libertà riconosciuti dalla Carta di Nizza deve risultare rispettosa della loro "essenza", mentre la Corte EDU, proprio con specifico riferimento all'impiego di nuove tecnologie, ha già avuto modo di chiarire che gli Stati dovrebbero trovare "un giusto equilibrio" tra la protezione dei diritti fondamentali e lo sviluppo delle nuove tecnologie.

A motivo di ciò, poiché l'obiettivo rimane quello di assicurare un livello elevato di protezione dei singoli, attraverso un approccio basato sul rischio, così come delineato all'interno dell'esaminata proposta di regolamento, appare opportuno che il legislatore europeo mantenga e, anzi, rafforzi, l'elenco di requisiti che devono esse-

[12] Si veda F. LAVIOLA, *Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa*, in *BioLaw Journal*, 3, 2020, p. 389 ss.

[13] Ovvero Corte di giustizia e Corte europea dei diritti dell'uomo.

re rispettati per garantire che vengano sviluppati sistemi affidabili e che siano istituiti rigorosi meccanismi di controllo. Positive in questo senso appaiono le previsioni della marchiatura europea e la dichiarazione di conformità, ma si potrebbe pensare anche a protocolli di sicurezza e di sviluppo. Qui si pone anche un problema molto delicato a cui, pur esulando della presente analisi, si ritiene opportuno accennare, ovvero il bilanciamento tra il diritto dell'operatore economico a veder tutelata la propria proprietà industriale, a cui consegue l'eventuale legittimo rifiuto di esporre i codici sorgente degli algoritmi, frutto magari di anni di attività di ricerca e sviluppo e di ingenti investimenti[14], e il diritto del singolo di conoscere le modalità di ragionamento e i parametri utilizzati da un algoritmo a cui magari è stato affidato, come nell'esaminato caso *Loomis*, il calcolo dell'ammontare della pena che gli verrà comminata.

Più aumenta l'automazione di questi sistemi, più si riduce la possibilità di supervisione umana e maggiore è il rischio che possano verificarsi violazioni dei diritti fondamentali, anche perché una stessa questione può essere vista da diverse prospettive e quindi interessare – in negativo – diversi diritti fondamentali[15]. Una decisione presa da un algoritmo potrebbe risultare lesiva della dignità umana, potrebbe violare la *privacy* dell'interessato e, finanche, risultare, nel merito, discriminatoria. Se poi non sono previsti meccanismi di tutela e di protezione adeguati potrebbe sfociare altresì nella violazione del diritto ad un rimedio efficace, alla buona amministrazione e al diritto a un ricorso effettivo e a un processo equo.

Peraltro, come è stato osservato[16], il continuo mutamento di questi sistemi e gli sviluppi che non risultano, *a priori* prevedibili, rappresentano degli ostacoli concreti alla possibilità di poter antici-

[14] Cfr. Per alcune riflessioni G.M. RUOTOLO, The God that failed. *La tutela dei* co-patterners *nell'ordinamento internazionale ed europeo, in Rivista di diritto dei media*, 2018, disponibile online.

[15] Si veda la posizione del Consiglio d'Europa sul punto espressa nella *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Appendix, para. A.8,* disponibile *online*.

[16] A. ADINOLFI, *L'unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 13 ss.

pare, in modo compiuto, i vari profili di ingerenza che potrebbero profilarsi con riferimento al rispetto dei diritti fondamentali[17].

Il ruolo del legislatore europeo appare dunque cruciale nell'imporre obblighi proporzionati e sufficientemente garantisti per tutti i partecipanti alla catena del valore. Potrebbe addirittura arrivarsi, attraverso una normativa flessibile ma sufficientemente garantista, a migliorare e promuovere la protezione dei diritti fondamentali – proponendo così l'idea non di una mera salvaguardia statica dei diritti ma addirittura di una tutela di tipo proattivo.

L'attenzione deve essere mantenuta alta, soprattutto all'alba dell'adozione di una normativa europea specifica sul punto[18]. A dimostrazione di quanto il tema sia sentito e del fatto che sono coinvolti *stakeholders* a livelli diversi, anche il gruppo di organizzazioni della società civile si è rivolta all'Europa presentando una dichiarazione tesa a richiedere una legge sull'intelligenza artificiale che metta in primo piano i diritti fondamentali[19].

Se non correttamente gestita a livello normativo e pratico, se non si interviene con un quadro chiaro necessario a mitigare i ri-

[17] Lo studio del 9 novembre 2018 realizzato per il Consiglio d'Europa evidenzia proprio questo aspetto. Si riferisce alla rivoluzione digitale in atto come alla *"New" Industrial Revolution* ed evidenzia che: «The 'New' Industrial Revolution now dawning is also likely to bring myriad benefits to individuals and societies yet, like the original Industrial Revolution, might also generate unintended adverse effects that were not recognised at the time of the revolution's unfolding. The same might also be true of the present networked digital revolution that societies now face, yet reliably predicting the aggregate, cumulative effects of the current networked digital revolution over time is extremely challenging». Lo studio è disponibile *online*.

[18] La Commissione ha reso noto di voler aumentare a 20 miliardi di euro l'anno gli investimenti privati e pubblici per le tecnologie di intelligenza artificiale, sta incrementando i suoi investimenti annuali del 70 % nell'ambito del programma di ricerca e innovazione *Horizon 2020*.

[19] La dichiarazione, disponibile *online*, è stata redatta da *European Digital Rights* (EDRi), insieme a Access Now, Fondazione Panoptykon, epicenter.works, *AlgorithmWatch, European Disability Forum* (EDF), *Bits of Freedom, Fair Trials, PICUM* e *ANEC,* ed elenca le raccomandazioni essenziali per guidare il Parlamento e il Consiglio dell'Unione europea nel modificare la proposta di Regolamento del 21.04.2021 che disegna un quadro di riferimento legale volto a normare il mercato dell'Unione Europea dell'intelligenza artificiale.

schi[20] in termini di diritti, se non si agisce con una comunicazione positiva e propositiva idonea a rafforzare una buona percezione dell'intelligenza artificiale negli individui, il rischio concreto è che da opportunità concreta per migliorare il benessere generale della società, l'intelligenza artificiale finisca per trasformarsi, ed essere percepita, come una minaccia[21].

Alla luce di tutto quanto fin qui analizzato, si pone un ulteriore quesito volto ad indagare se siano o meno necessari nuovi diritti sostanziali specifici e nuovi diritti procedurali digitali. Ma sono davvero necessari? O sarebbe sufficiente una nuova declinazione di quelli esistenti tutelati da Carta di Nizza e CEDU oltre che dai sistemi costituzionali interni?

Il *Rathenau Instituut*, in un rapporto[22] in cui analizza l'impatto dei diritti umani nell'era dei *robot*, propone il riconoscimento di due nuovi diritti fondamentali, al fine di mantenere l'intelligenza artificiale su un piano che sia effettivamente a misura d'uomo. In particolare, si propone il riconoscimento del diritto a non essere oggetto di misurazioni, di analisi e di "addestramento"[23] e il diritto a un contatto umano significativo[24] e, dunque, a poter stabilire e sviluppare relazioni profonde con altri esseri umani.

Questi due diritti, pur classificandosi come autonomi, risultano, in realtà, strettamente connessi tra di loro. A ben vedere costituiscono una declinazione specifica di diritti fondamentali già esistenti e si pongono come naturale sviluppo dei più tradizionali diritto alla

[20] Si veda al riguardo C. VAN VEEN, *Artificial Intelligence; What's Human Rights Got to Do with It?,* in *Data & Society: Points – blog of Data & Society Research Institute*, 14 May 2018, disponibile *online*.

[21] Sia consentito di rinviare per alcune considerazioni sul punto a C. GRIECO, *Intelligenza artificiale e diritti umani nel diritto internazionale e dell'Unione europea. Alla ricerca di un delicato equilibrio*, in *Ordine internazionale e diritti umani*, 2022, pp. 782-810.

[22] R. VAN EST, J. GERRITSEN, L. KOOL, *Report Human rights in the robot age, Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality,* 2017, disponibile *online.*

[23] *Right to not be measured, analysed or coached.*

[24] *Right to a meaningful human contact.*

privacy e alla non discriminazione, se contestualizzati nella diversa era dell'*IoT* (*Internet of Things*) e dell'intelligenza artificiale.

La necessità di tali nuovi diritti fondamentali specifici viene motivata sulla base del fatto che gli individui si trovano in una posizione di debolezza nei confronti alla cultura della sorveglianza di massa e del monopolio del digitale in mano alle *Big Tech*. Peraltro, è preoccupante notare che chi si trova ai vertici politici non sembra aver – ci si augura per il momento – sviluppato una consapevolezza e una sensibilità adeguate al problema[25]. Sembra infatti che gli interessi economici e politici sottesi all'impiego di sistemi di tracciamento e di raccolta dati siano valori ritenuti più importanti dei diritti dei singoli, inclusa la stessa *privacy*.

Sebbene, innegabilmente, in linea teorica appaia pregevole l'idea di avere delle previsioni specifiche in tema di diritti fondamentali digitali, ciò su cui si dubita, per tutto quanto sin qui analizzato e le caratteristiche intrinseche del mondo digitale, è la capacità di rendere effettiva tale tutela. Ciò su cui vale la pena interrogarsi, a parere di chi scrive, è se effettivamente la formale categorizzazione di nuovi diritti sia utile a fornire una 'reale' protezione, considerato che vi è un rischio concreto che la continua frammentazione e moltiplicazione di diritti, definiti come fondamentali, conduca, in realtà, ad ottenere nella pratica il risultato esattamente opposto, ovvero una minore tutela[26].

In assenza di adeguati strumenti per garantire l'effettività di tali diritti, potrebbe accadere che si vadano ad aggiungere ad una lista

[25] Per fare un altro esempio, in risposta alle preoccupazioni dei consumatori sul tracciamento *Wi-Fi* da parte dei proprietari di negozi, l'ex ministro olandese per gli affari economici e il segretario di stato per la sicurezza e la giustizia hanno dichiarato che le persone dovrebbero semplicemente spegnere il loro *smartphone* se non vogliono essere tracciate, Tweakers, *"Kabinet: zet telefoon uit om wifi-tracking tegen te gaan"*, 12 febbraio 2014, disponibile *online*.

[26] Mettono in guardia dal rischio di frammentazione e della moltiplicazione dei diritti S. RODOTÀ, *Il diritto al cibo,* in *Quaderni del Corriere della Sera,* 2014, p. 5 ss.; ID., *Il diritto di avere diritti*, Bari, 2012, p. 25 ss. e B. O'NEILL, *Inflating Away Our Human Rights*, in *MisesInstitute blog*, 14 dicembre 2009, disponibile *online*.

già estesa di diritti riconosciuti in potenza ma non nella sostanza[27]. Sarebbe probabilmente più opportuno prevedere meccanismi rigorosi di controllo che impongano ai produttori di sistemi di intelligenza artificiale di essere in *compliance* con dei requisiti chiari e selettivi che regolino non solo il lato di sviluppo del prodotto ma anche, e soprattutto, le loro modalità di impiego e la loro commercializzazione.

In caso di uso distorto e potenzialmente lesivo, devono essere previste sanzioni efficaci e tanto gravose in termini economici da riuscire a scoraggiare impieghi non etici e, soprattutto, da eccedere, nella bilancia, i profitti derivanti dall'enorme giro di affari che si cela dietro lo scambio di dati e, in generale, dietro al potere che solo informazione e controllo sono in grado di assicurare.

Peraltro, sul tema del rapporto tra individui e *Big Tech*[28] è stato correttamente posto in rilievo un altro problema sostanziale, ovvero il fatto che gli utenti, in questo scenario altamente complesso, non

[27] In questo senso anche A. SANTOSUOSSO, *Intelligenza artificiale e diritto, Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020, p. 413 ss. L'A. evidenzia che prima di muoversi verso la direzione dell'introduzione di nuovi diritti umani specifici «vale la pena di interrogarsi sull'utilità di infittire la selva dei diritti riconosciuti formalmente (e magari ignorati nella pratica) e sulla possibilità di applicare strumenti del tipo della *privacy by design*, che s'ispira a una logica diametralmente opposta».

[28] Non è un caso che Meta, nel novembre del 2019, abbia cambiato il proprio *slogan* storico da «è gratis e lo sarà sempre» a «è veloce e semplice» si veda K. MCCARTHY, *What we know about the small change to Facebook's slogan*, 28 agosto 2019, disponibile *online*. Da notare che il 29 novembre 2018 Meta era stata altresì sanzionata dall'AGCM per pratica commerciale scorretta consistente nell'informare gli utenti esclusivamente della gratuità del servizio, «senza evidenziare le finalità commerciali di utilizzo dei dati». La modifica operata da Meta nella comunicazione esterna con l'utenza è verosimilmente da ricondursi all'approvazione nel frattempo intervenuta della Dir. EU n. 770/2019 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, il cui considerando n. 24 chiarisce che «[l]a fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico». Nel testo della direttiva, inoltre, la definizione di prezzo viene estesa anche alla «rappresentazione di valore digitale dovuto come corrispettivo per la fornitura di contenuto digitale o di un servizio digitale» (art. 2 (7)).

sono solo consumatori, ma anche – e forse per alcuni aspetti soprattutto – produttori di dati[29], ma «il problema è che non lo sanno»[30].

Sfortunatamente finché gli individui non acquisiranno un'adeguata consapevolezza non solo delle modalità di funzionamento, seppure in termini generali, di tali tecnologie, ma anche e, forse soprattutto, del ruolo fondamentale che rivestono all'interno di questi meccanismi e su questo mercato, difficilmente riusciranno a percepire il valore fondamentale dei propri dati e delle informazioni che "scelgono" di condividere e di utilizzare come controprestazione per usufruire di un determinato servizio[31].

4. L'intelligenza artificiale come possibile strumento per la promozione dei diritti fondamentali

Nell'odierno dibattito dottrinale, tra i timori generalizzati legati alle nuove tecnologie e l'indagine sui potenziali rischi connessi, un filone di analisi, come evidenziato nel corso della presente analisi, guarda all'intelligenza artificiale come ad un possibile mezzo per implementare e consolidare il rispetto dei diritti fondamentali[32].

[29] L'espressione *walking data generators* è stata utilizzat da S. CALZOLAIO, (voce) *Protezione dei dati personali* (Dir. Pubbl.), in *Dig. disc. pubbl.*, *Aggiorn.*, 2017, p. 598.

[30] L'osservazione è di C. BERGONZINI, *"Prova A Prendermi". Ecosistema Digitale e Consapevolezza degli Utenti: Uno Spazio per la Regolazione Nazionale,* cit., p. 105 ss.

[31] *Ibidem*. L'A. sottolinea come in certi casi il problema sia "l'anafalbetismo digitale" e che la controprestazione richiesta all'utente appaia eccessiva rispetto al servizio offerto dal *provider* come ad esempio, quando il consenso alla cessione dei dati viene richiesto per accedere ad un *social network*.

[32] Nel documento *Tutela dei diritti fondamentali nell'era digitale - relazione annuale 2021 sull'applicazione della carta dei diritti fondamentali dell'Unione Europea*, 10/12/2021, COM [2021] 819*final*, p. 19, la Commissione europea ha chiarito che «uno specifico sottoinsieme di applicazioni di IA può subire un continuo adattamento, anche durante l'utilizzo, e cambiare l'evolvere in modo imprevisto senza poter essere facilmente monitorato. Ciò comporta un certo grado di imprevedibilità che può incidere sulla sicurezza o sui diritti fondamentali». A. ADINOLFI, *L'unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p.14.

Tale approccio è stato sostenuto anche nel rapporto della Commissione europea del dicembre 2021 in cui si sottolinea come l'intelligenza artificiale: «può avere importanti effetti positivi sulle nostre società. Può aumentare l'efficienza dei processi o stimolare l'innovazione la ricerca. Può inoltre servire a promuovere una serie di diritti fondamentali, quali i diritti alla libertà di espressione e di informazione o all'assistenza sanitaria, e promuovere importanti questioni di interesse pubblico quali la sicurezza pubblica o la sanità pubblica»[33].

La parola chiave resta bilanciamento, per non rischiare, da una parte, di perdere gli enormi vantaggi connessi all'impiego dei sistemi di intelligenza artificiale e, dall'altra, di non mettere a rischio le consolidate conquiste in termini di diritti e valori. Appare come non mai imperativo tracciare una linea netta, che divida ciò che deve considerarsi lecito da ciò che non lo è, preservando la libertà degli individui e garantendo, allo stesso tempo, la certezza giuridica.

È indiscutibile che i sistemi di intelligenza artificiale potrebbero effettivamente migliorare la protezione di alcuni diritti fondamentali. Si pensi al diritto alla salute. È recente la notizia di un *team* di ricercatori che ha utilizzato un algoritmo, lo Sphinks, per rilevare casi di tumori maligni e per suggerire le terapie più idonee ed efficaci. Si tratta, se si riuscirà a procedere nella sperimentazione, di una scoperta sensazionale che potrebbe sconfiggere una delle malattie più terribili e letali dei tempi moderni. In questo caso è evidente che il sistema di intelligenza artificiale, ben lontano dal creare una minaccia ad un diritto fondamentale, ha esattamente l'effetto opposto, ovvero quello di promuovere e migliorare la tutela, peraltro, non su carta ma in modo fattivo, di un diritto fondamentale come quello alla salute[34].

In conclusione dunque, si potrebbe dire, utilizzando un'im-

[33] *Ibidem,* p. 18.

[34] Il *team* di ricercatori italiani è guidato dal Prof. Antonio Iavarone. I risultati raggiunti sono stati pubblicati si veda S. MIGLIOZZI, Y.T. OH, M. HASANAIN ET AL., *Integrative multi.omics networks identify PKCϑ and DNA-PK as master kinases of glioblastoma subtypes and guide target cancer therapy,* in *Nature Cancer, 2023,* disponibile *online.*

magine certamente evocativa, che all'interno dei sistemi di intelligenza artificiale convivono due "anime": una 'negativa', che se male utilizzata rischia di mettere in pericolo i diritti fondamentali degli individui, privandoli della loro dimensione soggettiva, sociale e lavorativa; e una 'positiva' che promette (ed effettivamente dimostra) di poter dare un contributo fondamentale alla promozione e alla tutela di quegli stessi diritti. Tutto dipenderà da quale si deciderà di nutrire, pur consapevoli del fatto che nessuna delle due potrà essere del tutto messa a tacere e che la completa eliminazione dei rischi è un obiettivo utopistico.

La realtà è che paradossalmente è tutto umano, anche l'intelligenza artificiale. Questo significa che, in effetti, è difficile pensare ad una intelligenza artificiale non discriminatoria, posto che i dati immessi riflettono una società basata sulla discriminazione. Come è già stato evidenziato, il modello etico è fornito alle macchine dagli sviluppatori. Ne consegue che per avere un sistema di intelligenza artificiale ideale dovrebbe essere sviluppato da soggetti che vivono in una società ideale. Ne consegue che la neutralità e l'oggettività dell'algoritmo si tramutano in illusione, poiché, in effetti, pulire i dati significherebbe modificare il modo di approcciare e di percepire le differenze. L'intelligenza artificiale non è quindi di per sé discriminatoria, o non lo è necessariamente, il problema fondamentale è che progettata e sviluppata da intelligenze umane. I sistemi di *deep learning*, seppure altamente avanzati, elaborano e imparano da dati immessi. I sistemi *unsupervised*, come osservato, riproducono i pregiudizi insiti nella società che si riflettono, inevitabilmente, nei dati che vengono messi in relazione. Ne consegue che quello della discriminazione è un rischio che non può essere sempre gestito *ex ante,* poiché non è necessariamente legato al codice algoritmico.

Essendo utopistico immaginare di eliminare del tutto i rischi legati alla parte oscura dell'intelligenza artificiale, ciò a cui si deve tendere è il potenziamento dei vantaggi e il governo dei rischi, attraverso la regolamentazione.

Ma in quali termini? Occorre un approccio olistico e *by design* che passi da una normativa estremamente flessibile, idonea ad adeguarsi all'evoluzione tecnologica, ma anche sufficientemente rigo-

rosa, da garantire e laddove possibile promuovere, un generale senso di fiducia, imprescindibile affinché un'evoluzione digitale, seppur inarrestabile, possa essere accolta con favore dagli individui.

Sebbene il diritto fatichi a stare dietro all'impetuosità dei cambiamenti tecnologici in atto, in quanto caratterizzato da ritmi e processi normalmente molto più lenti, si pensi alla stessa proposta di regolamento, sono già passati oltre due anni da quando è stata presentata e già si sono poste nuove sfide per la Commissione europea con l'intelligenza artificiale generativa. Lo sviluppo tecnologico riesce a generare implicazioni e sollevare problematiche che le regole giuridiche non sempre sono pronte ad affrontare con strumenti adeguati. È stato osservato, in maniera lungimirante, che «[a]lcuni hanno insistito sul fatto che leggi e regolamenti giungerebbero sempre troppo tardi senza mai tenere il passo dell'IA, quando in realtà le norme non riguardano il ritmo ma la direzione dell'innovazione, poiché dovrebbero guidare il corretto sviluppo di una società. Se ci piace dove stiamo andando, possiamo andarci alla velocità che vogliamo»[35].

La direzione non può che essere quella verso la tutela dei diritti. E ciò, sebbene, al momento, sembra che l'intelligenza artificiale sia una questione molto politica e, indiscutibilmente, assai economica.

Non pare pertanto potersi confidare in un cambio di prospettiva *motu proprio* da parte di *Big Tech* e governanti. I giganti della tecnologia sembrano voler sottrarre i sistemi di intelligenza artificiale alla regolazione giuridica attraverso la politica dell'*ethics washing*, ovvero attraverso dichiarazioni di principi, linee guida, esperti, comitati e gruppi di lavoro sull'etica[36]. Non bisogna però cedere alle lusinghe dell'"etica"[37] ma la regolamentazione giuridica appare assolutamente necessaria in questo campo, soprattutto se i principali attori sulla scena sono proprio le *Big Tech*. Il legislatore europeo, con la proposta di regolamento sull'intelligenza artificiale, si

[35] L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., p. 86.

[36] D. TAFANI, *"Automaticamente illegali". Una proposta per i sistemi di intelligenza artificiale,* cit., disponibile *online*.

[37] B. WAGNER, *Ethics As An Escape From Regulation. From "Ethics-Washing" To Ethics-Shopping?*, cit., disponibile *online*.

sta muovendo nella direzione giusta per tentare di regolamentare il fenomeno e tutelare i diritti degli individui.

Il progresso non può essere certamente arrestato ma, in termini di diritti fondamentali, deve parlarsi di evoluzione e non di rivoluzione. Normalmente una rivoluzione tende a distruggere lo *status quo*. Nel caso dei diritti fondamentali, è quanto mai imperativo far sì che le conquiste, che si sono realizzate nel tempo, siano salvaguardate. La sfida consiste nel portare lo stato di diritto anche nel mondo digitale.

BIBLIOGRAFIA

AA.VV., *Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997*, E. Gabrielli (a cura di), Napoli, 1999.

ACCESSNOW, *Report Human Rights in the age of artificial intelligence,* disponibile online.

ADAMS-PRASSL J., *What if Your Boss was an Algorithm?*, in *Comparative Labor Law & Policy Journal*, 2019, 41, 1, p. 123.

ADINOLFI A., *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione, in Sezione "Atti convegni AISDUE*", n. 15, 14 marzo 2023, *Quaderni AISDUE*, p. 322.

ADINOLFI A., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), in *Intelligenza artificiale e diritto: una rivoluzione?*, Vol.1, *Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, p. 131.

ADINOLFI A., *L'unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 14.

ADINOLFI A., *Le innovazioni previste dal Trattato di Amsterdam in tema di politica sociale*, in *Il Diritto dell'Unione europea*, 1998, p. 563.

AGRAWAL A., GANS J., GOLDFARB A., *Macchine predittive*, Milano, 2018.

ALESSI C., *Lavoro tramite piattaforma e divieti di discriminazione nell'UE*, in *Impresa, lavoro e non lavoro nell'economia digitale*, (a cura di) Alessi C., Barbera M., Guaglianone L., Bari, 2019, p. 683.

ALEXANDRE L., *La guerra delle intelligenze. Intelligenza artificiale «contro» intelligenza umana*, Torino, 2018.

ALOISI A., GRAMANO E., *Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context*, in *Comparative Labor Law & Policy Journal*, 2019, 41, 1, p. 95.

AMALFITANO C., *Il diritto non scritto nell'accertamento dei diritti fondamentali dopo la riforma di Lisbona*, in *Il Diritto dell'Unione europea*, 1, 2016, p. 21.

AMALFITANO C., *Principi e diritti nella Carta e principi generali: sovrapposizioni, interferenze e assimilazioni*, in *I diritti fondamentali fra Carte e Costituzioni europee*, *Scuola superiore della magistratura*, Quaderno 11, Roma, 2022, disponibile online, p. 31.

AMATO S., *Emozioni sintetiche e sortilegi al silicio*, in *Ars interpretandi*, 2021, disponibile online, p. 1.

AMIGONI F., SCHIAFFONATI V., SOMALVICO M., Voce *Storia dell'Intelligenza artificiale,* in E*nciclopedia della Scienza e della Tecnica* (2008), in Treccani online.

AMIT D., ANUPAM D., *Automated Experiments on Ad Privacy Settings a Tale of Opacity, Choice and Discrimination*, in *Proceeding on Privacy Enhancing Technologies*, 2015, p. 105.

ANDREA B., *Artificial Intelligence Does Not Exist! Defying the Technology-Neutrality Narrative in The Regulation of Civil Liability for Advanced Technologies*, in *Europa e diritto privato*, 2022, n. 2, p. 369.

ANDREW P., *Gerrymandering Explained*, in *Vox*, 9 maggio 2019, disponibile online.

ANGELINI L., *A proposito di diritti sociali e principio di uguaglianza nella Carta dei diritti fondamentali dell'Unione Europea,* in *Giornale di diritto del lavoro e di relazioni industriali,* 2001, p. 636.

ASIMOV I., *Robot Visions*, Londra, 1990.

ASTA G., *Il Protocollo n. 16 alla CEDU: chiave di volta del sistema europeo di tutela dei diritti umani?*, in *La Comunità internazionale*, 2013, p. 773.

AULETTA T., *Diritto alla riservatezza e* "droit à l'oubli", in G. Alpa, M. Bessone, L. Boneschi e G. Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, p. 127.

BALBONI M. (a cura di), *The ECHR and the Principle of Non-discrimination*, in *La Ricerca del Diritto nella Comunità internazionale*, Napoli, 2017, p. 20.

BALDRATI A., *Se l'algoritmo diventa lo specchio dei nostri stereotipi: uno studio,* in *Agenda Digitale,* 26 febbraio 2021, disponibile online.

BALLESTRERO M. V., *Ancora sui rider. La cecità discriminatoria della piattaforma*, in *Labor*, 2021, 1, p. 104.

BARBARO C., *CEPEJ, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in *Questione Giustizia*, 7 dicembre 2018, disponibile online.

BARBERA M. (a cura di), *Il nuovo diritto antidiscriminatorio. Il quadro comunitario e nazionale*, Milano, 2007.

BARBERA M., *Discriminazioni ed eguaglianza nel rapporto di lavoro*, Milano, 1991.

BARBERA M., *Il cavallo e l'asino. Ovvero dalla tecnica della norma inderogabile alla tecnica antidiscriminatoria*, in *Eguaglianza e divieti di discriminazione nell'era del diritto del lavoro derogabile,* in O. Bonardi (a cura di), Roma, 2017, p. 17.

BARBERA M., *Il licenziamento alla luce del diritto antidiscriminatorio*, in *Rivista Giuridica del Lavoro*, 2013, p. 139.

BARBERA M., *Il nuovo diritto antidiscriminatorio: innovazione e continuità*, in M. Barbera (a cura di), *Il nuovo diritto antidiscriminatorio*, Milano, 2002, p. XLIII.

BARBERA M., *Principio di eguaglianza e divieti di discriminazione*, in M. Barbera, A. Guariso (a cura di), *La tutela antidiscriminatoria. Fonti, strumenti, interpreti,* Torino, 2019, p. 5.

BARNARD C., HEPPLE B., *Indirect Discrimination: Interpreting Seymour-Smith*, in *Cambridge Law Journal,* 1999, p. 399.

BARNARD C., *The Economic Objectivs of art. 119*, in T. Hervey, O'Keeffe (a cura di), *Sex Equality Law in European Union*, 1996, Wiley, 1996, p. 321.

BASSINI M., GREGORIO G., POLLICINO O., *Il Gdpr e la protezione dei dati nella società algoritmica: i nuovi sviluppi normativi e giuridici*, in *Agenda Digitale*, 9 settembre 2021, disponibile online.

BASSINI M., POLLICINO O., *Intelligenza artificiale e protezione dei dati personali*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol.1, *Diritti fondamentali, dati personali e regolazione*, p. 269.

BELL M., *Anti-Discrimination Law and the European Union*, Oxford, 2002.

BELL M., *The New Article 13 EC Treaty: a Sound Basis for European Anti – Discrimination Law?,* in *Maastricht Journal of European and comparative law*, 1999, n. 1, p. 6.

BENELHOCINE C, *La charte sociale européenne*, Strasbourg, 2011.

BERGONZINI C., *"Prova a prendermi". Ecosistema digitale e consapevolezza degli utenti: uno spazio per la regolazione nazionale?*, in

Osservatoriosullefonti.it, 2, 2022, p. 17 e in G. Di Cosimo (a cura di), *Processi democratici e tecnologie digitali*, in *Osservatorio sulle Fonti, Collana di Studi*, Torino, 2023, p. 91.

BIAGIONI G., CASTANGIA I. (a cura di), *Il principio di non discriminazione nell'Unione europea*, Napoli, 2011.

BIBAL A., LOGNOUL M., DE STREEL A., FRÉNAY B., *Legal Requirements on Explainability in Machine Learning*, in *Artificial Intelligence and Law*, 2021, p. 149.

BOLDRINI N., *Intelligenza Artificiale: Europa "terza incomoda" tra Cina e Usa?*, in *AI4Business*, 26 febbraio 2019, disponibile online.

BOLEGO G., *Intelligenza artificiale e regolazione delle relazioni di lavoro: prime riflessioni*, in *Labor*, 1, 2019, p. 51.

BOMBELLI G., *Tecnologia, diritto, antropologia: appunti sull'Information (Knowledge) Society*, in M. Megale (a cura di), *ICT e diritto nella società dell'informazione*, Torino, 2012, p. 18.

BONARDI O., MERAVIGLIA C., *Dati statistici e onere della prova nel diritto antidiscriminatorio, in Eguaglianza e divieti di discriminazione nell'era del diritto del lavoro derogabile,* a cura di Bonardi O., Roma, 2017, p. 351.

BONINI BARALDI M., *La pensione di reversibilità al convivente dello stesso sesso: prima applicazione della direttiva 2000/78/CE in materia di discriminazione basata sull'orientamento sessuale*, in *Famiglia e diritto*, n. 7/2008, p. 660.

BORGIA F., *L'uso militare dei droni, Profili di diritto internazionale*, Napoli, 2018.

BORZAGA M., MAZZETTI M., *Discriminazioni algoritmiche e tutela dei lavoratori: riflessioni a partire dall'Ordinanza del Tribunale di Bologna del 31 dicembre 2020*, in *BioLaw*, 2022, 1, p. 225, disponibile online.

BOWER J., CHRISTENSEN C. M., *Disruptive Technologies: Catching the Wave*, 1995, in *Harvard Business Review*, 73, 1, 1995, p. 43.

BRADFORD A., *Effetto Bruxelles. Come l'Unione europea regola il mondo*, Milano, 2021.

BRAVO F., *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 103.

BRAVO F., *Trasparenza del codice sorgente e decisioni automatizzate,* in *Diritto dell'informazione e dell'informatica*, 2020, 4, p. 693.

BRENNAN T., DIETERICH W., EHRET B., *Evaluating the Predictive Validity of the COMPAS Risk and Needs Assessment System*, in *Criminal Justice Behavior*, 2009, p. 21.

BRUNO E., *Gender gap: le donne guadagnano il 20% in meno degli uomini*, in *IlSole24Ore*, 28 gennaio 2022, disponibile online.

BULTRINI A., *La questione dell'adesione della Comunità europea alla Convenzione europea dei diritti dell'uomo di fronte alla Corte di giustizia*, in *Rivista di diritto internazionale privato e processuale*, 1997, p. 97.

BURR C., CRISTIANINI N., *Can Machines Read our Minds?,* in *Minds and Machines,* 29, 5, 2019, p. 461, disponibile online.

BURR C., CRISTIANINI N., LADYMAN J., *An Analysis of the Interaction Between Intelligent Software Agents and Human Users*, in *Minds & Machines*, 28, 2018, p. 735.

BYLER D., *In the Camps: Life in China's High-Tech Penal Colony*, Durham, 2022.

BYLER D., *Terror Capitalism Uyghur Dispossession and Masculinity in a Chinese City*, Durham, 2021.

CAGGIA F., *Libertà ed espressione del consenso*, in V. Cuffaro, R. Dorazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2018, p. 253.

CAGGIANO G., *Il quadro normativo del mercato unico digitale*, in *Eurojus*, fascicolo speciale *Mercato Unico Digitale, dati personali e diritti fondamentali*, 2020, p. 13.

CAIANELLO M., *Potenzialità e rischi derivanti dall'interazione tra I.A. e giustizia penale preventiva*, in U. Ruffolo (a cura di), *XXVI Lezioni di Diritto dell'Intelligenza artificiale*, Torino, 2021, p. 206.

CALISKAN A., BRYSON J., NARAYANAN A., *Semantics derived automatically from language corpora contain human-like biases. Science*, 2017, p. 183.

CALZOLAIO E., *Intelligenza artificiale ed autonomia della decisione: problemi e sfide*, in E. Calzolaio (a cura di) *La decisione nel prisma dell'intelligenza artificiale*, Milano, 2020.

CALZOLAIO S., *Protezione dei dati personali*, in *Digesto delle Discipline Pubblicistiche, Aggiornamento*, Torino, 2017, p. 594.

CAPORALE G., *Corso di statistica teorico-pratica*, Napoli, 1976.

CARBONE M.R., *Regolamento europeo sull'intelligenza artificiale in ritardo*, ecco perché, in *Agenda Digitale*, 22 febbraio 2022, disponibile online.

CARDON D., *Che cosa sognano gli algoritmi, Le nostre vite al tempo dei Big Data*, Milano, 2016.

CARPANO E., *État de droit et droits européens. L'évolution du modèle de l' État de droit dans la cadre de l'européanisazion des systèmes juridiques*, Paris-Budapest-Torino, 2005.

CARRER S., *Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin*, in *Giurisprudenza Penale Web*, 2019, disponibile online.

CARROZZA M.C. ET AL., *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, in *BioLaw Journal*, 3, 2019, p. 241.

CARTABIA M., *L'ora dei diritti fondamentali nell'Unione europea,* in M. Cartabia (a cura di), *I diritti in azione*, Bologna, 2007.

CASOLARI F., *Commento agli art. 20 e 21 della Carta dei diritti fondamentali dell'Unione europea*, in F. Pocar, M.C. Baruffi, *Commentario breve ai trattati dell'Unione europea*, II ed., 2011, Padova, p. 1719.

CELOTTO A., *Come regolare gli algoritmi. Il difficile bilanciamento tra scienza, etica e diritto*, in *Analisi Giuridica dell'Economia*, 1, 2019, p. 47.

CENTAMORE G., RATTI L., *Oltre il dilemma qualificatorio: potenzialità e limiti del diritto antidiscriminatorio nella protezione del lavoratore on-demand*, in *Lavoro tramite piattaforma e divieti di discriminazione nell'UE, in Impresa, lavoro e non lavoro nell'economia digitale*, in Alessi C., Barbera M., Guaglianone L. (a cura di), Bari, 2019, p. 663.

CEPEJ, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment adopted by the CEPEJ during its 31st Plenary meeting*, Strasburgo, 3-4 dicembre 2018, disponibile online.

CERESA GASTALDO F., *Lo statuto della giustizia digitale nella Carta etica della CEPEJ*, in *Iusitinere*, 2 aprile 2021, aggiornamento 6 giugno 2022, disponibile online.

CHERCHI R., DEFFENU A., *Le politiche comunitarie di lotta alla discriminazion*e, in *Rassegna di diritto pubblico europeo*, 1, 2004, p. 43.

CHIECO P., *Le nuove direttive comunitarie sul divieto di discriminazione*, in *Rivista Italiana di Diritto del Lavoro,* 2002, p. 75.

CIANCI L., *Dichiarazione europea sui diritti e principi digitali: quid pluris?*, in *Diritto pubblico comparato ed europeo*, 2022, p. 381.

CIHON P., KLEINALTENKAMP M., SCHUETT J., BAUM S. D., *AI Certification: Advancing Ethical Practice by Reducing Information Asymmetries*, in *IEEE Transactions on Technology and Society*, 2021, p. 200.

CIRILLO G.P., *I soggetti giuridici digitali*, in *Contratto e impresa*, 2020, p. 574.

CIRONE E., *Big Data e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale,* Pisa, 2020, p. 143.

COLAPIETRO C., *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Napoli, 2018.

COMANDÈ G., *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità,* in *Analisi giuridica dell'economia*, 2019, p. 172.

COMMISSIONE DELLE COMUNITÀ EUROPEE, *Libro Verde. Uguaglianza e non discriminazione nell'Unione Europea allargata*, Bruxelles, 28.05.2004, COM(2004)379 def.

COMMITTEE OF EXPERT OF INTERNET INTERMEDIARIES, ALGORITHMS AND HUMAN RIGHTS, *Study on the Human Rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, Council of Europe, 2017, disponibile online.

CONDINANZI M., *Diritti, principi e principi generali nell'ordinamento giuridico dell'Unione europea*, in L. D'Andrea, G. Moschella, A. Ruggeri, A. Saitta, *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, Torino, 2016, p. 71.

CONDINANZI M., *Il "livello comunitario" di tutela dei diritti fondamentali dell'individuo*, in P. Bilancia, E. De Marco (a cura di), *La tutela multilivello dei diritti*, Milano, 2004, pp. 35-55.

CONSIGLIO D'EUROPA, *Fifth negotiation meeting between the CDDH and ad hoc negotiation group and the European Commission on the accession of the European Union to the European Convention on Human Rights. Final Report to the CDDH*, (47+1(2013)008Rev2), Strasburgo, 13 giugno 2013.

CONSIGLIO D'EUROPA, *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Appendix, para. A.8,* disponibile online.

CONTALDI G., *La proposta di regolamento sull'intelligenza artificiale la protezione dei dati personali,* in G. Caggiano, G. Contaldi, P. Manzini (a cura di), *Verso una legislazione europea sui mercati e i servizi digitali*, Bari, 2021, p. 207.

CONTI R., *CEDU e Carta UE dei diritti fondamentali, tra contenuti affini e ambiti di applicazione divergenti*, in *I diritti fondamentali fra Carte e Costituzioni europee*, *Scuola superiore della magistratura*, Quaderno 11, Roma, 2022, p. 49, disponibile online.

CONTI R., *La richiesta di "parere consultivo" alla Corte europea delle Alte Corti introdotto dal Protocollo n. 16 annesso alla CEDU e il rinvio pregiudiziale alla Corte di Giustizia UE. Prove d'orchestra per una nomofilachia europea*, in *Consulta Online*;

CONTISSA G., GALLI F., GODANO F., SARTOR G., *Il Regolamento Europeo Sull'intelligenza Artificiale, Analisi informatico-giuridica*, in *i-lex*, 2, 2021, disponibile online.

COSTANTINI F., *Profilazione e "automated decision making" in ambito lavorativo nella giurisprudenza italiana*, in *LG*, 11, 2019, p. 984.

COWGER A., *The Threats of Algorithms and AI to Civil Rights, Legal Remedies, and American Jurisprudence: One Nation Under Algorithms*, Lanham, 2020.

CRAWFORD K., *Artificial Intelligence's White Guy Problem,* 25 giugno 2016, in *New York Times,* disponibile online.

CRUZ VILLALON J., *Lo sviluppo della tutela antidiscriminatoria nel diritto comunitario*, in *Giornale di diritto del lavoro e di relazioni industriali,* 2003, n. 99-100, p. 353.

CURCIO L., GUARISO A., *Articolo 21. Non discriminazione*, in G. Bisogni, G. Bronzini, V. Piccone (a cura di), *La Carta dei diritti dell'Unione Europea. Casi e materiali*, Taranto, 2009, p. 257.

CURREN L., KAYE J., *Revoking Consent: a "Blind Spot" in Data Protection Law?,* in *Computer Law & Security Review*, 2010, Vol. 26, n. 3 p. 273-283.

D. LANEY, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, in *Technical report*, META Group, 2001, disponibile online.

D'ARCANGELO L., *L'obbligo di protezione dei dati del lavoratore: adempimento e sanzioni*, in *Diritti lavori mercati*, 2020, 1, p. 75.

DAELMAN C., *AI through a Human Rights Lens. The Role of Human Rights in Fulfilling AI's Potential*, in J. De Bruyne, C. Vanleenhove (eds.), *Artificial Intelligence and the Law*, Cambridge, 2021, p. 140.

DAGNINO E., ARMAROLI I., *A Seat at the Table: Negotiating Data Processing in the Workplace: A National Case Study and Comparative Insights*, in *Comparative Labor Law & Policy Journal*, 2019, 41, 1, p. 173 ss.

DAGNINO E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, Modena, 2019.

DAGNINO E., *People Analytics: lavoro e tutele al tempo del management tramite big data,* in *Labour & Law Issues*, 2017, 3, p. I.2.

DANIELE L., *La protezione dei diritti fondamentali nell'Unione europea dopo il trattato di Lisbona: un quadro d'insieme,* in *Il Diritto dell'Unione europea*, 4, 2009, p. 640.

DARREN B., *China's Hi-Tech War on its Muslim Minority*, in *The Guardian*, 11 aprile 2019, p. 13, disponibile online.

DASTIN J., *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, in *Reuters*, 10 ottobre 2018, disponibile online.

DE ANNA G., *Automi, Responsabilità e diritto*, in *Rivista di filosofia del diritto*, 2019, p. 125.

DE FRANCESCHI A., *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017.

DE HERT P., PAPAKONSTANTINOU V., *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals*, in *Computer Law & Security Review*, 2012, Vol. 28, n. 2, p. 130.

DE MEYER J., *The Domestication of Smart Home Assistants: Recommendations for Data Controllers on How to Protect Children's Personal Data in Accordance with the GDPR – A Case of Study of Amazon Alexa, Google Assistant and Apple Siri,* Master's Dissertation in Law Ghent University, disponibile online.

DE PASQUALE P., *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *Osservatorio europeo, Il Diritto dell'Unione europea*, 2022, disponibile online.

DE SENA P., *Caratteri e prospettive del Protocollo 16 nel prisma dell'esperienza del sistema interamericano di protezione dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2014, p. 593.

DE SHUTTER O., LEJEUNE Y., *L'adhésion de la Communauté à la Convention européenne des droits de l'homme à propos de l'avis 2/94 de la Cour de justice des Communautés*, in *Cahiers de doit euroéenne*, 1996, p. 555.

DE STEFANO V., "*Negotiating the Algorithm*": *Automation, Artificial Intelligence, and Labor Protection*, in *CLL&PJ*, 2019, 41, 1, p. 15.

DEL PUNTA R*., Innovazioni tecnologiche e diritto del lavoro, in Rivista degli infortuni e delle malattie professionali*, 2019, 106, fasc. 2/3, p. 261.

DELL'UTRI M., *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. Dorazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2018, p. 179.

DELMASTRO M., NICITA A., *Big data. Come stanno cambiando il nostro mondo,* Bologna, 2019.

DI FEDERICO G., *Access to Healthcare in the European Union: Are EU Patients (Effectively) Protected Against Discriminatory Practices?*, in L.S. Rossi, F. Casolari, *The Principle of Equality in EU Law*, Cham, 2017, p. 229;

DI FEDERICO G., *L'accesso alle cure mediche nell'Unione europea tra diritti fondamentali e sovranità nazionali*, in *Quaderni Costituzionali*, 2013, p. 679.

DI FEDERICO G., NEGRI S., *Unione Europea e salute. Principi, azioni, diritti e sicurezza*, Padova, 2020.

DI FEDERICO G., *Protezione della salute,* in S. Di Allegrezza, R. Mastroianni, F. Pappalardo, O. Pollicino, O. Razzolini, (a cura di), *Carta dei diritti fondamentali dell'Unione europea,* Milano, *2017,* p. 664.

DIGNUM V., *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Cham, 2019.

DIRECTORATE OF HUMAN RIGHTS*, Secretariat of the European Commission for the Efficiency of Justice, The CEPEJ European Ethical Charter on the Use of Artificial Intelligence (AI) in Judicial Systems and their Environment. Presentation Note*, 4 dicembre 2018, disponibile online.

DONATI F., *L'adesione dell'Unione europea alla CEDU alla luce del parere 2/13,* in *Rassegna Astrid*, 3/2016, disponibile online.

DONINI A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali*, 2018, p. 222.

DOUGLAS-SCOTT S., *Opinion 2/13 on EU Accession to the ECHR: a Christmas Bombshell from the European Court of Justice*, in *UK Constitutional Law Association*, disponibile online.

DRIGO A., *Sistemi emergenti di intelligenza artificiale e personalità giuridica: un contributo interdisciplinare alla tematica*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 179.

DUBOIS D.J., *Smart Speakers Study - When Speakers Are All Ears: Understanding When Smart Speakers Mistankenly Record Conversations*, *Mon(IoT)r Research Group*, 2020, disponibile online.

DYMITRUK M., *Ethical Artificial Intelligence in Judiciary*, in *Jusletter.it*, 2019, disponibile online.

EBERS M., *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. Ebers, S. Navas Navarro (eds.), *Algorithms and Law*, Cambridge, 2019, p. 49.

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices (2020),* disponibile online.

EDPB, *Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (2020)*, disponibile online.

EDPB, *Guidelines 8/2020 on the Targeting of Social Media Users (2020)*, disponibile online.

EUROPEAN INSTITUTE FOR GENDER EQUALITY, *Artifcial Intelligence, Platform Work and Gender Equality*, 2021, disponibile online.

EY, *Report Taking New Steps Into the Smart Home,* disponibile online.

F. FERRARO, N. LAZZERINI, *Articolo 52*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p.1061.

FAIOLI M., *Discriminazioni digitali e tutela giudiziaria su iniziativa delle organizzazioni sindacali*, in *Diritto delle Relazioni Industriali*, 31, 1, 2021, p. 204.

FALLETTI E., *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in *Diritto dell'informazione e dell'informatica*, 2020, 2, p. 169.

FANCIULLO D., *Parere 2/13 della Corte di giustizia dell'Unione europea: la novissima quaestio dell'adesione dell'Unione europea alla CEDU*, in *Federalismi, Focus Human Rights*, 3 aprile 2015, disponibile online;

FAVILLI C., *La Corte di giustizia rinvia a data da destinarsi l'adesione dell'UE alla CEDU*, in *Questione giustizia*, 3 febbraio 2015, disponibile online.

FAVILLI C., *La non discriminazione nell'Unione europea*, Bologna, 2008.

FEAST J., *4 Ways to Address Gender Bias in AI*, in *Harvard Business Review*, 2019, disponibile online.

FERRARO F., LAZZERINI N., *Articolo 52*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p.1061.

FERRI F., *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Trento, 2022.

FERRI G.B., *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, p. 801.

FINOCCHIARO G., *Considerazioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo *(a cura di)*, *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, Torino, 2021, p. 332.

FINOCCHIARO G., *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza italiana*, 2019, p. 1670.

FINOCCHIARO G., *La memoria della Rete e il diritto all'oblio*, Anno XXVI, fasc. 3, p. 391.

FISICHELLA D., *Elezioni e democrazia. Un'analisi comparata*, Bologna, 2008.

FLOR R., *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di internet*, 2019, 3, p. 453.

FLORIDI L., CABITZA F., *Intelligenza Artificiale – L'uso Delle Nuove Macchine*, Milano, 2021.

FLORIDI L., *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022.

FLORIDI L., *La quarta rivoluzione: Come l'infosfera sta trasformando il mondo*, Milano, 2017.

FLORIDI L., *On Human Dignity as a Foundation for the Right to Privacy*, in *Philosophy and Technology*, 29, 4, 2016, p. 307.

FLORIDI L., *Soft Ethics and the Governance of the Digital* and the General Data Protection Regulation, in *Philos Trans A Math Phys Eng Sci.*, 2018, disponibile online.

FLORIDI L., *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy and Technology*, n. 3, 2020.

FLORIDI L., *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Berlino, 2015.

FLORIDI L., *Translating Principles into Practices of Digital Ethics: Five Risks of Being, in Philosophy and Technology,* 32, 2, 2019, p. 185.

FOGLIA R., *La politica sociale nell'ordinamento comunitario*, in A. Tizzano, *Il diritto privato dell'Unione europea*, Torino, 2000, II, p. 807.

FRA, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, 2018.

FRANCESCONI E., *Intelligenza artificiale e diritto: tra scienza e fantascienza*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 11.

FREEMAN K., *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis*, in *North Carolina Journal of Law & Technology*, 2016, 18, p. 75, disponibile online.

FREEMAN L., *Digital Evidence and War Crimes Prosecutions*: *The Impact of Digital technologies and International Criminal Investigations and Trials,* in *Fordham International Law Journal*, 2018, 41, 2, p. 283.

FRY H., *Don't Believe the Algorithm*, in *The Wall Street Journal*, 5 settembre 2018, disponibile online.

FUMAGALLI MERAVIGLIA M., *Le nuove normative europee sulla protezione dei dati personali,* in *Diritto comunitario e degli scambi internazionali*, 2016, p. 12.

G. MALGIERI, F. A. PASQUALE, *From Transparency to Justification: Toward Ex Ante Accountability for AI*, May 3, 2022, *Brooklyn Law School, Legal Studies Paper No. 712, Brussels Privacy Hub Working Paper, No. 33*, consultabile online.

GAJA G., ADINOLFI A., *Introduzione al diritto dell'Unione europea*, Bari, 2020.

GAJA G., *Opinion 2/94,* in *Common Market Law Review*, 1996, p. 973.

GAJA G., *Una mancata disconnessione relativamente alla Convenzione europea dei diritti dell'uomo?,* in *Rivista di diritto internazionale*, 2015, p. 148.

GAUDIO G., *Algorithmic management, poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo*, in *Labour & Law Issues*, 2020, 2, p. 21.

GÉRON A., *Hands-On Machine Learning with Scikit-Learn, Keras, and Tensorflow: Concepts, Tools, and Techniques to Build Intelligent Systems,* 2nd ed., Sebastopol, 2019.

GIACOMELLI L., *Big Brother is "gendering" you*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 208.

GIACOMELLI L., *Big brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?*, in *BioLaw Journal*, 2019, p. 269.

GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Diritto Penale Contemporaneo*, 2019, p. 12.

GILS T., WAUTERS E., BÉNICHOU B., DE BRUYNE J., VALCKE P., *Artificiële Intelligentie en gegevensbescherming: een verkennende gids. Kenniscentrum Data & Maatschappij*, Brussel, 2020, disponibile online.

GINI C., *I pericoli della Statistica*, *Relazione inaugurale della prima riunione scientifica della Società Italiana di Statistica*, Pisa, 9 ottobre 1939, disponibile online.

GIRAUDO M., *On Legal Bubbles: Some Thoughts on Legal Shockwaves at the Core of the Digital Economy,* in *Journal of Institutional Economics,* 2022, 18, p. 587.

GLESS S., *AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials*, Georgetown Journal of International Law, 2020, vol. 51 n. 2, p. 195.

GONZÁLEZ FUSTER G., GELLERT G., *The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right*, in *International Review of Law, Computers and Technology*, Vol. 26, 1, 2012, p. 73.

GOODFELLOW I., BENGIO Y., COURVILLE A., *Deep Learning*, Cambridge, 2016.

GORI G., *Domestic Enforcement of the European Social Charter: The Way Forward*, in G. De Burca, B. De Witte, *Social rights in Europe*, New York, 2005, p. 70.

GOTTARDI D., *Giustizia retributiva e trasparenza,* in *Studi in Memoria di Massimo Roccella*, Torino, 2021, p. 185.

GRANIERI M., *Il trattamento di categorie particolari di dati personali nel regolamento UE 2016/679*, in *NLCC*, 2017, p. 165.

GRECO L., MENEGHETTI M.C., *Articolo 3*, in F. Delfini, G. Finocchiaro (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014*, Torino, 2017, p. 29 ss.

GRIECO C., *Ancora sul diritto all'oblio: la Corte di giustizia si pronuncia sull'obbligo di deindicizzazione di contenuti nel caso in cui contengano informazioni inesatte*, in *Osservatorio sulla Corte di giustizia dell'Unione europea n.1/2023*, *Ordine internazionale e diritti umani*, 2023, p. 199.

GRIECO C., *Il Protocollo n. 16 allegato alla CEDU e la funzione consultiva della Corte Europea dei Diritti dell'Uomo anche alla luce della*

futura e ancora incerta ratifica italiana, in *Cuadernos de Derecho Transnacional*, 2022, 14, 1, p. 313.

GRIECO C., *Intelligenza artificiale e diritti umani nel diritto internazionale e dell'Unione europea. Alla ricerca di un delicato equilibrio*, in *Ordine internazionale e diritti umani*, 2022, p. 782.

GRIECO C., *L'attuazione in Italia del diritto all'oblio*, in *Il Mercato Unico Digitale*, (a cura di) Gianluca Contaldi, *Diritto, Mercato e Tecnologia, numero speciale 2017, Atti del Convegno*, p. 161.

GRIECO C., *Le linee guida della Commissione europea e il libro bianco sull'intelligenza artificiale*, in R. Giordano, A. panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale, Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, p. 475.

GRUPPO DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE (AI HLEG), *Orientamenti etici per un'IA affidabile*, 8 aprile 2019, disponibile online.

GUIMARÃES R.C.A., *A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal,* in *Revista Brasileira de Direito Processual Penal*, 5, 3, 2019, p. 1555.

HÄBERLE P., *I diritti fondamentali nelle società pluraliste e la Costituzione del pluralismo*, in M. Luciani (a cura di), *La democrazia alla fine del secolo*, Roma-Bari, 1994, p. 97.

HÄBERLE P., voce *Stato costituzionale I) Principi generali*, trad. it. di F. Politi, S. Rossi, in *Enc. giur. Trecc.*, Aggiornamento, Vol. IX, Roma, p. 1.

HACKER P., *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Discrimination Under EU Law*, in *Common Market Law Review,* 2018, p. 1143.

HALBERSTAM D., *"It's the Autonomy, Stupid!" A Modest Defense of Opinion 2/13 on EU Accession to the ECHR, and the Way Forward*, in *German law journal*, 2015, Vol. 16, 1, p. 105;

HARDESTY L., *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems. Examination of Facial-Analysis Software Shows Error Rate Of 0.8 Percent for Light-Skinned Men, 34.7 Percent for Dark-Skinned Women*, in *MIT News*, disponibile online.

HENDRICKX F., *Privacy 4.0 at Work: Regulating Employment, Technology and Automation*, in *CLL&PJ*, 2019, 41, 1, p. 147.

HENRIKSEN A., *Certification Standards and Explanation Methods in Applied IA*, in *AIES 21, Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics and Society*, 2021, p. 574.

HIJMANS H., *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Brussels, 2016.

HUMAN RIGHTS COMMITTEE, *General Comment No. 32, Article 14: Right to Equality Before Courts and Tribunals and to a Fair Trial*, U.N. Doc. CCPR/C/GC/32 (2007).

HUMAN RIGHTS WATCH, *China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App*, 1 maggio 2019, disponibile online.

INGRAO A., *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *LLI*, 2019, 2, p. 129.

JORDAN E., *How Computers Turned Gerrymandering Into a Science*, in *New York Times*, 6 ottobre 2017, disponibile online.

KANT E., *Critica della ragion pratica*, trad. Francesco Capra, Bari, 1909; revisione della traduzione di Eugenio Garin (basata sull'edizione dell'Accademia di Prussia), Glossario e Indice a cura di Vittorio Mathieu, Bari, 1971; Introduzione di Sergio Landucci, Bari, 1997.

KIERKEGAARD S., WATERS N., GREENLEAF G., BYGRAVE L.A., LLOYD I., SAXBY S., *30 years on – The review of the Council of Europe Data Protection Convention 108, Computer Law & Security Review*, Vol. 27, n. 3, 2011, pp. 223-231.

KING A. G., MRKONICH M., *"Big Data" and the Risk of Employment Discrimination,* in *Oklahoma Law Review*, 2016, 68, 3, p. 557.

KRAFT J.T., *Big Data Analytics, Rising Crime, and Fourth Amendment*, in *University of Illinois Journal of Law, Technology & Policy*, 2017, p. 249.

KULLMAN M., *Platform Work, Algoritm Decision-Making, and EU Gender Equality Law*, in *IJCLLIR*, 2018, 34, p. 11.

LAMARQUE E. (a cura di), *La richiesta di pareri consultivi alla Corte di Strasburgo da parte delle più alte giurisdizioni nazionali: prime riflessioni in vista della ratifica del Protocollo 16 alla Convenzione europea dei diritti dell'uomo*, Milano, 2015.

LANGHANKE C., SCHMIDT-KESSEL M., *Consumer Data as Consideration*, in *Journal of European Consumer and Market Law*, 2015, 6, p. 218.

LANZO R., GIORDANO M., *Diritto all'oblio e motori di ricerca: Il diritto di essere dimenticati. I casi decisi dal garante,* Milano, 2021.

LARSON J., ANGWIN L., MATTU S., KIRCHNER L., *Machine Bias, There's software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks, ProPublica*, 23 maggio 2016, disponibile online.

LAU J., ZIMMERMAN B., SCHAUB F., *Alexa are you listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviours with Smart Speakers*,

in *Proceedings of the ACM on Human-Computer Interaction*, 2018, Vol. 2, Art. 102, disponibile online.

LAVIOLA F., *Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa*, in *BioLaw Journal*, 3, 2020, p. 389 ss.

LAVORGNA A., SUFFIA G., *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*, in *Diritto Penale Contemporaneo*, 2021, p. 88.

LAZZERINI N., *"Questo matrimonio (così?) non s'ha da fare": il parere 2/13 della Corte di giustizia sull'adesione dell'Unione Europea alla Convenzione europea sui diritti dell'uomo*, in *Osservatorio sulle fonti*, disponibile online.

LOCHAK D., *La notion de discrimination*, in *Confluences Méditerranée*, 2004, p. 13.

LOCHAK D., *Réflexion sur la notion de discrimination,* in *Droit social*, 1987, p. 778.

LOCK T., *Oops! We did it again – the CJEU's Opinion on EU Accession to the ECHR*, 18 dicembre 2014, disponibile online.

LONGO A., SCORZA G., *Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà*, Milano, 2020.

LONGO E., *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol.1, *Diritti fondamentali, dati personali e regolazione*, p. 352.

LYNSKEY O., D*econstructing Data Protection: The 'Added-Value' of a Right To Data Protection in the EU Legal Order*, in *International And Comparative Law Quarterly,* 2014, Vol. 63, n. 3, p. 569.

LYNSKY O., *Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing*, In *International Journal Of Law In Context*, 2019, p. 162.

LYON D., *Surveillance Society. Monitoring Everyday Life*, in *Open University Press*, 2001, disponibile online.

M. SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, p. 123.

MACKENZIE C., ROGERS W., DODDS S., *Vulnerability: New Essays in Ethics and Feminist Philosophy*, Oxford, 2014, p. 20.

MADOTTO P., *ChatGPT, ora basta giocare: ecco utilizzi e rischi (seri)*, in *Agenda Digitale*, 20 gennaio 2023, disponibile online.

MAIO V., *Il diritto del lavoro e le nuove sfide della rivoluzione robotica*, in *ADL*, 2018, 6, p. 1414.

MALGIERI G., CUSTERS B., *Pricing Privacy – The Right to Know the Value of Your Personal Data*, in *Computer Law & Security Review*, 34, 2017, p. 294.

MARANELLA S., *La protezione dei dati personali contro un uso distopico dell'AI*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale, Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, p. 51.

MARCHINI A., *Intelligenza artificiale e responsabilità civile: dal "Responsibility Gap" alla responsabilità elettronica dei robot*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 231.

MATZ S. C., KOSINSKI M., NAVE G., STILLWELL D.J., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion, Proceedings of the National Academy of Sciences*, 2017, p. 12714.

MCCARTHY J., MINSKY M.L., ROCHESTER N., SHANNON C.E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955, in *AI Magazine Volume 27 Number 4,* 2006.

MCCARTHY K., *What We Know About the Small Change to Facebook's Slogan*, 28 agosto 2019, disponibile online.

METZGER A., *Data as CounterPerformance: What Rights and Duties do Parties Have?,* in *Journal of Intellectual Property*, *Information Technology and Electronic Commerce Law*, 8, 2017, p. 1;

MEZZANOTTE M., *Il Diritto all'oblio, Contributo all'analisi della privacy storica*, Napoli, 2009.

MIGLIOZZI S., OH Y.T., HASANAIN M. ET AL., *Integrative Multi-Omics Networks Identify PKCϑ and DNA-PK as Master Kinases of Glioblastoma Subtypes and Guide Target Cancer Therapy,* in *Nature Cancer, 2023,* disponibile *online.*

MILITELLO M., *Principio di uguaglianza e di non discriminazione tra Costituzione italiana e Carta dei diritti fondamentali dell'Unione Europea* (*artt. 3 Cost.; art. 20 e art. 21 Carta di Nizza)*, in *Biblioteca '20 Maggio'*, 1, 2010, p. 140, originariamente pubblicato come WP C.S.D.L.E. "Massimo D'Antona".INT – 77/2010.

MILITELLO M., STRAZZARI D., *I fattori di discriminazione*, in Barbera M. Guariso A. (a cura di), *La tutela antidiscriminatoria,* Milano, 2019, p. 85.

MITCHELL T.*, Machine Learning,* New York, 1997.

MOBILIO G., *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *Federalismi.it*, n. 16, 2020, p. 266.

MÖKANDER J., AXENTE M., CASOLARI F., FLORIDI L., *Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation,* in *Minds and Machines*, 2021, p. 1.

MONACO M. P., *Controlli a distanza sui lavoratori: evoluzione, riforme e privacy*, in *Labor*, 2021, 2, p. 155.

MORELLI C., *Intelligenza artificiale e la partita della Explainable AI*, in *Altalex*, 14 giugno 2021, disponibile online.

MORELLI S., *voce Oblio (diritto all')*, in *Enc. dir. agg.*, VI, Milano, 2002, p. 851;

MORGESE G., *La tutela del software in Europa tra normativa internazionale e comunitaria*, in *Sud in Europa*, 2009, disponibile online.

MORGESE G., *Principio e strumenti della democrazia partecipativa nell'Unione europea*, in E. Triggiani (a cura di), *Le nuove frontiere della cittadinanza europea*, Bari, 2011, p. 37.

MORO P., *Alle frontiere della soggettività: indizi di responsabilità delle macchine intelligenti*, in U. Ruffolo (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, p. 55.

MOSCONI F., *Il trattato di Maastricht: una costituzione per l'Europa?,* in *Il Politico*, Vol. 57, No. 3, Luglio-Settembre 1992, p. 421.

NALIN E., *I Protocolli n. 15 e 16 alla Convenzione europea dei diritti dell'uomo*, in *Studi sull'integrazione europea*, 2014, p. 117.

NATO A.*, Il diritto alla salute dei cittadini dell'Unione e l'assistenza sanitaria transfrontaliera: recenti sviluppi,* in *Studi sull'integrazione europea,* 2-3/2016, p. 573.

NAUDTS L., *AI en algoritmische categorisatie: gelijkheid en non-discriminatie*, in Jan De Bruyne, Nicolas Bouteca (eds.) *Artificiële intelligentie en maatschappij*, Oud-Turnhout/'s-Hertogenbosch, 2021, p. 223.

NI LOIDEAIN N., ADAMS R., *From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistant and the Role of Data Protection Impact Assessments*, in *Computer Law and Security Review*, 2020, p. 1.

NIGER S., *Il diritto all'oblio*, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale,* Padova, 2007, p. 59.

NINATTI S., *Il caso Romer: limiti di materia, principio di uguaglianza o tutela di diritti?*, in *Quaderni costituzionali*, n. 3/2011, p. 693.

NUMERICO T., *Social network e algoritmi di machine learning: problemi cognitivi e propagazione dei pregiudizi*, in *Sistemi intelligenti*, 2019, p. 469.

O'NEIL C., *Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy*, New York, 2016.

O'NEILL B., *Inflating Away Our Human Rights*, in *MisesInstitute blog*, 14 dicembre 2009, disponibile online.

OGRISEG C., *GDPR and Personal Data Protection in the Employment Context*, in *LLI*, 2017, 2, p. R-1.

OLIVERI F., *La Carta sociale europea tra enunciazione dei diritti, meccanismi di controllo e applicazione nelle corti nazionali. La lunga marcia verso l'effettività*, in *Rivista del Diritto della Sicurezza Sociale*, n. 3/2008, p. 509.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT*, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OEDC *Digital Economy Papers* No. 220, 2013 disponibile online.

PACELLA G., *La nozione euro-unitaria di lavoratore dipendente alla prova della gig-economy: si pronuncia la Corte di giustizia europea*, in *Labour & Law Issues*, 2020, 1, p. R.17.

PACKARD V., PAYNE R., *The Hidden Persuaders*, New York, 1957.

PAJNO A., BASSINI M., DE GREGORIO G., MACCHIA M., PATTI F.P., POLLICINO O., QUATTROCOLO S., SIMEOLI D., SIRENA P., *AI: profili giuridici – Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *Rivista di Biodiritto*, vol. 3, 2019, p. 210.

PALMIRANI M., *Big Data e conoscenza*, in *Rivista di filosofia del diritto,* n. 1/2020, p. 73.

PARISI N., URSO G., *I principi di eguaglianza e di non discriminazione nell'ordinamento dell'Unione europea, Osservatorio sul rispetto dei diritti fondamentali in Europa,* 2011, n. 24, disponibile online.

PARODI M., *L' adesione dell'Unione Europea alla Cedu*: *dinamiche sostanziali e prospettive formali*, Padova, 2020.

PARODI M., *L'adesione dell'Unione europea alla CEDU: un "nuovo" inizio?*, in *Osservatorio sulle fonti*, 3, 2020, disponibile online.

PASQUALE F., *The Black Box society. The Secret Algorithms Money and Information*, Cambridge, 2016.

PATEL K., *Incremental Journey for World Wide Web: Introduced with Web 1.0 to Recent Web 5.0 – A Servey Paper*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013, 3, 10, p. 410.

PECK D., *They're Watching You at Work*, in *Theatlantic.com*, 2013, disponibile online.

PEERS S., *The CJEU and the EU's Accession to the ECHR: A Clear and Present Danger to Human Rights Protection*, 18 dicembre 2014, disponibile online.

PELAGALLI F., *IA, cinque principi per un modello di sviluppo etico,* in *Il Sole24Ore*, 15 luglio 2018, disponibile online.

PELLECCHIA E., *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation,* in *Le Nuove leggi civili commentate*, 2018, p. 1209.

PENROSE R., *La mente nuova dell'imperatore*, Milano, 1992.

PERULLI A., *La "soggettivazione regolativa" nel diritto del lavoro*, in *DRI*, 2019, 1, p. 111.

PERULLI A., *La discriminazione algoritmica: brevi note introduttive a margine dell'Ordinanza del Tribunale di Bologna*, in *LDE*, 1, 2021, disponibile online.

PERUZZI M., *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *LLI*, Vol. 7, No. 1, 2021, p. I-50.

PERUZZI M., *La prova del licenziamento ingiustificato e discriminatorio*, Torino, 2017.

PICARELLA G., *Le discriminazioni fondate sull'orientamento sessuale nella giurisprudenza della Corte di Giustizia: dal caso P. alla sentenza Romer*, in *Rivista Italiana del Diritto del Lavoro*, n. 4/2011, p. 1325.

PIZZETTI F., (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

PIZZETTI F., *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 5.

PIZZETTI F., *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il 'Velo di Maya'*, in G. Resta, Zeno-Zencovich (a cura di), *Il Diritto all'oblio su internet dopo il caso Google Spain*, Roma, 2015, p. 255.

POCCIANTI P., *Le potenze investono sull'intelligenza artificiale: il ruolo dell'Europa tra Usa e Cina*, in *Agenda Digitale*, 22 febbraio 2019, disponibile online.

POLETTI D., *Le condizioni di liceità del trattamento dei dati personali, in Giurisprudenza italiana*, 2019, n. 12, p. 2783.

POLLICINO O., BASSINI M., *Art. 8*, *Protezione dei dati personali*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 134.

POLLICINO O., *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it,* n. 19, 2019, p. 2.

POLLICINO O., SCIARABBA V., *La Carta di Nizza oggi, tra "sdoganamento giurisprudenziale" e Trattato di Lisbona*, in *Diritto Pubblico Comparato e Europeo*, 2008, p. 101.

QUATTROCOLO S., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche, in Legislazione Penale*, 18 dicembre 2018, disponibile online.

QUINN E., *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in *verfassungsblog.de*, 22 December 2022, disponibile online.

RESTA F., *Sub art punto 6, reg. UE n. 679/2016*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2018, p. 63.

RESTA G., *Codice della privacy e data protection*, Milano, 2021.

RESTA G., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza,* in *Politica del diritto*, 2019, p. 199.

RESTA G., ZENO-ZENCOVICH V., *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, p. 436.

RICCIO G.M., GIANNONE CODIGLIONE G., *La rilevanza delle basi giuridiche per il trattamento di dati personali mediante sistemi di intelligenza artificiale*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol.1, *Diritti fondamentali, dati personali e regolazione*, p. 285.

RICCIUTO V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. Inf.,* 2018, 4-5, p. 689.

ROCCELLA M., TREU T., *Diritto del lavoro della Comunità Europea*, Padova, 2002.

RODOTÀ S., *Il diritto al cibo,* in *Quaderni del Corriere della Sera,* 2014, p. 5.

RODOTÀ S., *Il diritto di avere diritti*, Bari, 2012.

RODOTÀ S., *Il mondo nella rete. Quali diritti, quali vincoli*, Bari, 2014.

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997.

ROSSI L. S., *Il Parere 2/13 della CGUE sull'adesione dell'UE alla CEDU: scontro fra Corti?,* 22 dicembre 2014, in *Sidi Blog*, disponibile online.

ROSSI L. S., *Il parere 2/94 sull'adesione della comunità europea alla Convenzione europea dei diritti dell'uomo*, in *Il diritto dell'Unione europea*, 1996, p. 839.

ROTA A., *Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, in *LLI*, 2017, 3, 1, p. I. 32-52.

RUFFOLO U., *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giurisprudenza Italiana*, 2019, 7, p. 1657.

RUFFOLO U., *La personalità elettronica tra "doveri" e "diritti" della macchina*, in U. Ruffolo (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, p. 115.

RUOTOLO G.M., *La disciplina europea della responsabilità dei fornitori dei servizi online tra regime pregresso, proposte di riforma e un rischio di* bis in idem, in G. Caggiano, G. Contaldi, P. Manzini (a cura di), *Verso una legislazione europea sui mercati e i servizi digitali*, Bari, 2021, p. 59.

RUOTOLO G.M., *Imparzialità e indipendenza dei giudici, intelligenza artificiale, diritto internazionale,* in S. CAFARO (a cura di), *Beni e valori comuni nella dimensione internazionale e sovranazionale – Atti del XXV Convegno annuale della Società italiana di Diritto internazionale e di Diritto dell'Unione europea (SIDI)*, Lecce, 24 e 25 settembre 2021, Napoli, 2022, p. 357.

RUOTOLO G.M., *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, p. 97.

RUOTOLO G.M., The God that failed. *La tutela dei* co-patterners *nell'ordinamento internazionale ed europeo, in Rivista di diritto dei media*, 2018, disponibile online.

RUOTOLO G.M., *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021.

SACCUCCI A., *Profili di tutela dei diritti umani tra Nazioni Unite e Consiglio d'Europa*, Padova, 2005, p. 180.

SALENTO A., *Digitalizzazione delle imprese e trasformazione delle competenze. Quadro analitico e riscontri empirici*, in *Labor*, 2019, 2, p. 131.

SANDULLI S., *Algoritmi, trasparenza ed effettività del consenso*, in *Ius Civile*, 2021, 5, p. 1528.

SANGUINETTI G., *Machine Learning: accuratezza, interpretabilità e incertezza, in Ithaca: Viaggio nella Scienza*, 2020, 16, p. 71.

SANTAGATA DE CASTRO R., *Anti-discrimination Law in the Italian Courts: the new frontiers of the topic in the age of algorithms*, in WP C.S.D.L.E. "Massimo D'Antona".IT – 440/2021, disponibile online.

SANTOSUOSSO A., *Intelligenza artificiale e diritto*, *Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020.

SARTOR G., *Artificial Intelligence: Challenges for EU Citizens and Consumers. Briefing. Requested by the IMCO committee*, 2019, disponibile online.

SARTOR G., *Artificial Intelligence: Challenges for Eu Citizens and Consumers*, gennaio 2019, *Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies,* disponibile online.

SARTORI A., *Il controllo tecnologico sui lavoratori*, Torino, 2020.

SARTORI L., *Il digital divide*, Bologna, 2006

SCHEPISI C., *Diritti fondamentali, principi democratici e rule of law: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol.1, *Diritti fondamentali, dati personali e regolazione,* p. 203.

SCHEPISI C., *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *Quaderni AISDUE, Atti convegni AISDUE*, n. 16, 28, 2022, p. 330.

SCHILDT H., *The Data Imperative*, Oxford, 2020.

SCHOORS K., *Ai en digitale dictatuur,* in J. De Bruyne, N. Bouteca (a cura di), *Artificiële intelligentie en maatschppij*, Turnhout, 2021, p. 20.

SCIARRA S., *Integrazione dinamica tra fonti nazionali e comunitarie: il caso del lavoro notturno delle donne*, in *Il diritto del lavoro*, 1995, p. 153.

SELBST A. D., POWLES J., *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 2017, n. 4, p. 233.

SHIN H., ROTH H.R., GAO M., LE L., XU Z., NOGUES I., YAO J., MOLLURA D., SUMMERS R.M., *Deep Convolutional Neural Networks for*

Computer-Aided Detection: CNN Architectures, Dataset Characteristics and Transfer Learning, 35, 5, 2016, p. 1285, disponibile online.

SIANO M., *Il diritto all'oblio in Europa e il recente caso spagnolo*, in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, p.123.

SICA S., *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Rivista di diritto civile*, 2001, p. 621.

SICILIANOS L.-A., *L'élargissement de la compétence consultative de la Cour européenne des droits de l'homme – À propos du Protocole n° 16 à la Convention européenne des droits de l'homme*, in *Revue trimestrielle des droits de l'homme*, 2014, p. 9.

SIMITIS S., *Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?,* in *Neue Juristische Wochenschrift*, 1997, n. 5, p. 281.

SIMONCINI A., *Art. 22*, in R. D'Orazio, G. Finocchiario, O Pollicino, G. Resta (a cura di), *Codice della Privacy e data protection*, Milano, 2021, p. 387.

SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, p. 63, disponibile online.

SIMONCINI A., SUWEIS S., *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista internazionale di filosofia del diritto*, 1, 2019, p. 87.

SIMONE G., *Machine Learning e tutela della Privacy alla luce del GDPR*, in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, p. 125.

SITZIA A., CRAFA S., *Impronte digitali, algoritmo e trattamento di dati personali: questioni di "law and technology",* in *LG*, 2019, 3, p. 245.

SOMALVICO M., *Intelligenza artificiale*, Milano, 1987.

STANZIONE P., *La democrazia alla sfida degli algoritmi*, in Repubblica, 18 aprile 2021, disponibile online.

STEED R., CALISKAN A., *Image Representations Learned with Unsupervised Pre-Training Contain Human-like Biases*, in *arXiv:2010.15052 [cs.CY]*, 27 gennaio 2021, disponibile online.

STROZZI G., MASTROIANNI R., *Diritto dell'Unione europea*, Torino, 2017.

TAFANI D., *"Automaticamente illegali". Una proposta per i sistemi di intelligenza artificiale,* in *Bollettino telematico di filosofia politica*, 7 novembre 2022, consultabile online.

TEBANO L., *Tutela della privacy e potere di controllo del datore di lavoro tra l'ordinamento italiano e le fonti europee*, in *Labour & Law Issues*, 2017, 2, p. C-1.

TESAURO G:, *Bocciatura del progetto di accordo sull'adesione dell'Unione europea alla CEDU: nessuna sorpresa, nessun rammarico*, in *Foro Italiano*, 2015, 4, p. 77.

TESAURO G., *Eguaglianza e legalità nel diritto comunitario [Relazione presentata al Convegno dell'Associazione italiana dei Costituzionalisti, Trieste, 17-19 dicembre 1998*], in *Il diritto dell'Unione europea*, 1999, p. 1.

TESAURO G., *Manuale di diritto dell'Unione europea*, a cura di P. De Pasquale, F. Ferraro, volume I, Napoli, 2021.

THIENE A., *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, fasc. 2, p. 440;

THOBANI S., *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws*, 11, 2019, p. 132, disponibile online.

TIMMIS S., BROADFOOT P., SUTHERLAND R., OLDFIELD A., *Rethinking Assessment in a Digital Age: Opportunities, Challenges and Risks*, in *British Educational Research Journal*, 2016, p. 454 disponibile online.

TOMMASI S., *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo,* in *Revista de Direito Brasileira*, v. 27, n. 10, 2020, p. 112.

TREZZA R., *Diritto e intelligenza artificiale. Etica-Privacy-Responsabilità-Decisione*, Pisa, 2020.

TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.

TULLINI P., *Divieto di indagini sulle opinioni e trattamenti discriminatori, in Il nuovo mercato del lavoro*, coordinato da Pedrazzoli M., Bologna, 2004, p. 145 ss.

TULLINI P., *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in P. Tullini (a cura di) *Web e lavoro. Profili evolutivi e di tutela*, Torino, 2017, p. 3.

TULLINI P., *La salvaguardia dei diritti fondamentali della persona che lavora nella gig-economy*, in Costituzionalismo online, 2020, 1, p. 39.

TUOMI, I., *The Impact of Artificial Intelligence on Learning, Teaching, and Education*, Cabrera Giraldez M., Vuorikari R., Punie, Y. (eds.), Luxembourg, 2018, p. 27 ss.

TURING A.M., *Computing Machinery and Intelligence*, Oxford, 1950.

TWIGG-FLESNER C., *Disruptive Technology – Disruptive Law? How the Digital Revolution Affects (Contract) Law,* in A. De Franceschi (ed), *European Contract Law and the Digital Single Market: The Implications of*

the Digital Revolution, Cambridge-Antwerp-Portland, Intersentia, 2016, p. 21.

VAN DIJK J., *The digital divide*, Cambridge, 2020.

VAN EST R., GERRITSEN J., KOOL L., *Report Human Rights in the Robot Age, Challenges Arising from the Use of Robotics, Artificial Intelligence, and Virtual and Augmented Reality,* 2017, disponibile online.

VAN VEEN C., *Artificial Intelligence; What's Human Rights Got to Do with It?,* in *Data & Society: Points – blog of Data & Society Research Institute*, 14 May 2018, disponibile online.

VANDER MAELEN C., LIEVENS E., VERMEULEN J., MILKAITE I., *AI and Data Protection: The Case of Smart Home Assistant,* in J. De Bruyne, C. Vanleenhove (a cura di) *Artificial Intelligence and the Law*, Cambridge, 2022, p. 181.

VENANZONI A., *Intersezioni costituzionali – Internet e Intelligenze Artificiali tra ordine spontaneo, natura delle cose digitale e garanzia dei diritti fondamentali*, in *Forum di Quaderni Costituzionali*, 27 aprile 2018, p. 4.

VENEZIANI B., *Nel nome di Erasmo da Rotterdam. La faticosa marcia dei diritti sociali fondamentali nell'ordinamento comunitario*, in *Riv. Giur. Lav*. n. 1/2000, p. 779.

VEZZANI S., *"Gl'è tutto sbagliato, gl'è tutto da rifare!": la Corte di giustizia frena l'adesione dell'UE alla CEDU*, in *Sidi Blog*, disponibile online;

VIGONI D., *Entra in vigore (ma non per l'Italia) il Protocollo n. 16 alla CEDU che consente di richiedere alla Corte EDU un parere consultivo*, in *Processo Penale e Giustizia*, 2018, p. 6.

VILLANI U., *Il Protocollo n. 14 alla Convenzione europea dei diritti dell'uomo,* in *La Comunità internazionale*, 2004, p. 487.

VINCENT J., *Google 'fixed' its racist algorithm by removing gorillas from its image-labeling tech, The Verge*, 12 gennaio 2018, disponibile online.

VITERBO F. G., *Freedom of contract and the commercial value of personal data*, in *Contratto e impresa Europa*, 2, 2016, p. 606.

VIZIOLI M., *Il diritto comunitario tra principio di non discriminazione e tutela delle differenze*, in *Il diritto del mercato del lavoro*, n. 3/2004, p. 953.

VOLAND T., SCHIEBEL B., *Advisory Opinions of the European Court of Human Rights: Unbalancing the System of Human Rights Protection in Europe?*, in *Human Rights Law Review*, 2017, p. 73.

WACHTER S., MITTELSTADT B., FLORIDI L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, n. 2, p. 76.

WADDINGTON L., *Testing the Limits of the EC Treaty Article on Non-Discrimination*, in *Industrial Law Journal*, 1998, n. 1, p. 134.

WAGNER B., *Ethics As an Escape From Regulation. From "Ethics-Washing" to Ethics-Shopping?*, in *Being Profiled: Cogitas Ergo Sum*, Amsterdam, 2018, parte IV, disponibile online.

WIENER N., *The Human Use of Human Beings: Cybernetics and Society*, Boston, 1954.

WORLD ECONOMIC FORUM, *Jobs of Tomorrow – Mapping Opportunity in the New Economy*, gennaio 2020, disponibile online.

WP ART. 29, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12*, 26 novembre 2014, disponibili online.

WP29, *Guidelines on consent under Regulation 2016/679 (2018)*, disponibile online.

WU T., *The Attention Merchants. The Epic Struggle to Get inside Our Heads*, New York, 2016, p. 25.

YORDANOVA K., *AI is a Girl's Best Friend? A Gender-Based Analysis of the Legal and Ethical Challenge of AI Systems*, in *Global Wo-Men Hub Blog*, 2020-11, disponibile online.

ZANGHÌ C., *Un'altra critica al parere 2/94 della Corte sull'adesione della Comunità alla Convenzione europea dei diritti dell'uomo*, in *Scritti in onore di Giuseppe Federico Mancini,* Milano, 1998, p. 1101.

ZANICHELLI M., *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in A. D'ALOIA (a cura di) *Intelligenza artificiale e diritto, come regolare un mondo nuovo*, Milano 2021, p. 56.

ZAPPALÀ L., *Informatizzazione dei processi decisionali e diritto del lavoro: algoritmi, poteri datoriali e responsabilità del prestatore nell'era dell'intelligenza artificiale,* in S. Aleo (a cura di), *Evoluzione scientifica e profili di responsabilità*, Pisa, 2021, p. 363.

ZENO-ZENCOVICH V., *Do "Data Markets" Exist?,* in *MediaLaws*, 1, 2019, p. 22 ss.

ZUBOF S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma, 2019.

ZUDDAS P., *Intelligenza artificiale e discriminazioni*, in *Consulta online*, 2020, p. 1.

Elenco siti internet

https://doi.org/10.1002/berj.3
https://www.ohchr.org/en/documents/country-reports/ohchr-assessment-human-rights-concerns-xinjiang-uyghur-autonomous-region
https://www.ilsole24ore.com/art/il-gender-gap-tempi-covid-donne-guadagnano-20percento-meno-uomini-AE6QYpAB
https://gwmh.org/ai-is-a-girls-best-friend-a-gender-based-analysis-of-the-legal-and-ethical-challenges-of-ai-systems/
https://rm.coe.int/artificial-intelligence-platform-work-and-gender-equality/1680a56b24
https://hbr.org/2019/11/4-ways-to-address-gender-bias-in-ai
https://rm.coe.int/artificial-intelligence-platform-work-and-gender-equality/1680a56b24
https://teachtoone.org
https://read.oecd-ilibrary.org/education/trustworthy-artificial-intelligence-ai-in-education_a6c90fa9-en#page1
file:///Users/Cri/Downloads/jrc113226_jrcb4_the_impact_of_artificial_intelligence_on_learning_final_2.pdf
https://www.vox.com/2014/8/5/17991934/gerrymandering-explained
https://www.nytimes.com/2017/10/06/opinion/sunday/computers-gerrymandering-wisconsin.html
https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212
https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass
https://scholarship.law.unc.edu/ncjolt/vol18/iss5/3
https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
https://www.iusinitinere.it/lo-statuto-della-giustizia-digitale-nella-carta-etica-della-cepej-36950#_ftn7
http://blog.petiteplaisance.it/wp-content/uploads/2018/01/04-Corrado-Gini-I-pericoli-della-statistica_08.pdf
https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/631043/IPOL_BRI(2019)631043_EN.pdf
https://www.wsj.com/articles/dontbelieve-the-algorithm-1536157620
https://feliciapelagalli.nova100.ilsole24ore.com/2018/07/15/ia-cinque-principi-per-un-modello-di-sviluppo-etico/

https://www.agendadigitale.eu/cultura-digitale/le-potenze-investono-sullintelligenza-artificiale-il-ruolo-delleuropa-tra-usa-e-cina/
https://hbr. org/2019/11/4-ways-to-address-gender-biasin-ai
https://www.rathenau.nl/en/digitale-samenleving/human-rights-robot-age
https://tweakers.net/nieuws/94273/kabinet-zet-telefoon-uit-omwifi-tracking-tegen-te-gaan.html
https://www.altalex.com/documents/news/2021/06/14/intelligenza-artificiale-e-partita-explainable-ai
https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html
http://blog.petiteplaisance.it/wpcontent/uploads/2018/01/04-Corrado-Gini-I-pericoli-della-statistica_08.pdf
https://teachtoone.org
https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf
https://www.lavorodirittieuropa.it/images/T._Bologna_rider_perulli_1.pdf
garanteprivacy.it/temi/assistenti-digitali

Giurisprudenza
Decisioni della Corte di giustizia dell'Unione europea

8 aprile 1976, causa C-43/75, *Defrenne/SABENA*, ECLI:EU:C:1976:56.
12 luglio 1984, causa C-184/83, *Hofmann*, ECLI:EU:C:1994:273.
13 maggio 1986, causa C-170/84, *Bilka*, ECLI:EU:C:1986:204.
30 giugno 1988, causa C-318/86, *Commissione c. Francia*, ECLI:EU:C:1988:352.
17 maggio 1990, causa C-262/88, *Barber*, ECLI:EU:C:1990:209.
8 novembre 1990, in causa C-177/88, *Dekker*, ECLI:EU:C:1990:383.
8 novembre 1990, causa C-179/88, *Handels- og Kontorfunktionærernes Forbund i Danmark c. Dansk Arbejdsgiverforening*. ECLI:EU:C:1990:384.
17 ottobre 1995, causa C-450/93, *Kalanke*, ECLI:EU:C:1995:322.
11 novembre 1997, causa C-409/95, *Marschall*, ECLI:EU:C:1997:533.
17 febbraio 1998, causa C-249/96, *Grant*, ECLI:EU:C:1998:63.
19 novembre 1998, causa C-66/96, *Høj Pedersen e a.,* ECLI:EU:C:1998:549.
26 ottobre 1999, causa C-273/97, *Sirdar*, ECLI:EU:C:1999:523.
26 febbraio 2008, causa C-506/06, *Mayr*, ECLI:EU:C:2008:119.
1° aprile 2008, causa C-267/06, *Maruko*, ECLI:EU:C:2008:179.
1° marzo 2011, causa C-236/09, *Test-Achats*, ECLI:EU:C:2011:100.
12 dicembre 2013, causa C-267/12, *Hay*, ECLI:EU:C:2013:823.
29 aprile 2015, causa C-528/13, *Léger*, ECLI:EU:C:2015:288.
9 marzo 2017, causa C-406/15, *Petya Milkova*, ECLI:EU:C:2017:198.
19 ottobre 2017, causa C-531/15, *Otero Ramos*, ECLI:EU:C:2017:789.
5 giugno 2018, causa C-673/16, *Coman*, ECLI:EU:C:2018:385.

Sentenze della Corte di europea dei diritti dell'uomo

7 novembre 2013, *Vallianatos e a. c. Grecia*, ECLI:CE:ECHR:2013:1107JUD002938109.
14 dicembre 2017, *Orlandi e a. c. Italia*, ECLI:CE:ECHR:2017:1214JUD002643112.
7 luglio 1989, *Gaskin c. Regno Unito*, n. 10454/83,
Godelli c. Italia, n. 33783/09, 25 settembre 2012
K.H. e a. c. Slovacchia, n. 32881/04, 28 aprile 2009
Leander c. Svezia, n. 9248/81, 26 marzo 1987

M.K. c. Francia, n. 19522/09, 18 aprile 2013
Odièvre c. Francia [GC], n. 42326/98, 13 febbraio 2003
Axel Springer AG c. Germania [GC], n. 39954/08, 7 febbraio 2012
Bohlen c. Germania, n. 53495/09, 19 febbraio 2015
Coudec e Hachette Filipacchi Associés c. Francia [GC], n. 40454/07, 10 novembre 2015
Magyar Helsinki Bizottság c. Ungheria [GC], n. 18030/11, 8 novembre 2016
Müller e a. c. Svizzera, n. 10737/84, 24 maggio 1988
Vereinigung bildender Künstler c. Austria, n. 68345/01, 25 gennaio 2007
Von Hannover c. Germania (n. 2) [GC], nn. 40660/08 e 60641/08, 7 febbraio 2012
Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia [GC], n. 931/13, 27 giugno 2017
Sinan Işık c. Turchia, n. 21924/05, 2 febbraio 2010
Haralambie c. Romania, n. 21737/03, 27 ottobre 2009 K.H. e a. c. Slovacchia, n. 32881/04, 28 aprile 2009
Segerstedt-Wiberg e a. c. Svezia, n. 62332/00, 6 giugno 2006
Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia [GC], n. 931/13, 27 giugno 2017

Finito di stampare nel mese di maggio 2023
presso Grafica Elettronica srl, Napoli

in copertina: *Il banditore del Comune* pubblicizza l'apertura della scuola di diritto.
Affresco di Giulio Rolland (1890), Aula Magna Palazzo dell'Università (sede storica), Macerata.

euro 16,00

ISBN 979-12-5976-642-7