GUERRA COGNITIVA E SICUREZZA NAZIONALE
Profili giuridici e istituzionali

a cura di
Roberto Sgalla
Alessandro Sterpa

EDITORIALE SCIENTIFICA

GUERRA COGNITIVA E SICUREZZA NAZIONALE

Profili giuridici e istituzionali

a cura di
ROBERTO SGALLA e ALESSANDRO STERPA

EDITORIALE SCIENTIFICA

Il presente volume è stato realizzato nell'ambito di una Convenzione per finalità di ricerca tra il Dipartimento di Economia, Ingegneria, Società e Impresa (DEIM) dell'Università della Tuscia e il Centro Studi Americani (CSA). In particolare, la spesa di stampa, ai sensi dell'art. 7 della Convenzione è stata sostenuta e rendicontata dal DEIM con il cofinanziamento del CSA.

I contributi del volume sono stati sottoposti a referaggio.

www.algofreedomsociety.it

Via San Biagio dei Librai, 39 – 80138 Napoli
www.editorialescientifica.it info@editorialescientifica.com

ISBN 979-12-235-0697-4

Indice

Prospettive operative

INTRODUZIONE

di *Roberto Sgalla* e *Alessandro Sterpa*

La dimensione delle minacce ibride costringe istituzioni e individui a operare in scenari inediti per la sicurezza nazionale. La guerra cognitiva, in particolare, tende a sottoporre gli ordinamenti giuridici delle democrazie liberali ad una minaccia del tutto nuova, impegnando il diritto e le scienze sociali nella identificazione di strumenti di azione e nella costruzione di regole di intervento che siano adeguati alle novità, ma sempre ancorati alla cornice delle previsioni costituzionali tese a tenere insieme libertà e sicurezza, diritti e doveri, dimensione di intervento pubblico e autodeterminazione soggettiva.

Per ragionare di questi profili, il 21 gennaio 2026, alla presenza di autorevoli esponenti delle istituzioni della Repubblica e dell'Accademia, si è tenuto un seminario presso il Centro Studi Americani in occasione della presentazione del volume di Alessandro Sterpa, *La difesa della democrazia dalle minacce ibride* (Napoli, Editoriale Scientifica, 2025). Durante l'incontro, intenso e partecipato, sono emerse molte riflessioni, alcune delle quali riportiamo in questo volume che nasce dalla proficua collaborazione tra il Centro Studi Americani e l'Università degli Studi della Tuscia, da tempo molto attiva sui temi della sicurezza, anche con il dottorato di ricerca in "Società in trasformazione: politiche, diritti e sicurezza".

Gli interventi presenti nel volume affrontano il tema da punti di vista diversi e complementari, confermando come questa nuova minaccia – a maggior ragione per la sua concretezza – meriti un adeguato approfondimento di studio, nell'ambito del più generale processo di trasformazione anche delle attività di *intelligence* che, come ricorda la dottrina più attenta, costringono ad abbattere i confini tra le tradizionali specializzazioni professionali e scientifiche. Oggi, infatti, l'innalzamento della qualità della minaccia induce le istituzioni a definire le proprie linee di azione e il diritto a misurarsi con una rivisitazione sia del concetto di guerra che di quello di sicurezza nazionale al fine di difendere, nel contesto aperto dei nuovi media e delle interdipendenze globali, i valori dei nostri sistemi giuridici costituzionali.

Un ringraziamento per la collaborazione editoriale a Anna Calabrese, Paolo Campagna, Claudia Capasso, Candida Conti e Victor Maximilian Hartl.

Il volume è dedicato alla memoria di Roberto Arditti, che molto si è occupato di sicurezza in questi anni, scomparso il 2 aprile scorso.

Roma, 9 maggio 2026

IL DOMINIO COGNITIVO E LA MINACCIA IBRIDA

Vittorio Rizzi[*]

1. *Introduzione*

Ogni epoca è attraversata da questioni che ne rivelano la fisionomia più profonda, oltre il rumore dell'immediato. Sono questioni che non sempre occupano stabilmente le prime pagine, ma che incidono in modo silenzioso e strutturale sull'evoluzione delle istituzioni e dei rapporti sociali. Non sono temi che si consumano nel ciclo della notizia, né si esauriscono nel confronto politico contingente; sono piuttosto categorie interpretative del tempo storico che viviamo. Aiutano a comprendere in quale direzione si stiano trasformando le nostre democrazie e quali fragilità stiano emergendo sotto la superficie dell'ordinario.

Il dominio cognitivo e la minaccia ibrida si collocano precisamente in questa prospettiva: non riguardano soltanto la trasformazione delle tecniche di conflitto o l'evoluzione delle tecnologie dell'informazione; intercettano, piuttosto, una dimensione più profonda e più decisiva: la tenuta stessa dei nostri ordinamenti democratici e, in ultima analisi, la sicurezza nazionale nel suo significato più pieno, maturo e moderno. Si tratta, dunque, di un tema che investe direttamente la qualità della nostra vita pubblica e la solidità delle istituzioni che la regolano.

Per un'istituzione pubblica, ciò significa riconoscere che la sicurezza non è più confinabile in un settore amministrativo o in un perimetro tecnico-operativo; si tratta di un campo integrato, nel quale strumenti

[*] Prefetto e Direttore del Dipartimento per le Informazioni per la Sicurezza (DIS) presso la Presidenza del Consiglio dei Ministri.

normativi, capacità tecnologiche, politiche educative e credibilità istituzionale concorrono a un unico obiettivo: preservare la continuità del patto democratico. In concreto, questo implica coordinamento stabile tra amministrazioni, condivisione di informazioni, capacità di dialogo con il settore privato e con il mondo accademico. In questa prospettiva, "dominio cognitivo" non è un'etichetta ma indica un ambito concreto di rischio e, insieme, di responsabilità pubblica. Non è uno slogan evocativo, ma la descrizione di uno spazio nel quale si giocano equilibri reali e misurabili. Siamo entrati in una fase storica nella quale la sicurezza non coincide più soltanto con la protezione del territorio o con la difesa delle infrastrutture fisiche. La sicurezza, oggi, è stabilità del patto sociale, credibilità delle istituzioni, fiducia collettiva che rende possibile la convivenza democratica. È anche capacità di mantenere coerenza e affidabilità nel tempo, evitando fratture che possano essere sfruttate da attori ostili. In altri termini, è la capacità di una comunità politica di orientarsi e decidere senza essere distorta dall'esterno. È la possibilità di esercitare la propria sovranità senza subire interferenze occulte nei processi decisionali.

La sicurezza diventa quindi anche capacità di governo dell'incertezza: prevenire non solo l'evento critico, ma l'erosione delle condizioni che rendono governabile una società complessa. Quando la fiducia si indebolisce, la reazione dello Stato alle crisi – qualunque sia la loro natura – diventa più lenta e più conflittuale. Le decisioni faticano a essere accettate e ogni intervento rischia di essere interpretato come arbitrario o sospetto.

Questo è il punto centrale, spesso sottovalutato: una democrazia non è soltanto un insieme di norme, procedure, elezioni, poteri e contrappesi. È anche – e soprattutto – un ecosistema di senso, un sistema condiviso di interpretazione della realtà che consente ai cittadini di orientarsi, comprendere, deliberare. È il terreno comune sul quale si costruisce il confronto pubblico e si accetta l'esito delle decisioni collettive, anche quando non coincidono con le preferenze individuali. Quando tale ecosistema si altera, quando la percezione comune del reale viene deformata, quando il confine tra vero, verosimile e falso si fa indistinto, la democrazia perde progressivamente la propria capacità di autodifesa. Non perché vengano meno formalmente le regole, ma perché si indebolisce la loro legittimazione sostanziale.

Questo spazio condiviso di significati funziona come un'infrastruttura invisibile: non si vede, ma sostiene l'intero edificio democratico. Se i cittadini non condividono più un linguaggio minimo del vero e del verificabile, la dialettica democratica scivola dalla critica alla delegittimazione, dal dissenso alla disgregazione. A quel punto la vulnerabilità diventa

istituzionale, non solo informativa, perché il problema non è più tanto la circolazione di contenuti fuorvianti quanto piuttosto la difficoltà di ricostruire un quadro comune di riferimento.

È in questo contesto che assume rilevanza strategica un concetto destinato a diventare centrale nel lessico della sicurezza contemporanea: il dominio cognitivo.

È il dominio in cui si formano le decisioni collettive prima ancora che siano atti: nelle percezioni che le precedono, nelle emozioni che le accompagnano, nelle narrazioni che le giustificano o le respingono. È lo spazio in cui maturano convinzioni e orientamenti che, solo successivamente, si traducono in scelte politiche o comportamenti sociali.

2. *La trasformazione dello scenario: la minaccia invisibile*

Viviamo un tempo in cui le minacce si manifestano con modalità sempre meno riconoscibili e sempre più elusive. Non assumono più necessariamente la forma di un attacco identificabile o di una dichiarazione ostile formalmente riconoscibile. Non si presentano più necessariamente sotto forma di aggressione frontale, di attacco dichiarato o di crisi improvvisa. Spesso operano in modo graduale, penetrando negli spazi della comunicazione, della cultura, della percezione. Si insinuano nel dibattito pubblico, sfruttano tensioni preesistenti, amplificano paure e divisioni che già attraversano la società.

Questa caratteristica pone un problema tipicamente istituzionale: la minaccia invisibile non attiva automaticamente i dispositivi tradizionali di risposta, perché non produce un "evento" univoco e riconoscibile. Non vi è un momento preciso in cui sia possibile affermare che un attacco sia iniziato, né un confine netto che consenta di separare l'ordinario dallo straordinario. Ne deriva che la prevenzione deve dotarsi di strumenti di lettura anticipata: analisi dei segnali deboli, monitoraggio delle campagne coordinate, capacità di attribuzione, cooperazione interistituzionale.

Non è cambiata soltanto la natura delle minacce ma è cambiato il loro obiettivo: non si mira solo a interrompere funzioni, ma a indebolire la fiducia; non solo a colpire lo Stato dall'esterno, ma a renderlo fragile dall'interno; l'attenzione si sposta dal danno immediato al deterioramento progressivo del clima pubblico e della coesione sociale.

La sicurezza, quindi, non si misura più esclusivamente nella capacità di prevenire eventi visibili o di reagire a crisi manifeste. Si misura nella

facoltà di preservare ciò che rende possibile ogni altra forma di sicurezza: la capacità di una comunità politica di pensare, decidere e scegliere liberamente.

Qui la dimensione pubblica è decisiva: la libertà di scelta collettiva dipende dalla qualità dell'ambiente informativo e dalla credibilità delle istituzioni nel renderlo leggibile, trasparente, verificabile perché se l'informazione è opaca o sistematicamente manipolata, anche le scelte formalmente libere rischiano di essere, di fatto, condizionate.

Quando una società perde la capacità di distinguere ciò che è vero da ciò che è plausibile, e ciò che è plausibile da ciò che è artificiosamente costruito, essa diventa vulnerabile non tanto sul piano materiale quanto su quello più decisivo: la coesione interna. Una società disorientata è una società indebolita. Una società polarizzata è una società più fragile. Una società che dubita sistematicamente delle proprie istituzioni è una società esposta.

La coesione interna è una risorsa strategica: non si improvvisa nel momento della crisi, si costruisce nella normalità, attraverso continuità amministrativa, qualità dei servizi, affidabilità comunicativa e capacità di risposta. Quando la coesione si rompe, lo Stato resta formalmente integro, ma perde "presa" sulla realtà sociale: e questo è l'esito più ricercato dalle dinamiche ibride.

La minaccia contemporanea lavora sul tempo lungo: il suo successo si misura nella stanchezza democratica, nel cinismo, nella delegittimazione progressiva dell'autorità pubblica e nella perdita di fiducia nella possibilità stessa di una verità comune.

3. *La moltiplicazione dei domini e la logica del* deep blue

L'innovazione tecnologica ha prodotto una trasformazione di natura quasi antropologica, proiettandoci in uno spazio operativo sempre più multidimensionale e interconnesso. Le nostre attività quotidiane – comunicare, lavorare, informarci, spostarci – dipendono ormai da reti e infrastrutture che attraversano più domini contemporaneamente. Ai tradizionali terra, mare e cielo si sono affiancati lo spazio extra-atmosferico, il dominio cibernetico e, in misura crescente, quello sottomarino. Ambiti distinti, ma ormai intimamente interdipendenti.

Per la sicurezza nazionale ciò significa che la protezione non può essere pensata per "*silos*": la vulnerabilità di un dominio diventa vulnerabilità dell'intero sistema. Un'interruzione in ambito cibernetico può

avere ricadute su trasporti, energia, finanza e comunicazioni nel giro di poche ore e poiché le infrastrutture critiche sono sempre più digitalizzate e interconnesse, la continuità dei servizi essenziali dipende da una governance multilivello e da un coordinamento costante tra attori pubblici e privati. Nessun soggetto, da solo, è in grado di presidiare l'intera catena delle dipendenze.

Questa interdipendenza viene spesso descritta attraverso l'immagine suggestiva del *deep blue*: l'intreccio tra il blu profondo dello spazio e quello degli oceani. È una metafora potente perché restituisce la percezione di una profondità strategica che non è più confinabile. La profondità strategica non coincide più con la distanza geografica, ma con la stratificazione delle dipendenze: dati, energia, connettività, navigazione satellitare, catene logistiche. È una profondità fatta di livelli sovrapposti e reciprocamente condizionanti.

Il cielo non è soltanto atmosfera: è un sistema di piattaforme satellitari che regola comunicazioni, navigazione, osservazione. Il mare non è soltanto dimensione geopolitica tradizionale: ospita infrastrutture invisibili e decisive – cavi sottomarini, reti energetiche, collegamenti strategici – che sorreggono la vita digitale delle nazioni. Il cyberspazio non è un altrove immateriale: è il tessuto connettivo dell'intero sistema, l'ambiente in cui transitano dati, comunicazioni, decisioni.

Ne consegue che un'azione condotta in un singolo dominio può produrre effetti sistemici negli altri, rendendo la sicurezza più fragile e più complessa da governare. Questa consapevolezza però, pur se fondamentale, non è ancora sufficiente. Per comprendere pienamente la minaccia contemporanea occorre compiere un ulteriore salto concettuale.

4. Il dominio decisivo: lo spazio cognitivo

Accanto ai domini materiali e tecnologici esiste uno spazio immateriale ma decisivo, nel quale gli effetti dell'interconnessione si concentrano e si amplificano: il dominio cognitivo, uno spazio che non ha confini geografici, ma che produce conseguenze molto concrete nella vita politica e istituzionale.

È il punto di convergenza tra tecnologia, comunicazione e psicologia sociale: dove una perturbazione informativa può trasformarsi in polarizzazione, e la polarizzazione in vulnerabilità istituzionale. Un contenuto distorsivo, se reiterato e amplificato, può modificare percezioni diffuse e incidere sul clima complessivo del dibattito pubblico.

Il dominio che oggi incide in modo più diretto sulla sicurezza nazionale non è soltanto quello delle infrastrutture. È quello in cui si formano le decisioni, si orientano le scelte, si costruisce – o si erode – la fiducia collettiva. Nel dominio cognitivo non si colpiscono soltanto reti o impianti ma le percezioni, le emozioni e le convinzioni, andando a incidere sul rapporto tra cittadino e istituzioni. Si interviene sulla rappresentazione della realtà, influenzando il modo in cui eventi e decisioni vengono interpretati.

Per questo la difesa del dominio cognitivo non può essere affidata a un solo attore: richiede cooperazione tra intelligence, forze di polizia, autorità di regolazione, sistema educativo, informazione responsabile e piattaforme digitali.

È una dimensione più delicata e più strategica perché tocca ciò che rende possibile la democrazia: la libertà di giudizio. Senza libertà di giudizio non vi è partecipazione consapevole; senza partecipazione consapevole non vi è democrazia sostanziale.

Il più grande spazio di libertà dell'essere umano è la libertà di pensiero. Ed è precisamente questo spazio a risultare oggi particolarmente esposto e vulnerabile. Le operazioni nel dominio cognitivo non mirano soltanto a diffondere notizie false. Mirano a disarticolare la fiducia, a creare una percezione di caos, a costruire un clima permanente di sospetto.

L'obiettivo finale non è la vittoria immediata, ma la stanchezza democratica. Non è il crollo improvviso, ma l'erosione graduale della fiducia. Una società in cui tutto è sospetto è una società più governabile dall'esterno, perché più difficilmente capace di reagire in modo unitario.

Quando ogni affermazione appare contestabile, quando ogni fonte appare sospetta, quando ogni fatto viene immediatamente relativizzato, la deliberazione si paralizza. E una democrazia paralizzata è una democrazia vulnerabile.

Oggi, infatti, manipolazione, disinformazione, ibridazione deliberata tra vero, verosimile e falso non sono più fenomeni episodici. Sono diventati strumenti sistemici di influenza strategica.

L'informazione non è più soltanto un mezzo: è diventata un ambiente. Un ecosistema di potere nel quale si modellano percezioni, emozioni e comportamenti collettivi.

La disinformazione contemporanea non è grossolana, ma raffinata, scientificamente costruita, calibrata per segmenti sociali differenti, adattata a *bias* cognitivi specifici, progettata per produrre reazioni emotive prevedibili. Non si limita ad affermare il falso; costruisce narrazioni alter-

native plausibili, ripetute, amplificate, inserite in un flusso informativo in cui si fatica a distinguere l'autentico dall'artificiale.

In definitiva oggi la libertà formale di informarsi rischia di trasformarsi in una libertà apparente. Un cittadino sommerso da informazioni contraddittorie, iperstimolato, polarizzato, è meno libero.

In questo scenario, la funzione dello Stato non può limitarsi alla repressione delle condotte illecite, ma deve estendersi alla costruzione di resilienza, alla promozione di alfabetizzazione mediatica, al rafforzamento degli anticorpi culturali.

5. Onlife *e guerra ibrida: il nuovo teatro del conflitto permanente*

Viviamo in quella condizione che il filosofo Luciano Floridi ha definito *onlife*: una dimensione esistenziale nella quale il confine tra *online* e *offline* si dissolve. Questo dato non è semplicemente sociologico: è strategico. Se la vita sociale è "ibridata" con la dimensione digitale, anche la vulnerabilità sociale lo è. Le dinamiche digitali non restano confinate nello spazio virtuale, ma producono effetti tangibili nelle relazioni e nelle scelte collettive.

Il digitale non è più un ambiente separato: è l'ambiente nel quale si svolge una parte crescente dell'esperienza umana. Le opinioni si formano attraverso piattaforme, le emozioni si diffondono attraverso reti, le identità si costruiscono tramite dinamiche di riconoscimento digitale. La reputazione pubblica può essere influenzata in tempi rapidissimi, con effetti difficilmente reversibili.

Nell'era degli *zettabyte*, il 90 per cento delle informazioni disponibili è stato generato negli ultimi due anni. Questo dato è strategico. L'umanità produce più informazione di quanta sia in grado di metabolizzare. È proprio in questo eccesso che la minaccia trova spazio. La quantità rende più complessa la verifica e favorisce la circolazione di contenuti manipolativi.

L'eccesso informativo crea saturazione, stanchezza cognitiva e abbassamento delle soglie critiche: condizioni ideali per l'amplificazione di contenuti manipolativi e per la polarizzazione. Incidere sulla percezione della realtà può risultare più efficace che colpire un'infrastruttura fisica, perché altera il terreno sul quale si fondano il consenso democratico, la coesione sociale e la legittimazione delle istituzioni.

La minaccia ibrida combina strumenti diversi: cyberattacchi, pressione economica, propaganda, infiltrazioni informative, destabilizzazio-

ne sociale, sfruttamento delle fratture interne. Agisce sotto la soglia del conflitto aperto, in una zona grigia che non supera linee rosse evidenti e non produce un evento bellico riconoscibile, ma genera effetti di lungo periodo.

Non mira soltanto a far credere qualcosa: mira a far dubitare di tutto. Non punta a convincere, ma a paralizzare la capacità di giudizio e la paralisi del giudizio è il risultato più pericoloso: una comunità che non sa più a cosa credere fatica a decidere e una democrazia che fatica a decidere è più vulnerabile a qualunque forma di pressione.

La guerra cognitiva è la forma strutturale di questo conflitto. Per utilizzare un'espressione del Prof. Alessandro Sterpa, quella attuale è una «*guerra tiepida*»: non abbastanza calda da generare scontri armati, non abbastanza fredda da garantire regole condivise. Una guerra permanente, diffusa, quotidiana, che non cerca il collasso immediato, ma l'indebolimento graduale del tessuto democratico.

In tale scenario, la sicurezza diventa tenuta psicologica, culturale e valoriale della comunità nazionale. Difendere la democrazia non significa soltanto proteggere lo Stato. Significa proteggere la mente collettiva che rende lo Stato possibile.

6. *Intelligenza artificiale e sovranità cognitiva: il primato della decisione umana*

In questa cornice emerge con forza un concetto decisivo: la sovranità cognitiva. Senza sovranità cognitiva non esiste sicurezza nazionale. Senza la possibilità di formare opinioni libere, ogni altra forma di sovranità rischia di essere svuotata dall'interno.

Sovranità cognitiva significa garantire tre condizioni fondamentali: che i cittadini possano formarsi un'opinione libera da condizionamenti sistemici; che il dibattito pubblico non sia ostaggio di campagne manipolative; che la pluralità delle idee non degeneri in caos informativo.

In ultima analisi, sovranità cognitiva significa difendere il libero arbitrio come infrastruttura critica della democrazia moderna. La libertà non è soltanto un diritto giuridico: è una condizione culturale. Richiede consapevolezza, capacità critica, strumenti cognitivi adeguati a interpretare un ambiente informativo sempre più complesso.

L'intelligenza artificiale rappresenta una sfida ambivalente. Da un lato è uno strumento indispensabile per la difesa (analisi della complessità, individuazione di segnali deboli, riconoscimento di schemi ricor-

renti), dall'altro potenzia le capacità offensive di attori ostili. Infatti, l'IA consente di generare testi, immagini, video, audio credibili, di simulare persone, eventi, dichiarazioni e financo di creare una realtà alternativa perfettamente plausibile. Nell'era dell'IA non è più necessario convincere milioni di persone con un unico messaggio: è possibile convincere migliaia di micro-comunità con messaggi differenti, calibrati sulle loro paure, sulle loro convinzioni, sulle loro frustrazioni.

Tuttavia, l'IA non possiede coscienza. È un mezzo di calcolo potentissimo, non un soggetto morale. La differenza tra uomo e macchina risiede nella coscienza, nella creatività, nella libertà di scelta. Delegare il giudizio alle macchine significherebbe rinunciare a ciò che intendiamo difendere.

In termini istituzionali, ciò significa affermare un principio di responsabilità: l'algoritmo può assistere, ma non può sostituire. La catena decisionale deve restare umana, controllabile, imputabile.

La lezione di Stanislav Petrov, l'ufficiale sovietico che nel 1983 ricevette un segnale che indicava un imminente attacco missilistico e scelse di non affidarsi ciecamente a un sistema automatico scongiurando una potenziale catastrofe nucleare, ci ricorda che la sicurezza, nei momenti decisivi, passa dall'uomo. La difesa del dominio cognitivo implica anche la preservazione della capacità umana di discernere. È una lezione che vale oggi in modo particolare: quando le tecnologie accelerano, il compito delle istituzioni è preservare la lucidità del giudizio e la responsabilità della scelta.

7. Sovranità digitale, scudo democratico e responsabilità civica

Da quanto precede discende una conclusione che non ammette ambiguità: la sovranità cognitiva non rappresenta un'opzione tra le altre, ma la condizione strutturale della sicurezza nel XXI secolo. La sovranità digitale, con le sue infrastrutture, le sue architetture di rete, le sue capacità computazionali, costituisce un presupposto indispensabile; tuttavia, essa rimane insufficiente se non è orientata e sorretta da una piena sovranità cognitiva.

La sicurezza digitale protegge le reti; la sovranità cognitiva protegge ciò che passa attraverso le reti: fiducia, orientamento, capacità deliberativa.

Possiamo rafforzare la cybersicurezza, proteggere i dati strategici, sviluppare piattaforme autonome, investire in intelligenza artificiale e in tecnologie critiche. Ma se non presidiamo i processi attraverso cui si

formano opinioni, percezioni e decisioni collettive; se non difendiamo lo spazio pubblico della deliberazione; se non coltiviamo una cultura democratica capace di resistere alla manipolazione, rischiamo di edificare una fortezza tecnologica dalle mura solide e dalle fondamenta fragili.

La vulnerabilità più insidiosa non riguarda i sistemi, bensì le coscienze. È per questo che la questione cognitiva è ormai entrata stabilmente nelle politiche pubbliche: l'inclusione della disinformazione tra le minacce di primo livello alla sicurezza nazionale nel Regno Unito, insieme alla proposta di un'Agenzia dedicata alla resilienza cognitiva, segna un cambio di paradigma definitivo.

La disinformazione non è più un problema mediatico; è una questione di sicurezza. Analogamente, lo *European Democracy Shield* presentato dalla Commissione Europea il 12 novembre 2025 si propone di rafforzare la tenuta democratica dell'Unione nello spazio informativo e cognitivo attraverso un approccio integrato che combina tutela dello spazio informativo, protezione dei processi elettorali e promozione dell'alfabetizzazione mediatica e civica. Il principio che sorregge tali iniziative è chiaro: la democrazia, per essere difesa, deve essere protetta nella sua dimensione cognitiva. In altre parole: la risposta deve essere europea perché la minaccia è transnazionale; deve essere multilivello perché la vulnerabilità è sistemica.

Nessun Paese può affrontare da solo un ecosistema informativo globale.

In questa prospettiva, la sovranità cognitiva non può essere delegata esclusivamente agli apparati statali o alle architetture normative: essa richiede una responsabilità diffusa, una cittadinanza consapevole, una vera e propria militanza cognitiva nel senso più alto e civile del termine. Il cittadino del nostro tempo non è più soltanto destinatario di decisioni pubbliche, ma parte integrante dell'ecosistema di sicurezza democratica. Reagire alla guerra cognitiva significa assumere un'etica dell'informazione: esercitare prudenza nella condivisione dei contenuti, sottrarsi alla seduzione della semplificazione aggressiva, difendere la complessità contro la polarizzazione, custodire il pluralismo senza scivolare nel relativismo paralizzante.

Difendere la democrazia oggi significa, in ultima analisi, difendere la mente collettiva che la rende possibile. La sicurezza nazionale coincide sempre più con la capacità di pensare, distinguere, giudicare; con la forza degli anticorpi culturali che impediscono alla sfiducia di trasformarsi in paralisi. Il dominio cognitivo è lo spazio silenzioso nel quale si decide la qualità della nostra libertà. E sarà dalla maturità della nostra coscienza

civica – più ancora che dalla sofisticazione delle nostre tecnologie – che dipenderà la tenuta delle democrazie liberali.

Questa è la sfida del nostro tempo; questa è, oggi, la forma più alta della difesa democratica. Ed è una sfida che chiama in causa tutte le istituzioni: non solo quelle deputate alla sicurezza in senso stretto, ma l'intero sistema pubblico, perché la resilienza cognitiva è una funzione generale dello Stato democratico.

MINACCIA IBRIDA E OFFENSIVITÀ MULTIDOMINIO: LA CYBERSICUREZZA A TUTELA DELLA DEMOCRAZIA

Bruno Frattasi[*]

1. *Minaccia ibrida e offensività multidominio*

La difesa della pace, della libertà e della sicurezza nazionale e internazionale diventano una priorità strategica anche dinanzi al diffondersi di meccanismi di offesa estranei alle categorie belliche tradizionali.

Si pensi, a tal proposito, alla c.d. guerra ibrida[1], una forma di conflitto moderna e complessa che sfuma i confini tradizionali della guerra, utilizzando armi non convenzionali per raggiungere obiettivi strategici, spesso evitando lo scontro militare diretto su larga scala. L'obiettivo, infatti, è quello di destabilizzare, indebolire, influenzare o coercere l'avversario senza necessariamente superare la soglia che scatenerebbe una risposta militare convenzionale, operando, dunque, nella cosiddetta «zona grigia». Spesso le azioni sono condotte in modo da rendere difficile l'attribuzione chiara a uno Stato specifico, mantenendo una negabilità plausibile.

Si opera deliberatamente per confondere le linee tra guerra e pace, tra combattenti e civili, tra attori statali e non statali. Si tratta, quindi, di una strategia che combina diversi tipi di strumenti e tattiche – convenzionali, cibernetiche, informative, economiche e politiche – in modo coordinato e sincronizzato per raggiungere obiettivi strategici. Inoltre, i più recenti sviluppi denotano come l'evoluzione del conflitto è costantemente aggiornata dall'utilizzo sul campo di nuove tecnologie, ad esempio droni e altre apparecchiature robotiche, in grado spesso di condizionare anche

[*] Prefetto e Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale (ACN).

[1] FONDAZIONE LUIGI EINAUDI (a cura di), *Difesa: l'industria necessaria*, 2025.

il corso degli eventi, riducendo, se non azzerando del tutto, l'esposizione umana. Tale modalità di conflitto invisibile, sottosoglia ma comunque letale, comporta l'imprescindibile necessità di proteggere la popolazione e gli asset critici, civili e militari, anche da attacchi intangibili, quali sono quelli *cyber*.

La conflittualità, dunque, si è spostata dal vecchio campo di battaglia alla dimensione cibernetica, alle *covert actions*, alle *false flag operations*, alla guerra dell'informazione e della disinformazione, alla guerra economica, alla lotta per la supremazia nello spazio e nel cyberspazio.

2. *La partecipazione di ACN a Gruppi di lavoro europei volti a contrastare la minaccia ibrida*

L'Agenzia per la Cybersicurezza Nazionale (ACN) contribuisce attivamente a diverse iniziative dell'UE volte al contrasto della minaccia ibrida.

Tra i pericoli principali figurano le interferenze informatiche ai processi elettorali. In proposito, l'ACN partecipa al Gruppo di Cooperazione NIS, ove è stato istituito un Gruppo di Lavoro dedicato, denominato *Work Stream on elections cybersecurity*, che esplora le implicazioni per la cybersicurezza delle tecnologie utilizzate nel contesto elettorale, in particolare considerando la minaccia ibrida.

Sempre a livello europeo, l'ACN assicura il proprio contributo, per i profili di competenza, in supporto al delegato della Rappresentanza permanente d'Italia presso l'UE, al Gruppo di Lavoro per il contrasto per le minacce ibride (*Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats*, HWP ERCHT). Il Gruppo persegue l'obiettivo di agire in modo proattivo contro le minacce derivanti dalla guerra ibrida e di potenziare la resilienza degli Stati membri e della società civile europea, accrescendone la capacità di prevenire, assorbire e rispondere efficacemente agli attacchi. Attraverso un approccio coordinato e trasversale, l'HWP ERCHT assicura coerenza tra le iniziative europee e promuove una risposta integrata e strategica alle minacce ibride.

In tale contesto, si evidenzia, inoltre, l'iniziativa europea *EU Hybrid Toolbox* (EUHT), concepita come un insieme integrato di strumenti civili e militari da impiegare nella risposta a minacce ibride, qualora uno Stato decidesse di invocare l'assistenza dell'UE. L'obiettivo del *toolbox* è garantire una reazione tempestiva e coordinata, permettendo l'adozione di contromisure proporzionate, soprattutto nel caso in cui l'attacco rap-

presenti un illecito internazionale. L'*Hybrid Toolbox* si affianca e integra il *Cyber Diplomacy Toolbox*, ampliando significativamente il ventaglio delle risposte diplomatiche, civili e militari, e rafforzando la resilienza europea di fronte a minacce ibride e cibernetiche sempre più sofisticate e interconnesse.

Lo sforzo dell'UE per contrastare le suddette minacce si sviluppa anche attraverso strumenti di *policy*. In particolare, il 12 novembre 2025 la Commissione europea ha presentato il c.d. Scudo europeo per la Democrazia. Tale strumento adotta un approccio integrato e olistico alla sicurezza, considerando fondamentale la resilienza cibernetica delle istituzioni democratiche, la protezione delle infrastrutture digitali e la difesa contro la disinformazione e gli attacchi informatici. Il rafforzamento della democrazia, dunque, non è solo un obiettivo politico, ma costituisce un presupposto imprescindibile per il consolidamento della sicurezza collettiva nell'era digitale. È questa la traiettoria segnata anche da recenti provvedimenti europei come il *Cyber Solidarity Act.*

3. Cyber Solidarity Act*: verso una politica di difesa comune*

Le attuali tensioni geopolitiche hanno determinato lo spostamento del baricentro europeo dalla tutela del mercato alla difesa comune unionale.

Ci troviamo di fronte a un fatto trasformativo di grandissima rilevanza che segna un'evoluzione degli stessi obiettivi di riferimento che l'Europa ha seguito quando ha scelto di porre al centro della disciplina della digitalizzazione gli interessi del consumatore, affinché il mercato potesse offrire a tutti i consumatori europei, ovunque fossero, la possibilità di utilizzare prodotti digitali performanti e a basso prezzo.

Oggi, però, siamo chiamati a tutelare un ventaglio di esigenze più ampio, che ha determinato lo spostamento del baricentro degli interessi unionali. Si assiste a un'ibridazione tra il mercato unico fondato su un principio sovranazionale e il profilo della difesa, che è un tema securitario nazionale, intergovernativo, dove non c'è mai stata una sovrapposizione dell'Europa rispetto alla dimensione nazionale. Tuttavia, questi due grandi filoni si stanno pian piano avvicinando e incrociando.

I crescenti rischi di cybersicurezza e un panorama di minacce globalmente complesso, con il chiaro pericolo di rapida propagazione di incidenti da uno Stato membro all'altro e da un Paese terzo all'Unione, richiedono il rafforzamento della solidarietà digitale per migliorare il ri-

levamento delle minacce e degli incidenti informatici, nonché la preparazione e la risposta agli stessi.

È questa la *ratio* del *Cyber Solidarity Act*, volto a rendere l'Europa più resiliente e reattiva di fronte alle minacce informatiche, rafforzando al contempo il meccanismo di cooperazione esistente.

Il Regolamento introduce il c.d. scudo europeo per la cybersicurezza. Si tratta di un sistema europeo di allerta per la cybersicurezza composto da centri operativi di sicurezza (SOC) nazionali e transfrontalieri in tutta l'UE, che utilizzeranno tecnologie avanzate come l'intelligenza artificiale (IA) e l'analisi dei dati per rilevare e condividere avvisi sulle minacce. Il Regolamento rappresenta un passaggio strategico nella costruzione di una difesa cibernetica comune poiché introduce strumenti innovativi volti a garantire un alto livello di sicurezza e reattività nell'intero spazio digitale europeo.

4. Emerging Disruptive Technologies*: opportunità e rischi*

Il contesto di accelerazione tecnologica nel quale ci troviamo richiede, inoltre, una costante attività di aggiornamento delle *policies* di cybersicurezza al fine di garantire che la superficie digitale nazionale, sempre più in rapida espansione, sia difesa adeguatamente e in modo proporzionale al crescere delle capacità offensive degli attaccanti. Lo sviluppo di sistemi di IA sempre più sofisticati, insieme alle nuove capacità esponenziali di calcolo offerte dalla tecnologia quantistica, da un lato consentono di prevenire e contrastare la minaccia cibernetica, mitigandone i rischi e favorendo lo sviluppo di controlli, strumenti di analisi e metodologie di test condivisi; dall'altro, tuttavia, amplificano la portata offensiva degli attacchi cibernetici, che ormai sono in grado di provocare danni gravi alle infrastrutture critiche del Paese.

Occorre, dunque, che l'IA e la tecnologia quantistica e post-quantistica trovino concreta applicazione in una molteplicità di casi d'uso e in settori strategici per lo sviluppo del Paese, come la sanità, il lavoro, la giustizia, le pubbliche amministrazioni e altre importanti aree nelle quali bisogna garantire un utilizzo delle tecnologie emergenti basato su criteri improntati a una corretta gestione dei rischi connessi.

Gli strumenti tecnologici consentono, ormai, di compiere attacchi informatici senza richiedere specifiche competenze in capo agli attaccanti e, allo stesso tempo, rischiano di accrescere il livello di pericolosità degli attori esperti. Ci sono *ransomware* che generano il proprio codice male-

volo in tempo reale sfruttando l'IA; modi per introdursi nei software di navigazione *online* senza che gli utenti se ne accorgano; tecniche di ingegneria sociale che riescono a manipolare le persone, come il *vibe-hacking*. Anche il vecchio *phishing* con l'IA si evolve e diventa più personalizzato, dal momento che quest'ultima consente ai cybercriminali di creare *e-mail*, messaggi e siti estremamente convincenti, in grado di simulare fonti legittime ed eliminare gli errori grammaticali che un tempo smascheravano le truffe[2].

Particolare preoccupazione suscita la diffusione dei cd. *deepfake*, ossia immagini, video o voci falsificate mediante sistemi di IA, in modo tanto realistico da potere indurre in inganno sulla non veridicità delle medesime. Sul punto, il legislatore nazionale è intervenuto[3] introducendo una nuova fattispecie di reato all'interno del Codice penale, all'art. 612 *quater* ("Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale"), al fine di reprimere questa insidiosa pratica.

La diffusione dei modelli di IA richiede, quindi, un ripensamento fondamentale delle strategie di sicurezza informatica. Le Pubbliche Amministrazioni e le aziende devono prepararsi non solo a implementare queste nuove tecnologie per migliorare le proprie difese, ma anche a difendersi da minacce completamente nuove che sfruttano le stesse innovazioni.

In questo senso, quei soggetti che iniziano oggi la preparazione attraverso la pianificazione strategica, lo sviluppo delle competenze e le implementazioni pilota saranno meglio posizionati per sfruttare queste tecnologie, mitigando contemporaneamente i rischi.

Il successo dipenderà dalla capacità di creare *partnership human-AI* potenti, che combinano il meglio dell'intelligenza biologica e artificiale[4]. Il binomio IA e cybersicurezza non rappresenta più, dunque, un ambito settoriale o meramente tecnico, ma è divenuto un vero e proprio snodo costituzionale dell'era contemporanea, la cui evoluzione incide sui delicati equilibri geopolitici del nostro tempo e sul godimento dei diritti fondamentali.

È stato rilevato come la sovranità tecnologica non possa più prescindere dalla disponibilità di infrastrutture di calcolo avanzate, necessarie per elaborare grandi volumi di dati, sostenere analisi complesse e operare

[2] T. Santamato, *L'IA cambia la cybersicurezza*, in *La Sicilia*, 1 settembre 2025.

[3] V. art. 26, legge del 26 settembre 2025 n. 132.

[4] *Come l'IA neuromorfica e i modelli fondazionali stanno ridefinendo il panorama delle minacce alla cybersecurity*, in *ICT Security Magazine*, 18 settembre 2025.

efficacemente nel dominio digitale e cognitivo. Nel dotarsi di capacità computazionali incrementali è necessario però fare sistema, non disperdendo gli importanti risultati già raggiunti e che hanno portato l'Italia a essere tra i primi 4 Paesi al mondo per potenza di calcolo installata. Basti pensare, a questo proposito, al supercomputer Leonardo, ospitato presso il Tecnopolo di Bologna e gestito dal consorzio CINECA, uno dei supercalcolatori più potenti al mondo e tra i principali in Europa, fondamentale per la ricerca scientifica e l'intelligenza artificiale.

Sono queste le finalità che lo scorso 27 giugno, a Napoli, presso la sede del CINECA a San Giovanni a Teduccio, hanno consentito di inaugurare il *data center* Megaride, un sistema di calcolo ad alte prestazioni (HPC) che nasce da un'iniziativa dell'Agenzia per la cybersicurezza nazionale (ACN) e del Ministero dell'Università e della Ricerca (MUR), con il supporto di ICSC (Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing), del Consiglio Nazionale delle Ricerche (CNR) e del CINECA, che ospita e gestisce il *data center*. Obiettivo del nuovo sistema HPC, interconnesso con il supercalcolatore Leonardo, è supportare la ricerca scientifica, le imprese e le *startup*, e rispondere alle esigenze dell'ecosistema della cybersicurezza nazionale attraverso lo sviluppo di soluzioni avanzate di IA.

5. Tra minaccia ibrida e guerra cognitiva

La guerra cognitiva può essere definita come un'operazione multidominio che impiega mezzi, azioni e strumenti attraverso le connessioni esistenti tra i domini (terrestre, marittimo, aereo, spaziale e *cyber*) e l'ambiente informativo per generare effetti nella dimensione cognitiva e influenzare il comportamento umano per ottenere un vantaggio sull'avversario.

In questa direzione si inserisce il volume del Prof. Alessandro Sterpa[5]. L'Autore parte dall'idea che le democrazie liberali europee non siano, oggi, minacciate soltanto da conflitti armati tradizionali, ma da una forma più sottile – e per questo più insidiosa – di conflitto, che il Prof. Sterpa qualifica come guerra ibrida e, in particolare, guerra cognitiva[6].

[5] A. STERPA, *La difesa della democrazia dalle minacce ibride*, Editoriale Scientifica, Napoli, 2025.

[6] L'Autore spiega che guerra ibrida e guerra cognitiva costituiscono una metonimia nella misura in cui la guerra cognitiva è un sottogruppo della guerra ibrida.

Una guerra che non mira a conquistare territori, ma a condizionare le menti e a indebolire dall'interno la fiducia dei cittadini nelle istituzioni democratiche.

Il Prof. Sterpa definisce questo scenario come una «guerra tiepida», cioè non abbastanza calda per generare conflitti armati e non abbastanza fredda per garantire la convivenza dei due modelli. In questo contesto, il ruolo delle tecnologie digitali e degli algoritmi è decisivo. La comunicazione *cyber*, se utilizzata per fini malevoli, può amplificare contenuti emotivamente forti e spesso falsi, riducendo la capacità critica degli individui e trasformando la sicurezza in una questione di percezione soggettiva, con l'effetto di rendere la paura un fattore capace di orientare i comportamenti. La disinformazione, infatti, erode la fiducia nelle istituzioni e nei mezzi di comunicazione digitali e tradizionali e danneggia le nostre democrazie, ostacolando la capacità dei cittadini di prendere decisioni informate[7].

Per questo motivo, la risposta alla guerra cognitiva deve essere parte di una strategia profonda che valorizzi il ruolo dell'individuo consapevole attraverso quella che Sterpa chiama «militanza cognitiva», cioè la capacità dei cittadini di esercitare spirito critico, difendere il pluralismo informativo e partecipare attivamente alla tutela dei valori democratici. Ciò è possibile contribuendo, innanzitutto, alla formazione e alla diffusione di una cultura della cybersicurezza.

[7] A. Sterpa, *La difesa della democrazia dalle minacce ibride*, cit., p. 59, nota 33.

LA COSTITUZIONE E LA "NUOVA GUERRA": STATO E INDIVIDUO NELLA GUERRA COGNITIVA*

*Alessandro Sterpa***

SOMMARIO: 1. La guerra cognitiva tra "guerra" e sicurezza nazionale. – 2. L'individuo nel "sesto dominio": come difendere la forma di stato. – 2.1. La "militanza cognitiva" come politica di sicurezza. – 3. Considerazioni conclusive.

1. *La guerra cognitiva tra "guerra" e sicurezza nazionale*

La Costituzione contempla l'ipotesi che la Repubblica possa essere impegnata in una guerra, tanto da prevedere la deliberazione dello stato di guerra da parte del Parlamento con l'eventuale conferimento dei «necessari» (quindi non predeterminati dalla Carta) poteri al Governo (art. 78)[1] e la sua proclamazione da parte del Presidente della Repubblica (art. 87)[2]. La guerra, nonostante alcune infondate letture ideologiche del testo della Carta, è parte integrante delle dinamiche istituzionali anche se, come è evidente, è ivi intesa come guerra per difendersi e non per attaccare unilateralmente qualcun altro senza alcuna ragione; in questo senso milita non solo il noto (spesso travisato)[3]

* Il saggio riprende le riflessioni svolte nell'ambito della tavola rotonda tenutasi presso il Centro Studi Americani il 21 gennaio 2026 e pubblicate in *federalismi.it*, n. 14/2026, pp. 229-246.

** Professore in Diritto costituzionale e pubblico nell'Università degli Studi della Tuscia.

[1] Sul "conferire" come "delegare", G. FERRARI, *Guerra (stato di)*, in *Enc. Dir.*, Giuffrè, Milano, 1970, p. 845; cfr. anche A. GIARDINA, *Art. 78*, in G. BRANCA (a cura di), *Commentario della Costituzione*, Zanichelli-Foro it., Bologna-Roma, 1979, pp. 103 e ss..

[2] Sul rapporto giuridico tra deliberazione delle Camere e atto del Presidente della Repubblica, G. FERRARI, *Guerra (stato di)*, cit., pp. 842-843.

[3] Di "pace come valore primario ma non assoluto" argomenta G. DE VERGOTTINI, *Guerra e costituzione. Nuovi conflitti e sfide alla democrazia*, il Mulino, Bologna, 2004, pp. 95-103; di eclissi del dettato costituzionale, partendo dall'idea che la disposizione costituzionale introduca il "principio pacifista"; C. DE FIORES parla di una dottrina rassegnata "di fronte a questo strisciante tentativo di rimozione del fondamento pacifista della nostra Costituzione" *("L'Italia ripudia la guerra"? La Costituzione di fronte al nuovo ordine globale*, Ediesse, Roma, 2002, p. 27). Come vedremo, in realtà il rischio è del tutto

art. 11[4], ma anche il diritto internazionale che, soprattutto dopo il secondo conflitto mondiale, ha tentato di rafforzare il divieto formale dell'uso della forza sotto l'egida del diritto[5]. La Costituzione italiana – dunque – non è la norma fondamentale di un paese neutrale non solo perché l'Assemblea costituente scelse di rigettare espressamente questa ipotesi[6], ma anche perché ogni sistema giuridico è tenuto a difendersi nei suoi elementi costitutivi, come ci ricorda la stessa carta costituzionale anche quando fa riferimento «alla sicurezza dello stato» e alla «sicurezza nazionale» formalmente nelle proprie previsioni[7].

Se la guerra è costituzionalmente prevista e quindi a certe condizioni legittima, tema diverso è quale tipo di guerra si intenda consentire nel testo costituzionale. È evidente che il concetto di guerra, a maggior ragione quella difensiva, dipende dalla minaccia che si realizza concretamente e alla quale si intende rispondere: in ultima istanza essa dipende quindi dall'inquadramento fattuale e giuridico della minaccia che incombe sulla Repubblica. La stessa scelta costituzionale della legittimità della sola guerra difensiva – vedremo di seguito cosa si debba intendere in ogni

opposto a quello segnalato dall'A. ossia pare oggi quello di una assunzione del principio pacifista a prescindere dal contesto che rischia di esporre la nostra Costituzione e la Repubblica alle nuove minacce.

[4] Con tutto ciò che comporta l'emendamento di Mario Zagari teso a inserire il termine "ripudia" che ne accentua il rifiuto a strumento ordinario, senza negare la realtà delle dinamiche politiche; cfr. A. CASSESE, *Commento all'articolo 11*, in G. BRANCA (a cura di), *Commentario della Costituzione*, *articoli 1-12*, *Principi generali*, Zanichelli-Foro it., Bologna-Roma, 1975, pp. 569 ss..

[5] Su questo aspetto, se si vuole, si rinvia alla riflessione L. CHIUSSI CURZI, A. STERPA, *Uso della forza, diritto internazionale e* rule of law *nelle oscillazioni dell'ordine globale* in *federalismi.it*, n. 8/2026. Come nota G. DE VERGOTTINI, esiste una inevitabile dialettica tra diritto costituzionale e internazionale sul concetto di guerra (*Guerra e attuazione della Costituzione*, Atti del Convegno AIC "Guerra e Costituzione" tenutosi a Roma il 12 aprile 2002, in *www.associazionedeicostituzionalisti.it*).

[6] Lo ricorda da ultimo LORENZIO CHIEFFI, *Pace e guerra in un'epoca di profonde trasformazioni delle relazioni internazionali* in *Rivista AIC*, supplemento n. 4 del 2025, pp. 20 e ss..

[7] Così l'art. 117, comma 2, Cost. assegna al legislatore statale la competenza in materia di "sicurezza dello Stato" mentre l'art. 126 Cost. fa espresso riferimento al limite della sicurezza nazionale. Sulla differenza lessicale ma non sostanziale delle due espressioni, cfr. A. STERPA, *Commento all'art. 126 Cost.*, in F. CLEMENTI, L. CUOCOLO, F. ROSA, G. VIGEVANI (a cura di), *La Costituzione italiana. Commento articolo per articolo*, il Mulino, Bologna, vol. II, 2021, pp. 420-425; M. VALENTINI, *Sicurezza della Repubblica e democrazia costituzionale*, Editoriale Scientifica, Napoli, 2017; C. MOSCA, *Democrazie e intelligence italiana*, Editoriale Scientifica, Napoli, 2018 che pone in particolare risalto la dialettica tra atipicità dei mezzi e chiarezza dei fini (spec. pp. 8 e ss.).

caso per "difensiva" – è condizionata dalla concreta forma dei pregiudizi incombenti: *senza minaccia nessuna guerra è legittima*. Qui sta il punto del rapporto tra guerra e Costituzione ossia la qualità e la riconoscibilità delle minacce quali condizioni di legittimazione dell'impiego della forza e la loro configurazione tra la sfera giuridica e quella politica[8].

Con riguardo a questo aspetto, sappiamo che nel 1946-47 i domini di intervento bellico coincidevano con i tre tradizionalmente assunti dalle discipline militari ossia terra, mare e cielo. Attraverso di essi la minaccia – per quanto intrinsecamente di suo non tipizzabile – si poteva indirizzare ad uno dei classici elementi costitutivi dello Stato ossia territorio, popolo e sovranità. I costituenti, insomma, avevano in mente – tipiche e purtroppo fresche di esperienza – le minacce classiche della guerra tra Stati attraverso le forze di terra, mare e aria. Oggi il quadro è del tutto diverso e le minacce che possono legittimare una guerra non hanno conservato le forme di allora; dette minacce si atteggiano a conformazioni nuove che hanno un impatto sullo stesso concetto di guerra dal punto di vista giuridico nella misura in cui se non si riconosce la minaccia non si può, conseguentemente, neppure agire.

Dobbiamo dunque chiederci come si inserisce, in questo contesto, la "guerra cognitiva" di cui è destinataria la Repubblica da alcuni anni per iniziativa di potenze nemiche e che pare, purtroppo, poco analizzata dagli studiosi di diritto costituzionale[9]. A tal fine, dobbiamo chiarire che cosa evochi l'espressione "guerra cognitiva". In ambito militare, per *cognitive warfare* si intende «un'operazione multidominio (o parte di essa) che impiega mezzi, azioni e strumenti attraverso le connessioni esistenti tra i domini (terrestre, marittimo, aereo, spaziale e *cyber*), l'ambiente informativo e lo spettro elettromagnetico per generare effetti nella dimensione cognitiva e influenzare il comportamento umano per ottenere un vantaggio sull'avversario»[10].

[8] Non a caso, il rapporto tra tipologia di minaccia e risposta istituzionale è alla base dell'impianto della Dichiarazione Schuman del 9 maggio 1950 con riferimento al rapporto tra gli Stati europei: "la pace mondiale non potrà essere salvaguardata se non con sforzi creativi, proporzionali ai pericoli che la minacciano". In senso simile l'espressione "siamo soli insieme" di fronte alle nuove minacce impiegata da Mario Draghi il 14 maggio 2026 ad Aquisgrana.

[9] Emblematico che nel numero speciale della rivista dell'Associazione italiana dei costituzionalisti (supplemento n. 4 del 2025), dedicato agli atti del Convegno su guerra e pace, fatta eccezione per alcuni riferimenti dovuti al contributo in particolare al Paolo Bonetti, in pochi si interroghino sulle nuove forme con le quali si presentano le minacce per il nostro ordinamento giuridico inclusa quella cognitiva.

[10] https://www.difesa.it/assets/allegati/31787/4.cognitive_warfarela_competizio-

Le modalità di conduzione della guerra cognitiva sono molto differenziate anche se possiedono un unico obiettivo di fondo: condizionare la volontà e le azioni degli individui che fanno parte di un ordinamento giuridico per indirizzarli a compiere atti che producano effetti negativi per il proprio Paese. Attenzione però, ciò non accade concretizzando (solo) le classiche fattispecie già previste: si pensi, in ambito penale, ai delitti contro lo Stato come, ad esempio, le «Intelligenze con il nemico» che, perché si perfezionino, postulano l'esistenza di una volontà cosciente di agire in danno del proprio Paese[11]. *Nella "guerra cognitiva", invece, l'individuo che fa parte della comunità della Repubblica opera contro di essa e le sue istituzioni senza avere neppure idea di farlo, ma mosso da altri obiettivi spesso assunti soggettivamente come legittimi dal punto di vista politico e giuridico*. Si pensi al condizionamento elettorale ossia al consenso per un candidato o una lista che, nel proprio programma politico, annovera formalmente o implicitamente un atteggiamento che avvantaggia – direttamente o indirettamente – una potenza straniera. L'esempio più semplice è costituito, in questi anni, dalle sanzioni dell'Unione europea verso la Russia a seguito dell'invasione illegale della Ucraina del 2022. Il governo russo ha tutto l'interesse che i governi dei Paesi membri si pronuncino contrariamente ad esse in modo da bloccarne o rallentarne l'applicazione e stessa cosa vale per l'impiego dei fondi Ue per sostenere a vario titolo il Paese invaso[12]. L'ipotesi in questione si è consumata concretamente nel corso delle elezioni presidenziali romene del 2024 che hanno portato all'annullamento – da parte della Corte costituzionale – del primo turno di voto e successivamente alla esclusione dalla parteci-

ne_nella_dimensione_cognitiva._ed.2023.pdf; come ricorda ENRICO BORGHI (membro del Copasir e autore di *Sotto attacco*, Rubbettino, Soveria Mannelli, 2025), già nel 2021 la Nato ha adottato il documento "*Countering cognitive Warfare: awareness and resilience*" nel quale si legge che "l'obiettivo delle operazioni cognitive è di cambiare non soltanto ciò che le persone pensano, ma anche come agiscono" nonché di "plasmare e influenzare le convinzioni e i comportamenti degli individui e di interi gruppi, favorendo gli obiettivi tattici o strategici dell'aggressore"; come sottolinea l'A. si realizza quel "pensiero coerente disallineato" (e forme di dissonanza cognitiva) ossia attivo per ciascuna diversa questione sottoposta a battaglia cognitiva (p. 225) e in certi casi si studia finanche la condizione di "annientamento della consapevolezza situazionale delle masse" (p. 231).

[11] Il riferimento è agli artt. 241 e ss. del Codice penale e riferiti ai "*delitti contro la personalità dello Stato*".

[12] Cfr. di recente il cambiamento di maggioranza politica in Ungheria con la fine dell'esperienza di governo di Orbán e le decisioni sul prestito finanziario da 90 miliardi di euro a favore dell'Ucraina (aprile 2026).

pazione del candidato filo-russo[13]; simili influenze sono state acclarate anche nel referendum del Regno Unito sulla Brexit (2016) e sulle altre consultazioni dell'anno (Italia e Usa), ma anche più di recente nel caso delle elezioni nella Repubblica di Moldova.

Ma c'è di più. Molto più spesso l'intervento ibrido opera senza un obiettivo a breve termine precisamente individuabile, come può essere per l'appunto un momento elettorale, ma lavora in sottofondo, spesso potremmo dire – nel linguaggio della sicurezza nazionale – "sottosoglia" con un fine strategico e non tattico. Si attua un vero e proprio surriscaldamento lento delle comunità, cercando di sfaldarle con la diffusione continua e silenziosa di sfiducia verso le proprie istituzioni e il proprio ordinamento giuridico: non una guerra calda, come quelle già note e tradizionali, ma neppure una "guerra fredda" come quella tra "mondo libero" e blocco sovietico della seconda metà del Novecento. Piuttosto una «guerra tiepida» come è stato detto in altro contesto[14], che senza eventi clamorosi incide in modo profondo e in radice indebolisce i sistemi liberaldemocratici inserendosi nella nostra forma di stato e incidendo sul piano assiologico della sua struttura. Nell'equilibrio della convivenza sotto lo stesso "tetto giuridico", gli elementi di autorevolezza integrano quelli di autorità in un circuito di fiducia reciproca[15] sul quale è costruito lo stato di diritto inteso come «prevedibilità delle conseguenze del comportamento umano» in un regime di libertà individuale[16].

"Siamo in guerra?" ci si potrebbe chiedere, intendendo per guerra, con von Clausewitz, «un atto di violenza inteso a costringere l'avversario ad obbedire alla [altrui] volontà»[17]? Meglio ancora però dovremmo do-

[13] Sia consentito rinviare a S. Sassi, A. Sterpa, *La Corte costituzionale della Romania difende la democrazia liberale dalla disinformazione. Prime note sulla sentenza n. 32 del 6 dicembre 2024*, in *federalismi.it*, n. 4/2025, pp. 162-181.

[14] Impiego l'espressione in A. Sterpa, *La difesa della democrazia dalle minacce ibride*, Editoriale Scientifica, Napoli, 2025. In precedenza, in diverso contesto, l'espressione è evocata da E. Casini e A. Manciulli (a cura di), *La guerra tiepida*, LUP, Roma, 2023, dedicato al conflitto tra Russia e Ucraina.

[15] Il rinvio, in particolare, è agli studi di E. Resta, *Le regole della fiducia*, Laterza, Roma-Bari, 2009 e Id., *Il diritto fraterno*, Laterza, Roma-Bari, 2005.

[16] Peraltro, la capacità della propaganda autocratica nei regimi liberi può essere percepita come coerente proprio perché l'Occidente è stato sempre caratterizzato, diversamente da altre esperienze politiche, dall'essere quella parte del mondo dove si è affermata la crisi dell'autorità come elemento di evoluzione delle forme organizzative (da quella divina e religiosa a quella monarchica) come ricorda A. Del Noce, *Autorità* (1979), Treccani, Roma, 2024, spec. pp. 49 e ss..

[17] C. Von Clausewitz, *La guerra* (1832), Le Monnier, Firenze, 1942, p. 3.

mandarci "siamo minacciati?" stante che il concetto operativo di guerra presuppone la costruzione di una dialettica che, a minaccia concretizzata, si nutre di azioni bilaterali ossia dell'aggressore e dell'aggredito.

La minaccia è palese anche se ancora comprensibile solo ad un numero ridotto di soggetti e di studiosi visto che per individuarla occorre abbandonare categorie obsolete e rivolgersi a nuovi strumenti di lettura della realtà e delle forme di violenza che riesce a condizionare la libertà. Non è un caso che la prima battaglia cognitiva che occorre combattere è proprio quella che vede, da parte dei nostri nemici, la negazione della presenza della minaccia stessa, anche invocando un astratto pacifismo globale lastricato di buone intenzioni. Tuttavia, come è facile comprendere, la realtà fornisce elementi evidenti di questa minaccia e, da costituzionalisti, la possiamo collocare sul piano di un tema classico quale la forma di stato attraverso anche una evoluzione del concetto di sicurezza nazionale per come fino ad oggi assunto dall'ordinamento giuridico.

Come sappiamo, il concetto di forma di stato attiene al rapporto tra autorità e libertà e, nella prospettiva del costituzionalismo liberale e democratico, essa caratterizza la dialettica tra l'individuo e il potere sulla base di un sistema di valori fissati nella Carta[18]. Il costituzionalismo non è davvero tale in ordinamenti che non conoscono i principi liberaldemocratici, visto che suo compito è dividere il potere e garantire i diritti soggettivi e può svolgerlo solo laddove esistano questi presupposti da governare. Quelle delle autocrazie e delle dittature, pur formalmente presenti, sono "costituzioni di carta" visto che sono organizzate per contraddire proprio i principi insiti nel costituzionalismo: il potere in quei Paesi è concentrato, non legittimato e sottoposto al ricambio con elezioni libere e i diritti non sono garantiti. Si potrebbe immaginare – certo – che le due diverse tipologie di forme di stato – quella liberaldemocratica e quella autocratica – possano convivere nelle diverse aree del mondo in una sorta di "guerra fredda" rinnovata con l'Ue, gli Usa e i Paesi Nato da una parte e dall'altra i "Paesi della parata di Pechino" tenutasi il 3 settembre 2025.

Al netto delle volontà politiche delle parti, però, va considerato che il precedente equilibrio della guerra fredda successivo alla fine del Secondo conflitto mondiale possedeva caratteristiche che oggi non sono più

[18] Cfr. G.U. RESCIGNO, *Forme di Stato e forme di governo*, in *Enc. Giur.*, Treccani, Roma, 1989 che si riferisce al "modo di essere dello Stato considerato nel suo insieme rispetto ai suoi elementi costitutivi (oppure, detto diversamente, che descrive il rapporto o i rapporti fondamentali tra lo Stato, visto come unità sintetica, e i suoi elementi costitutivi essenziali)" (p. 1).

presenti: i due blocchi avevano vinto insieme una guerra conto i fascismi e il nazismo[19] e governavano insieme l'Onu con il diritto di veto incrociato in sede di Consiglio di sicurezza; la capacità economica, finanziaria e tecnica dei due fronti era del tutto sbilanciata a favore delle democrazie liberali, mentre oggi non è più così; il libero mercato era prerogativa di una parte del mondo con l'altra relegata in economie arretrate e tendenzialmente chiuse e in certi casi pianificate, mentre oggi il globo è integrato a livello economico con interdipendenze nuove rispetto al passato. Inoltre, è proprio il tema della volontà politica ad esser mutato: *le autocrazie hanno lanciato una sfida alle democrazie liberali* attraverso una visione di ampliamento del proprio spazio di dominio o di influenza disconoscendo *apertis verbis* il sistema liberale[20]. Basta pensare alla politica russa di controllo, con l'uso della forza, delle *ex* repubbliche sovietiche (alcune ancora costrette nella CSI[21]) o, in modo simbolico, alla mappa geografica del passaporto cinese che raffigura una Cina più ampia dei propri confini ufficiali come ad indicare una sorta di *Lebensraum* in salsa cinese, come è stato sottolineato[22]. In tal senso parlano anche gli atti formali, sia le norme e i decreti del Presidente russo[23], sia la dottrina cinese approvata dagli ultimi congressi del Partito comunista[24]. Ma non solo. Le autocrazie hanno assunto in Africa un ruolo da potenze *neo-coloniali* controllando interi Paesi dal punto di vista politico, infrastrutturale ed energetico, ma ormai anche militare con basi di *intelligence de facto* o *de iure*[25]. Ciò,

[19] Letta con la chiave che Peter Thiel costruisce partendo da Strauss, potremmo dire che (anche) allora l'ordine formale sarebbe nato da un omicidio che rendeva la violenza temporaneamente governabile dal diritto (*Il momento straussiano*, Liberilibri, Macerata, 2025, spec. pp. 50 e ss.).

[20] In questo senso la nota intervista del dittatore russo Putin rilasciata nel 2019 al *Financial Times* e reperibile sul sito *on line* del quotidiano.

[21] La Comunità degli Stati indipendenti, nata nel 1991, che lega tra loro alcune *ex* Repubbliche sovietiche dell'URSS (Armenia, Azerbaigian, Bielorussia, Kazakistan, Kirghizistan, Russia, Tagikistan, Uzbekistan mentre il Turkmenistan è membro associato), è stata di recente abbandonata dalla Repubblica di Moldova (atto del Parlamento del 2 aprile 2026).

[22] Cfr. G. Vernetti, *Il nuovo grande gioco. Dal Giappone all'Ucraina. Viaggio lungo la frontiera fra libertà e autoritarismo*, Solferino, Milano, 2025, spec. pp. 75 e ss..

[23] Su alcuni *Ukaz* che provano a convincere della ospitalità russa gli occidentali in fuga dal sistema liberale, cfr. E. Iannario, A. Sterpa, *Quando le autocrazie sfidano la forma di stato liberal-democratica: riflessioni a margine del recente "editto" russo*, in *federalismi.it*, n. 28 del 2024, pp. 192-224.

[24] Su questi profili si rinvia a E. Borghi, *op. cit*., G. Vernetti, *op. cit*. e R. Arditti, *Hard power. Perché la Guerra cambia la storia*, Giubilei Regnani, Roma-Cesena, 2025.

[25] Cfr. i saggi contenuti in Aa.Vv., *Il mondo in guerra*, Roma Tab, 2024 e in parti-

peraltro, accade mentre nei nostri sistemi politici alcuni sostengono in modo polemico – anche in Accademia – che sarebbe l'Occidente ad esercitare in solitudine azioni *neo-coloniali* sia nel linguaggio che nelle scelte di politica estera e commerciale. È emerso, ad esempio, l'impiego che viene fatto di contratti capestro per realizzare opere pubbliche in territori di Paesi africani che, non potendo più pagare, cedono sovranità a vantaggio di operatori delle autocrazie[26]; o ancora, i flussi migratori dall'Africa verso l'Europa costituiscono armi decisive per condizionare le opinioni pubbliche nazionali[27]. D'altronde, la *National Security Strategy* della seconda amministrazione Trump riflette la necessità di ridefinire gli equilibri dell'ordine internazionale e il ruolo dei soggetti che vi insistono per aree di influenza, ripensando le strutture istituzionali sorte a partire dalla fine del secondo conflitto mondiale[28]. La dimensione dei "grandi spazi" si intreccia a quella statuale in una dialettica ricorrente nel diritto[29].

Possiamo considerare concreta detta minaccia e, quindi, immaginare di costruire una legittima risposta? Se la minaccia è già un atto unilaterale di guerra quando produce effetti[30], occorre quindi rispondere, quantomeno difendendoci nei nostri confini, anche se una azione diretta e proporzionata sarebbe altrettanto legittima impiegando mezzi proporzionati; ma sul punto torneremo.

La presenza di questa minaccia, in ogni caso, pone la questione se *trattarla come un tema di sicurezza nazionale o come una vera e propria*

colare il saggio di L. MOCCI GUICCIARDI, *Gli investimenti cinesi in Africa Sub-Sahariana. Implicazioni geopolitiche, strategiche e di sicurezza*, pp. 25 e ss..

[26] Cfr. nota precedente.

[27] Abbiamo esaminato questi aspetti in S. SASSI, A. STERPA (a cura di), *Minacce ibride alla sicurezza nazionale. Disinformazione e migrazioni*, Editoriale Scientifica, Napoli, 2025.

[28] Consultabile al link https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

[29] Come scrive C. SCHMITT (*L'ordinamento dei grandi spazi nel diritto internazionale* (1941) ora in Id., *Stato, grande spazio, nomos*, Adelphi, Milano, 2015), il "grande spazio" esprime, dal nostro punto di vista, il mutamento delle dimensioni e delle rappresentazioni dello spazio terrestre che domina l'attuale sviluppo della politica mondiale" (p. 107) che si realizza in particolare nella sfera dell'economia e della organizzazione (p. 109).

[30] Un dovere che opera oltre lo stesso atto di guerra da parte di un altro Stato allorché, per usare le parole di Nitti sulla guerra che si fa e non si dichiara, Tosato ricorda che "quando uno Stato è aggredito da un altro Stato, lo stato di guerra si afferma di diritto; quando lo Stato è aggredito, il Governo ha non solo il diritto, ma il dovere di provvedere immediatamente, senza che vi sia bisogno di un testo costituzionale che gli conceda questo potere. Non facciamo quindi dell'umorismo, troppo facile, ma fuor di luogo, sul testo del progetto" (Assemblea costituente, seduta del 21 ottobre 1947).

guerra. Mentre in precedenza il confine tra sicurezza nazionale e guerra era formalmente più evidente, dobbiamo prendere atto che in questi ultimi decenni gli elementi di distinzione si sono assottigliati rendendo sempre più difficile collocare un fatto o una fattispecie concreta da un lato o dall'altro di una semplice e risolutiva partizione. Ciò, ci permettiamo di notare, dipende dalle forme che hanno nel tempo assunto le minacce e dal nuovo ruolo degli individui (come vedremo nel paragrafo successivo per molteplici aspetti); e non a caso, va ricordato, questo confine è stato reso poroso dal fenomeno del terrorismo che ha portato i due piani ad incrociarsi in modo crescente. Vediamo perché.

La guerra è in genere guerra tra Stati, per come tradizionalmente regolata dal diritto interno e internazionale[31]. Questa idea "statuale" della guerra, la rende gestibile in termini concettuali e formali attraverso atti e procedure tipicizzate: si pensi, appunto, alla Costituzione che impiega termini come *deliberare* e *dichiarare* la guerra o alle forme del diritto diplomatico e consolare anche con riguardo all'organizzazione della rappresentanza statuale all'estero[32]. L'azione di soggetti organizzati nuovi e singoli individui che hanno costruito minacce concrete nei Paesi liberi con attacchi terroristici hanno costretto gli Stati a rapportarsi con soggetti non statuali che, se non riconducibili ad un ordinamento giuridico, si muovono come "fantasmi giuridici" se si resta al concetto statuale di guerra, ma al tempo stesso sono in grado di colpire in profondità[33]. Non è un caso che la stessa definizione di terrorismo sia giuridicamente di difficile positivizzazione[34]. Il terrorismo religioso degli ultimi decenni ha

[31] Sulla concezione continentale (maggiormente entrata sullo stato) e su quella anglosassone (aperta alla dimensione demografica) cfr. M. Capasso, *Guerra* in *Nov.mo digesto it.*, Utet, Torino, 1968, spec. p. 55.

[32] Su questi profili non si può prescindere da C. Curti Gialdino, *Manuale di diritto diplomatico-consolare europeo e internazionale*, Giappichelli, Torino, 2024 che peraltro, da ultimo, ha anche riflettuto sulle dinamiche della rappresentanza diplomatica nella Federazione russa (*Le parole di Solov'ëv sono un atto ostile. Cosa può fare l'Italia* in *formiche.net*, 2026).

[33] Insiste su questo aspetto, nei suoi contributi, G. Santomartino, *Conoscere e contrastare il jihadismo*, Panda, Trento, 2020 e Id., *Storia del pensiero sulla guerra e la pace dalla Bibbia al Jihadismo*, Panda, Trento, 2022. Utili anche i saggi contenuti in F.M. Corrao, L. Violante (a cura di), *L'Islam non è terrorismo*, il Mulino, Bologna, 2018. Si vedano anche la pagine di A.Predieri sulle estraneità e le lacune dello stato islamico in *Sharî a e Costituzione*, Laterza, Roma-Bari, 2006, pp. 178 e ss..

[34] Cfr. P. Bonetti, *Terrorismo, emergenza e costituzioni democratiche*, il Mulino, Bologna, 2006, pp. 66 e ss.; cfr. anche C. Bassu, *La lotta al terrorismo nelle democrazie stabilizzate: garantire la pubblica sicurezza nel rispetto dei diritti umani fondamentali*, in C.

mantenuto in capo allo Stato le risposte alla minaccia, senza – per l'Italia – formalizzare una guerra (come accaduto anche in precedenza per il terrorismo politico interno)[35]; in ogni caso si è iniziata a manifestare una certa sovrapposizione dei piani. Si pensi a quanto accaduto con gli interventi militari all'estero (a vario titolo legittimati nelle missioni votate dal Parlamento), ma anche all'operatività dei servizi di informazione che hanno visto – sintomo del cambiamento – accrescere il contenzioso innanzi alla Corte costituzionale per conflitto tra poteri dello Stato proprio sull'impiego dell'istituto del segreto di Stato. Non a caso Massimo Luciani parla del segreto di Stato come di un tema di crescente interesse «dopo anni di scarsa attenzione da parte della stessa dottrina costituzionalistica»[36] e i numeri sono chiari: dopo le pochissime sentenze che muovono dal segreto militare tra la fine degli anni settanta e gli anni ottanta, dal 1998 ad oggi la Corte si è pronunciata in ben dieci casi[37].

Quando il terrorismo poteva essere ricondotto ad uno Stato (che lo finanziasse piuttosto che lo sostenesse in modo occulto), la risposta avrebbe potuto essere rivolta al Paese responsabile (si pensi agli interventi militari in Afghanistan, ma oggi ai fatti in Medioriente e in particolare in Palestina, Libano, Siria e Iran), mentre è più difficile combattere il nemico in casa (*foreign fighters*) senza avvalersi, nella dinamica conflittuale, degli individui del proprio ordinamento giuridico. Sia chiaro, resta sempre a carico dello Stato e dei suoi apparati garantire la sicurezza pubblica e dei privati, ma senza dubbio gli individui sono per la prima volta apparsi nel conflitto (osservazione, controllo sociale, segnalazione, riconoscimento della minaccia attività di contrasto personale nei momenti di concretizzazione). I sistemi di difesa militare tradizionale e quelli di difesa nazionale (civili e militari) si sono dovuti coordinare perché gli aspetti

BASSU, G. PISTORIO, A. STERPA (a cura di), *Diritto pubblico della sicurezza*, pp. 71 e ss.; da ultimo, riflette sul tema anche in chiave di nuove tecnologie, C. CAPASSO, *"Algo-sicurezza". Terrorismo, contesto digitale e sicurezza*, Editoriale Scientifica, Napoli, 2025, pp. 123 e ss.. Emblematico, d'altronde, il caso dei partigiani italiani, sul quale cfr. P. CALAMANDREI, *Situazione giuridica dei partigiani sotto l'aspetto del diritto interno e internazionale e del diritto interno*, Centro di Alti Studi militari, Roma, 1949/50.

[35] Cfr. G. NEPPI MODONA, *La giurisprudenza costituzionale italiana in tema di leggi di emergenza contro il terrorismo, la mafia e la criminalità organizzata* in T. GROPPI, *Democrazia e terrorismo*, Editoriale Scientifica, Napoli, 2006, pp. 84 e ss..

[36] M. LUCIANI, *Il segreto di Stato nell'ordinamento nazionale* in *Gnosis, Quaderno di intelligence*, *Il segreto di Stato*, n. 2, 2013, p. 12.

[37] Sul tema, cfr. N. VICECONTE, *Segreto di Stato*, in C. BASSU, G. PISTORIO, A. STERPA (a cura di), *Diritto pubblico della sicurezza*, Editoriale Scientifica, Napoli, 2023, pp. 109 e ss..

informativi e i settori di intervento si sono accavallati ancor più del solito e, in sostanza, si sono stretti in una forte collaborazione come d'altronde dimostra l'istituzione – prima in via sperimentale e poi normativa – del Comitato di analisi strategica antiterrorismo (CASA)[38].

Questo assottigliamento (oggi diremmo un vero superamento funzionale) tra ambito militare e civile, ma anche tra ambito istituzionale e attività degli individui, si è completato successivamente con la guerra ibrida e cognitiva allorché si è quasi rotto il confine tra la minaccia da gestire con la guerra (quale azione esclusivamente militare) per approdare ad un approccio integrato (complessivo) quindi anche sociale della sicurezza nazionale[39]. Non a caso, dopo l'emersione in sede militare e nei rapporti al Parlamento delle strutture di *intelligence*, a livello istituzionale, il tema della minaccia ibrida e cognitiva è emerso nel Consiglio supremo di difesa, organo di fatto di raccordo e coordinamento tra strutture che avevano una vocazione originaria differenziata[40]. E non è un caso – ancora – che la dottrina più attenta, che studia da tempo in modo scientifico l'*intelligence*, segnala da tempo il carattere multidisciplinare e ampio della analisi e del ruolo delle informazioni, grazie anche alla particolare attività svolta nel contrasto al terrorismo[41]. Da ultimo, con il DPCM del 22 aprile 2026 è stato adottato il nuovo regolamento che disciplina la "gestione

[38] Il Comitato di analisi strategica antiterrorismo è stato formalmente istituti con decreto del Ministro dell'interno del 6 maggio 2004 ma aveva iniziato ad operare prima in senso sperimentale (2003).

[39] "*Cognitive warfare is both a military and societal issue*" come precisa l'ultimo rapporto scientifico Nato consultabile al link www.sto.nato.int.

[40] Il Consiglio supremo di difesa, previsto dall'art. 78 della Costituzione, è presieduto dal Presidente della Repubblica ed è stato istituto con la legge n. 624 del 1950 secondo la quale l'organo "*esamina i problemi generali politici e tecnici attinenti alla difesa nazionale e determina i criteri e fissa le direttive per l'organizzazione e il coordinamento delle attività che comunque la riguardano*". La sua composizione, con esponenti del Governo e il Capo di Stato maggiore della difesa, è comunque variabile in base alle necessità, ferma restando la vice-presidenza assegnata al Presidente del Consiglio dei Ministri che di fatto crea un *unicum* nel panorama della Costituzione. Il 17 novembre 2025 il Presidente della Repubblica ha convocato il Consiglio supremo di difesa sui temi in questione e in quella occasione il Ministro della Difesa ha presentato il non-paper "il contrasto alle guerra ibrida: una strategia attiva" consultabile al link www.difesa.it.

[41] Cfr. M. Caligiuri, *Intelligence*, Treccani, Roma, 2025, spec. pp. 50-51; per usare le parole dell'A., "l'intelligence non si può restringere a una definizione specialistica, poiché, essendo il punto di incontro della conoscenza, assume un valore universale, mettendo in discussione l'attuale organizzazione di saperi accademici ridotti a decrepiti recinti disciplinari sempre meno adeguati a comprendere quello che ci circonda" (p. 20).

delle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale" che suffraga ampiamente l'evoluzione concettuale e organizzativa che qui segnaliamo[42].

Se, come sappiamo, la sicurezza nazionale attiene alla difesa dei valori fondanti del nostro sistema costituzionale e l'esistenza stessa dello Stato, come ci ha in più occasioni chiarito la Corte costituzionale[43], per la prima volta il fronte militare di azione – relativo alle minacce materiali e fisiche agli elementi istituiti dello Stato – si unisce a quello dell'*intelligence* tradizionalmente attivo sul piano conoscitivo al fine consentire al sistema istituzionale di assumere decisioni in senso più ampio di quello strettamente militare.

Il concetto di guerra, dunque, si spoglia dei caratteri costituzionali originari, cedendo i tratti tradizionali ormai superati, per dirigersi verso forme nuove che attendono regole adeguate affinché possano essere intraprese le azioni di difesa necessarie. D'altronde, già per le nostre missioni militari all'estero abbiamo assistito ad una deroga all'impianto della guerra previsto in Costituzione. Con la legge n. 145 del 2016 abbiamo previsto procedure di azione per autorizzare interventi militari che non hanno attivato il canale costituzionale della guerra, visto che le nuove minacce hanno costretto il giurista a identificare forme nuove di regolazione di tipologie nuove di "guerra"[44]. Insomma, l'ordinamento è già uscito dallo schema degli articoli costituzionali sulla "guerra tradizionale"[45]: si

[42] Sostituendo la quasi totalità della disciplina recata dal DPCM del 5 maggio 2010 recante "organizzazione nazionale per la gestione di crisi", l'atto è stato adottato in attuazione dell'art. 7-bis, comma 5, del decreto-legge 30 ottobre 2025 n. 174 (convertito nella legge n. 198 del 2015) e riguarda anche le attività del Comitato interministeriale per la sicurezza della Repubblica.

[43] La Corte costituzionale (sent. n. 40 del 2012), con riguardo al segreto di Stato, ha chiarito che "l'istituto in questione può rinvenire la sua base di legittimazione esclusivamente nell'esigenza di salvaguardare supremi interessi riferibili allo Stato-comunità, ponendosi quale «strumento necessario per raggiungere il fine della sicurezza», esterna e interna, «dello Stato e per garantirne l'esistenza, l'integrità, nonché l'assetto democratico»: valori che trovano espressione in un complesso di norme costituzionali, e particolarmente in quelle degli artt. 1, 5 e 52 Cost. (sent. n. 110 del 1998; in prospettiva analoga, sentt. n. 106 del 2009, n. 86 del 1977 e n. 82 del 1976).

[44] La legge, recante, "*disposizioni concernenti la partecipazione dell'Italia alle missioni internazionali*", fu anticipata da atti di diverso tipo per gli interventi precedenti (in ambito Onu o Nato).

[45] G. DE VERGOTTINI espone quello che definisce "il mutamento della prospettiva del costituente nella recente normativa subcostituzionale" (*Guerra e attuazione della Costituzione*…cit.); similmente in G. DE VERGOTTINI, *Guerra e costituzione*, cit., p. 142.

tratta con ogni probabilità di una uscita ancora parziale che le nuove minacce porteranno verso ulteriori sviluppi[46].

La guerra cognitiva, dunque, si atteggia come una nuova tipologia di risposta ad una serie di minacce che ci costringono ad abbattere le categorie precedenti sia nello Stato (assottigliando i confini tra militare e civile, tra azione di guerra nei singoli domini, nonché tra attività militare e servizi di *intelligence*), sia tra lo Stato e gli individui; e che ci costringe – nell'incontro contaminante tra il concetto di guerra e quello di sicurezza nazionale – a trovare nuovi strumenti istituzionali di azione e di difesa della Repubblica.

2. *L'individuo e il "sesto dominio": come difendere la forma di stato.*

Nelle guerre tradizionali, l'individuo era generalmente considerato un attore organizzato della guerra (nelle forze armate) o una vittima, tanto da dover identificare un distinto diritto dei belligeranti, sia dei militari che dei civili che non prendessero parte attiva nel conflitto. Le minacce che si presentavano sull'individuo erano in particolare fisiche (nel dominio terrestre, marittimo e aereo, ma anche in parte spaziale e *cyber*). La emersione del sesto dominio ossia della mente umana come terreno dell'azione di "guerra" tutto cambia e l'elemento fisico – come vedremo pur presente – lascia spazio (grazie ai nuovi *media*) ad un ampio intervento a distanza che non appare inizialmente come una violenza fisica. O almeno non sembra per come noi abbiamo in mente l'idea di danno fisico.

Il funzionamento del cervello umano non è ancora del tutto noto alla scienza, ma siamo a conoscenza solamente di alcune cose che è utile ricordare ai fini delle nostre riflessioni. Si tratta di uno strumento limitato ossia non in grado di processare e conservare tutto quello che acquisisce,

[46] Emblematico, in questo senso, quanto previsto dall'art. 1, comma 1, della legge citata: "*al di fuori dei casi di cui agli articoli 78 e 87, nono comma, della Costituzione, la partecipazione delle Forze armate, delle Forze di polizia ad ordinamento militare o civile e dei corpi civili di pace a missioni internazionali istituite nell'ambito dell'Organizzazione delle Nazioni Unite (ONU) o di altre organizzazioni internazionali cui l'Italia appartiene o comunque istituite in conformità al diritto internazionale, comprese le operazioni militari e le missioni civili di polizia e per lo Stato di diritto dell'Unione europea, nonché a missioni finalizzate ad eccezionali interventi umanitari, è consentita, in conformità a quanto disposto dalla presente legge, a condizione che avvenga nel rispetto dei principi di cui all'articolo 11 della Costituzione, del diritto internazionale generale, del diritto internazionale dei diritti umani, del diritto internazionale umanitario e del diritto penale internazionale*".

tanto che la notte cancella quello che non serve e libera spazio per i contenuti del giorno dopo[47]. Il cervello, inoltre, è composto – come sappiamo – da una componente razionale e da una emotiva che convivono nella assunzione delle informazioni tanto quanto nella loro elaborazione ai fini delle decisioni che assume[48]. Ancora, il cervello svolge una faticosa azione di messa in ordine dello scibile e per farlo assume spesso categorie, scorciatoie cognitive e modelli predefiniti. Si tratta di strumenti ordinari che impediscono al cervello di andare in *default* per *overbooking* di dati: schemi, *bias* e archetipi sui quali si sono soffermate sia le scienze cognitive che la psicologia[49].

Queste attività di organizzazione dello scibile sono avvenute in modo diverso nel tempo. All'inizio dell'esperienza sociale (e quindi politica umana), la regola generale era la prossimità fisica e il linguaggio (quello verbale e del corpo) garantiva che impiegassimo tutti i sensi per farci una idea dell'altro e dell'ambiente in cui interagivamo. Con l'avvento della tecnica, abbiamo via via ampliato le relazioni comunicative umane e la quantità di dati da elaborare, fino ad oggi quando di fatto – con la rete internet e i *big data* – utilizziamo solo vista e udito. Se è vero che quando il cervello impiega solo alcuni sensi si fa una idea imperfetta di ciò che acquisisce, oggi questo è un dato concretamente sperimentato ogni istante: la realtà e il contatto fisico sono assenti o ridotti al minimo e nel caso attivabili solo *ex post* per verificare ciò che ci viene prima somministrato o che costruiamo *on line* impiegando solamente con vista e tatto. La qualità della nostra assunzione di informazioni risulta in questo modo molto ridotta. E c'è di più. La rete e i *social* forniscono così tanti elementi informativi che noi abbiamo bisogno di semplificare: il cervello è in difficoltà e chiede aiuto. Lo facciamo con categorie ideali (non necessariamente ideologiche come erano nel Novecento), *bias* cognitivi, quelli che Jung definiva archetipi e modelli sociali, ma anche attraverso il lavoro selettivo di algoritmi e motori di ricerca, come è stato ben evidenziato. In certi casi siamo anche costretti a invocare una difesa *de iure* da una vita sempre *on*

[47] G. MAIRA, *Il cervello è più grande del cielo*, Solferino, Milano, 2019.

[48] A. DAMASIO, *L'errore di Cartesio*, Adelphi, Milano, 1995; utile riferirsi anche alle "azioni non logiche" di Pareto sulle quali sia permesso rinviare anche a A. STERPA, *Quando le élite falliscono nelle società libere* in ID. (a cura di), *Il fallimento delle élite*, Giubilei Regnani, Cesena, 2025, pp. 5 e ss..

[49] G. MAIRA, *op. cit.* e C.G. JUNG, *L'Io e l'Inconscio* (1928), Boringhieri, Torino, 1948, *passim*. Cfr. anche i lavori di L. DI GREGORIO, *Demopatia. Sintomi, diagnosi e terapie del malessere democratico*, Rubbettino, Soveria Mannelli, 2019 e ID., *War Room Attori, strutture e processi della politica in campagna permanente*, Rubbettino, Soveria Mannelli, 2024.

line: non a caso la legge statale ha dovuto formalizzare il diritto a disconnettersi quasi a voler consentire al cervello di prendere fiato[50].

Ora la domanda che ci dobbiamo porre è semplice: quali strumenti possiede l'individuo per gestire questa pioggia di informazioni e di dati e quanto detti strumenti sono in grado di sottoporlo ad una manipolazione che ne condiziona la stessa identità? E questa manipolazione può costituire una minaccia per lo Stato?

Nell'individuo del Novecento, ossia che si relazionava con i simili attraverso i tradizionali mezzi di informazione, vi erano delle condizioni del tutto diverse da ora. Prima di tutto, le informazioni non solo erano minori ma erano "editate" da intermediari che, stante anche la limitatezza fisica degli strumenti, selezionavano quelle accessibili. Si pensi alla stampa cartacea e alla radio-televisione: il mondo analogico consentiva a dei professionisti di gestire un pluralismo limitato (esterno e interno) al quale accedeva un individuo organizzato socialmente e anche molto politicizzato o comunque cognitivamente armato dai sistemi di educazione e formazione e abituato ad una vita di prossimità fisica con gli altri. È come se sopra la nostra testa vi fosse stato un filtro che permetteva ad un numero ridotto di informazioni, peraltro non come materiale grezzo ma anche lavorato a livello informativo, di accedere al nostro cervello. Inoltre, il diritto statuale era in grado di controllare queste attività nel caso, ad esempio, violassero le leggi e comportassero pregiudizi di ordine personale o sociale[51].

L'individuo inoltre era dotato di altri "ombrelli protettivi" del cervello umano che, quindi, non solo accedeva ad una serie di informazioni selezionate ma era incentivato all'utilizzo di categorie sociali, politiche e culturali strutturate (ideologie, religioni, consuetudini e controllo sociale). Inoltre, la costante fisicità delle relazioni umane sottoponeva tutte le informazioni al vaglio della fisicità. Il classico esempio per cui nessuno assumeva dati affidabili dall'ubriaco che stazionava al Bar, presupponendone l'inaffidabilità e rivolgendosi invece al Sindaco, al Carabiniere o al Parroco del luogo[52]. La realtà dei corpi, insomma, anche quando sostituita per una quota dell'azione relazionale e informativa, ricompariva nella

[50] Cfr. la legge n. 81 del 2017 sul diritto alla disconnessione.

[51] Per una lettura in questo senso del passaggio dalla normazione dei media analogici a quelli digitali, cfr. A. Sterpa, *La libertà di comunicazione digitale, il potere e il costituzionalismo*, in M.E. Bucalo, M. Caporale e A. Sterpa, *Diritto pubblico di internet*, Editoriale Scientifica, Napoli, 2024, pp. 15-40.

[52] Il richiamo è alla nota intervista ad Umberto Eco consultabile sul sito *www.lastampa.it*.

sua forza definitrice, nella sua capacità legittimante e de-legittimante delle fonti di informazione[53].

Oggi questo quadro è del tutto mutato. La massa infinita di informazioni è gestita fuori da controlli come quelli del passato e i *social media* sono – anche dopo il DSA – meri conduttori di dati di ogni sorta e l'algoritmo – anch'esso difficilmente regolato dal diritto dell'UE – è dotato di un «fascino erotico»[54] proprio perché semplifica il caos a vantaggio di un cervello umano finito, incidendo sulla sua stessa identità personale laddove rivela o oscura ciò che ritiene senza che l'uomo possa realizzare una verifica concreta[55]. Inoltre, con la profilazione degli utenti, l'effetto della selezione delle informazioni accessibili e poi di fatto acquisite riesce anche a condizionare ancor di più l'identità del soggetto[56].

Ma non solo a distanza siamo minacciati. Se si guarda all'ambito corporeo materiale, non va dimenticato che la minaccia cognitiva al nostro cervello passa anche per attacchi materiali come le onde elettrometriche che interferiscono sulle capacità di connessione delle sinapsi cerebrali e sulla memoria, come dimostrato dal noto caso della "sindrome dell'Havana"[57].

Che fare, dunque, mentre gli individui sono bombardati nell'intimo della propria struttura cognitiva? In Assemblea costituente si discuteva della previsione nella Carta della mobilitazione (generale o parziale

[53] Di questo riflette anche D. ANTISERI, *Il prezzo della libertà è l'eterna vigilanza*, Editoriale Scientifica, Napoli, 2017, connettendo il tema a quello dell'educazione, pp. 48 e ss..

[54] In questo senso mi sono espresso sia in A. STERPA, *L'ordine giuridico dell'algoritmo: un nuovo ordinamento giuridico* in A. STERPA (a cura di), *L'ordine giuridico dell'algoritmo*, Editoriale Scientifica, Napoli, 2024, pp. 9-31 e in ID., *La difesa della democrazia dalle minacce ibride…*cit.; cfr. anche A. STERPA, I. DE VIVO, C. CAPASSO *L'ordine giuridico dell'algoritmo: la funzione regolatrice del diritto e la funzione ordinatrice dell'algoritmo* con I. DE VIVO E C. CAPASSO, in *Nuovi autoritarismi e democrazie. Diritto, istituzioni, società*, n. 2 del 2023, pp. 120-155.

[55] Cfr. il lavoro di S. TIRIBELLI, *Identità personale e algoritmi*, Carocci, Roma, 2023.

[56] Cfr. A. GATTI (*Profilazione e diritti fondamentali: modelli a confronto: Europa, Usa, America Latina*, Editoriale Scientifica, Napoli, 2025) che, nella prima parte dello studio, si sofferma sulla descrizione delle diverse tipologie di attività di profilazione. Sulla micro-profilazione a fini elettorali cfr. in particolare il Regolamento 900 del 2024 relativo alla trasparenza e al *targeting* della pubblicità politica che conferma, tra l'altro, l'impatto dell'integrazione europea sulla forma di stato.

[57] Si tratta dell'impiego di armi che emanano onde in grado di interferire con le attività cerebrali, menomandole in modo differente. Ne parla anche E. BORGHI, *op. cit.*, p. 232.

che fosse)[58] per assumere, in sede militare, l'organico sufficiente a combattere la guerra. Accanto a questa dimensione tradizionale della difesa che, come ha ben ricordato anche Roberto Arditti di recente[59], non è da sottovalutare, oggi sembra matura la giustificazione costituzionale di una "chiamata" all'azione dell'intera popolazione anche nella guerra cognitiva. Proprio l'idea parziale di guerra contenuta negli artt. 78 e 98 della Costituzione ci consente di costruire, come accaduto per le missioni all'estero in precedenza, canali legali alternativi di azione a difesa della Repubblica davanti alla nuova minaccia.

2.1. La "militanza cognitiva" come politica di sicurezza

La Costituzione, lo diciamo subito, non solo ci consente di armare gli individui in questa nuova guerra: ci obbliga ad adottare in primo luogo contromisure più a basso impatto e quindi a non dover innalzare il livello di minaccia al punto da comportare l'impiego di altri strumenti di difesa più incisivi e più drammatici, inclusa la guerra. Le modalità di questa azione possono ben essere individuate con legge statale nei limiti della Costituzione, come accaduto per le altre nuove minacce che hanno assottigliato i confini tra guerra e sicurezza nazionale. Possiamo provare a identificarne due diverse tipologie, non certo risolutive, ma complementari, di attività per una prima azione che potremmo complessivamente definire con l'espressione di "militanza cognitiva"[60].

La prima serie di strumenti che può essere annoverata attiene alla alimentazione e al rafforzamento delle capacità cognitive attraverso un potenziamento critico-cognitivo che rafforzi la competenza al discernimento da parte dell'individuo. Si tratta del profilo soggettivo della militanza cognitiva che oggi passa per la presa di coscienza dell'indebolimento degli strumenti cognitivi umani attraverso fenomeni noti come la riduzione

[58] L'art. 33 del progetto originario prevedeva "*Spetta all'Assemblea Nazionale deliberare la mobilitazione generale e l'entrata in guerra*". Cfr. discussione del 20 dicembre 1946 nella seconda Sottocommissione della Commissione per la Costituzione.

[59] Cfr. R. Arditti, *Hard power. Perchè la Guerra cambia la storia*, cit. che pone in risalto il lato militare degli equilibri e della gestione delle minacce attuali.

[60] Il concetto non evoca una formazione militante, tipica dei regimi autocratici, relativamente ai concetti, ma al metodo cognitivo lasciando l'individuo a svolgere liberamente la propria valutazione. Sulla formazione nello Stato etico relativamente al fascismo, cfr. M. Sterpa, *La scuola in linea*, Le Monnier, Firenze, 1940 e D. Roncarà, *Saggi sull'Educazione Fascista*, La Diana scolastica, Bologna, 1938 nella cui edizione consultata è stato apposto un timbro ad integrazione del titolo con il testo "ovvero temi svolti sull'educazione idealistica".

del vocabolario linguistico, la ridotta capacità di compiere connessioni tra eventi e di un adeguato bagaglio di memoria. Come si può capire, i sistemi liberaldemocratici non si possono difendere nello stesso modo in cui ciò accade in quelli autocratici ossia attraverso la censura in rete o sui *media* e neppure con l'educazione di regime che omette narrazioni scomode e veicola una "verità" storica[61]. Non possiamo censurare la rete e le informazioni perché così facendo non solo violeremmo i nostri valori costituzionali, ma anche il diritto europeo e soprattutto ci troveremmo a combattere la guerra con strumenti per noi ancor più inefficaci di quanto siano per i nostri nemici che li usano a deperimento della persona umana. La nostra ricchezza, di cui le autocrazie sono sprovviste, è proprio la libertà umana che gli altri vorrebbero trasformare in una nostra debolezza: essa costituisce invece la nostra forza. Si può da questo punto di vista immaginare che nel nostro sistema di istruzione l'insegnamento di educazione civica sia declinato proprio in senso cognitivo e di capacità critica. Con la legge n. 92 del 2019 è stato regolato l'insegnamento dell'educazione civica nelle scuole primarie e secondarie per un totale di trentatré ore minime, spettando all'autonomia delle strutture, nell'ambito delle previsioni ministeriali, l'attuazione delle norme di legge. La previsione statale pretende che la materia sviluppi "*la conoscenza e la comprensione delle strutture e dei profili sociali, economici, giuridici, civici e ambientali della società*" nelle scuole, mentre "*iniziative di sensibilizzazione alla cittadinanza responsabile sono avviate dalla scuola dell'infanzia*". È evidente che per come la legge descrive le attività, vi è già spazio per inserire le attività necessarie alla "militanza cognitiva".

Il secondo pacchetto di strumenti è invece costituto dal *profilo oggettivo* ossia consentire un accesso alle informazioni libero ma articolato e che, seppur ovviamente plurali, siano autorevoli e verificate: anche senza un bollino di verità, infatti, si può certamente isolare la bugia. L'idea è quella di regolare quello che deve restare comunque un libero mercato delle idee dove possa essere l'individuo colui il quale espelle le "informazioni cattive"[62]. Ciò può accadere sia con strumenti di ordine privato (si

[61] Cfr. il ragionamento di Y.N. HARARI sulla possibilità che l'IA si ribelli ai capi delle autocrazie, spec. quando parla della impossibilità di un "prigione dei bot", del dominio informativo che l'IA può avere sui vertici delle dittature portandoli a compiere gesti sbagliati, nell'ambito di un "doppio linguaggio" che simula democrazia dove essa non c'è (*Nexus. Breve storia delle reti di informazione dall'età della pietra all'IA*, Bompiani, Milano, 2024, pp. 459 e ss.).

[62] L'approccio del libero mercato delle idee, reso universale dalle pagine di J.S. MILL, *Sulla libertà* (1869), Mondadori, Milano, 2000, è in Italia ripreso in particolare da Luigi

pensi all'attività di *fact checking* come *Newsguard*) o con l'azione dell'*intelligence* che, non più sinonimo di oscurità, deve essere assunta come mezzo di conoscenza: il caso delle elezioni romene annullate insegna che senza i servizi di informazione che desegretassero quelle informazioni non sarebbe stato possibile scoprire l'attacco ibrido russo[63]. Tra gli strumenti di oggettivizzazione dei rischi, non può non citarsi anche la regolazione della circolazione delle idee e delle associazioni e dei partiti che le veicolano. Sappiamo bene che l'Italia ha costituzionalmente deciso, dopo il fascismo, di non aderire ad uno schema di democrazia protetta come accaduto ad esempio in Germania[64]. Ma se è vero che, pur non avendo altro limite costituzionale espresso alla libera manifestazione del pensiero che il buon costume e pur non avendo costruito limiti legislativi ad esso se non per mezzo del rispetto degli altri diritti (privacy, diffamazione…), anche a livello di diritto di associazione dobbiamo pensare ad una attività di verifica e informazione delle azioni poste in essere dai privati organizzati. L'ambiguità della XII disposizione transitoria e finale della Costituzione è indicativa. Essa prevede che sia vietata *"la riorganizzazione, sotto qualsiasi forma, del disciolto partito fascista"*[65] ma è chiaro che occorre allargare la portata "anti-totalitaria" (di cui l'anima anti-fascista è solo una parte, pur storicamente importantissima) della previsione integrando la normativa primaria[66].

Infine, tra questi strumenti non può non valorizzarsi l'incontro fi-

Einaudi e della tradizione liberale; cfr. L. Einaudi, *Il problema della stampa quotidiana* (28 settembre 1943) ora in A. Sterpa (a cura di), *I liberali e la ricostruzione della democrazia. I fascicoli del Movimento liberale italiano (1943-1944)*, Editoriale Scientifica, Napoli, 2025.

[63] Ho sostenuto questa tesi in S. Sassi, A. Sterpa, *La Corte costituzionale,* cit. e in A. Sterpa, *La difesa della democrazia*, cit.; in senso simile, cfr. anche M. Caligiuri, *Intelligence…*cit., secondo il quale "la recente evoluzione culturale ha trasformato l'*intelligence* da cono d'ombra delle democrazie a strumento indispensabile per stabilizzarle" (p. 22).

[64] Sul tema, cfr. A. Gatti, *La democrazia che si difende. Studio comparato su una pratica costituzionale*, Cedam, Padova, 2023, ma anche S. Ceccanti, *Le democrazie protette e semi-protette da eccezione a regola. Prima e dopo le Twin Towers,* Giappichelli, Torino, 2004 e S. Ceccanti, F. Ferroni, *Democrazia protetta,* in *Digesto delle discipline pubblicistiche*, Utet, Torino, 2015, pp. 55 e ss..

[65] Cfr. A. Sterpa, *Il "saluto romano" tra divieto di ricostituzione del partito fascista e difesa dei valori costituzionali* in *Rivista giuridica delle forze armate e di polizia*, Jovene, Napoli, n. 2 del 2024, pp. 5-26.

[66] Nella seduta del 19 novembre 1946 della Prima Sottocommissione il segretario del Pci Togliatti chiese agli esponenti della Dc (Dossetti e La Pira) di specificare il divieto di costituzione del partito fascista. La DC fu inizialmente contraria alla specificazione del divieto, motivando anche con il fatto che un partito come il Pci potesse ricadere nel divieto qualora al concetto di fascismo se fosse voluta dare un'accezione ampia. A quel punto

sico, ossia l'attivazione dei sensi di cui siamo naturalmente dotati per selezionare la realtà e assumerla: in questo senso la logistica funzionale all'esercizio delle libertà politiche dal tratto maggiormente corporeo come il diritto di riunione e di associazione, è un bene strumentale alla costruzione delle comunità libere[67]. Dette attività si possono inserire in una azione di esercizio, verso l'esterno, di una azione di *soft power* di cui l'Italia è in potenza molto forte fino a rafforzare anche quella che di recente Bassetti chiama l'italianità[68]. Il tema identitario, infatti, costituisce uno degli strumenti di resistenza al condizionamento cognitivo che punti a destrutturare il gruppo sociale di appartenenza.

Infine, intendendo sintetizzare, il terreno della militanza cognitiva è caratterizzato da un ragionevole bilanciamento tra le ragioni di diversificazione delle scelte del singolo e di appartenenza alla comunità nazionale fattasi ordinamento giuridico. Non va dimenticato che, quando altre minacce interne hanno impiegato gli individui come strumento di lotta allo Stato (si pensi al terrorismo politico), sono state impiegate leve diversificate, inclusa quella della spesa pubblica e dei diritti sociali, non senza conseguenze sui bilanci pubblici. Oggi il tema si pone in termini anche finanziari, ma più in generale nell'ambito della preferibilità dei sistemi democratici e liberali da parte dei consociati in termini di rendimento degli stessi anche per quanto riguarda la produzione della ricchezza (da utilizzare poi per le politiche pubbliche anche a scopi sociali). Rendere preferibile la liberaldemocrazia non per adesione dogmatica e fideistica è nella stessa logica delle democrazie liberali uno strumento di azione della guerra cognitiva perché valorizza la scelta soggettiva preclusa invece all'individuo che è confinato nei sistemi autocratici.

3. Considerazioni conclusive

Come in tutti i casi in cui la minaccia è articolata ed agisce con canali diversificati, quindi, così anche la risposta non può essere semplice e

il segretario del Pci precisò che il divieto avrebbe dovuto riguardare il partito fascista per come conosciuto storicamente come prevede il testo finale.

[67] Fanno riferimento ad "intelligenza di rete e socialità" nella democrazia in R. MENOTTI, M. SGROI, *La sfida della democrazia. Strategie per il migliore dei mondi possibili*, Licosia, Ogliastro Cilento, 2025, pp. 81 e ss..

[68] P. ACCOLLA, N. D'AQUINO, *Italici. An Encounter with Piero Bassetti*, Bordighera Press, New York, 2008, pubblicato, per l'appunto, anche tradotto in inglese.

univoca o, meglio, possiamo dire che non ha una forma ma più forme[69]. Il costituzionalismo è chiamato a definire e impiegare quella pluralità di risposte e a inquadrare gli strumenti nuovi di contrasto alle minacce imminenti che rischiano di porre fine, accanto alla liberaldemocrazia, anche alla esistenza del costituzionalismo. Sì, perché la guerra di difesa prevista dalla Costituzione era tale in quanto posta a presidio della esistenza stessa della nostra forma di stato per come declinata, a livello organizzativo e assiologico, dalla Costituzione. Con il mutare delle minacce, il concetto tradizionale di guerra si è svuotato di senso e resta come *extrema ratio* di fronte alle forme di minaccia che, invece, nei decenni repubblicani si sono diversificate costringendo il diritto ad armarsi di istituti e concetti nuovi che implementino l'arsenale di difesa giuridica; siamo già andati oltre il concetto bellico che avevano in mente i costituenti e il cammino a quanto pare continua.

L'espansione delle minacce gestite attraverso strumenti diversi dalla "guerra prevista in Costituzione" è testimonianza della pluralità delle azioni – diverse appunto dalla "guerra" – che già abbiamo sperimentato e che, in ogni caso, sono e debbono essere regolate nel rispetto della Costituzione visto che sono finalizzate alla conservazione del nostro assetto valoriale e della forma di stato. Rispetto al fenomeno del terrorismo, che ha stressato non poco l'impianto giuridico costituzionale, è necessario oggi un nuovo sforzo di riflessione che identifichi, in una logica di garanzia, innovativi strumenti di azione difensiva, inclusa la promozione dei nostri valori in chiave di narrazione positiva[70].

Pensare che la spesa pubblica per la sicurezza possa essere gestita solamente nei modi tradizionali – ossia come spesa *in primis* militare come si ragiona di recente anche in termini di impegni in sede Nato e Ue – sostanzia un approccio superato, tanto quanto l'idea di rendere preferibile il sistema democratico e liberale per le sole prestazioni sociali che garantisce verso i consociati.

In primo luogo, perché le strategie che in passato potevano essere seguite per questo approccio fondato sulla spesa pubblica militare e sociale non sono oggi più disponibili per le note ragioni che riguardano la riallocazione delle fonti di prelievo delle imposte statali e la riduzione del gettito; ma soprattutto lo sono per un'altra ragione di fondo.

[69] Il tema della mancanza di una forma ("senza forma", *wu-hsing*) davanti al nemico è in Sun-Tzu, *L'arte della guerra*, Bur, Milano, 1997, pp. 54-55.

[70] In questo senso ora P.F. Dettori, *Riconquistare menti e cuori. L'Occidente sul campo di battaglia digitale*, Rubbettino, Soveria Mannelli, 2026.

Come sappiamo, gli individui si organizzano in comunità per due ragioni distinte e in parte contradditorie: stare con i propri simili e ridurre i rischi di gestione della diversità (i c.d. "diritti di chiusura"), ma anche per poter rendere più efficiente la propria esistenza e dedicare il tempo libero da necessità appagate dallo stare insieme per sperimentare e innovare ("diritti di apertura")[71]. Se declinassimo la nostra azione contro le autocrazie solo sul primo aspetto, sceglieremmo un campo di battaglia nel quale le dittature sono più forti di noi (salvo poi crollare sul lungo periodo). Chi meglio di loro, infatti, sterilizzando la dignità e l'unicità della persona, può realizzare un ordine egualitario e senza movimenti? Dove invece le democrazie liberali sono imbattibili è proprio nel terreno dei diritti/doveri ossia della costruzione della libertà di ognuno di diventare un *unicum* irripetibile. Questo terreno, però, sconta comunque una serie di rischi perché non coincide con il "dirittismo" ossia con la mera e continua estensione normativa di diritti (quel «diritto ai diritti» di Stefano Rodotà giustamente criticato da Gustavo Zagrebelsky)[72]; esso è invece il campo dei diritti necessari ad espandere la libera azione individuale.

Insomma, per rispondere alle autocrazie serve più libertà che permetta a ciascun componente della comunità di tendere all'unicità, alla propria progettualità quanto possibile fondata sull'autodeterminazione nella dignità. L'alternativa è stata ben narrata da Hannah Arendt nella descrizione del processo a Eichmann; in quel caso più volte l'esponente nazista faceva riferimento a come, grazie al proprio inserimento in un ordine sovradeterminato, egli fosse uscito dalla sua condizione di mediocrità e si sentisse utile e vivo. Un sistema, quello autocratico, dove «ogni ingranaggio, ossia ogni persona, deve esser poter sostituita senza modificare il sistema stesso»[73].

Difendere l'ordine costituzionale liberale e democratico, quindi, esclude la trasformazione dell'individuo in un ingranaggio sostituibile,

[71] M. WEBER, *Economia e società* (1922), Edizioni di Comunità, Milano, voll. I, 1961, pp. 51 e ss.; M. DE CAROLIS, *Il paradosso antropologico. Nicchie, micromondi e dissociazione psichica*, Quodlibet, Macerata, 2008, pp. 27-28.

[72] Il riferimento è in particolare a S. RODOTÀ, *Il diritto di avere diritti*,Laterza, Roma-Bari, 2012 e alla critica a G. ZAGREBELSKY, *Diritti per forza*, Einaudi, Torino, 2017, p. 23; come nota, peraltro, Zagrebelsky fu Hannah Arendt ad impiegare per prima l'espressione del diritto ai diritti (p. 83).

[73] H. ARENDT, *Responsabilità e giudizio*, Einaudi, Torino, 2003, p. 25. L'opera citata nel volume fu pubblicata per la prima volta, in diversa versione rispetto a quella riportata nel volume, nel 1964.

ma pretende la valorizzazione di tutti gli istituti e le condizioni che lo rendano un elemento unico e caratterizzante; e ciò è in perfetta coerenza con i principi fondamentali della Costituzione ossia con il principio personalista e la dignità umana, fondamenti della nostra forma di stato e del nostro costituzionalismo. Come ricorda Franco Modugno, infatti, «l'art. 2 come generale statuizione sul riconoscimento-garanzia dei diritti inviolabili, oltre e indipendentemente dalle specifiche e puntuali previsioni costituzionali dei diritti, può significare in fondo proprio questo: che la libertà come valore non può essere circoscritta a previsioni determinate e specifiche delle esplicazioni e direzioni in cui esso si realizza»[74].

La guerra cognitiva, dunque, pretende una azione istituzionale e costituzionalmente orientata a difesa della dignità umana quale conseguenza non della mera "ragione di stato" delle guerre tradizionali, quanto dell'esigenza della "ragione di libertà" degli individui[75].

[74] F. Modugno, *I "nuovi diritti" nella giurisprudenza costituzionale*, Giappichelli, Torino, 1995, p. 8.

[75] Una guerra per "ragione di libertà" è intesa al fine di ribaltare la retorica pacifista contro la guerra come politica di potenza legata alla ragion di stato espressa anche da E. Krippendorff, *Lo Stato e la guerra* (1985), Gandhi Edizioni, Pisa, 2008 e dal filone della c.d. "scienza della pace".

TRA AUTORITÀ E LIBERTÀ: LA MINACCIA NELL'ECOSISTEMA DIGITALE

Victor Maximilian Hartl[*]

SOMMARIO: 1. Autorità e libertà nello stato costituzionale. – 2. Piattaforme digitali e autorità. – 3. Piattaforme digitali e libertà – 3.1. La costruzione interna della libertà. – 3.2. La proiezione esterna della libertà.

1. *Autorità e libertà nello stato costituzionale*

All'interno dell'ampio spettro dei caratteri e dei contenuti che definiscono la categoria di forma di stato[1], una costante delle diverse ricostruzioni offerte dalla dottrina pare rinvenirsi nella individuazione dei termini della relazione che sostanziano, concettualmente, la forma di stato, e differenziano, tipologicamente, le forme di stato: autorità e libertà. La forma di stato, allora, può essere ricostruita come una relazione di potere fra questi due termini e, più dettagliatamente e sfruttando, anche con superficialità, il momento logico hegeliano, quale sintesi e combinazione dei poteri di cui è titolare lo "stato-persona", esercitati dallo "stato-apparato", e dei poteri dello "stato-comunità" (*rectius* la somma delle posizio-

[*] Dottorando di ricerca in "Società in mutamento: politiche, diritti e sicurezza" nell'Università degli Studi della Tuscia.

[1] Cfr. F. LANCHESTER, *Stato (forme di)*, in *Enciclopedia del diritto*, vol. XLIII, Giuffrè, Milano, 1990, secondo il quale i diversi criteri possono essere raggruppati in "l'inclusione o meno all'interno della società politica della totalità degli individui appartenenti al gruppo aventi un livello minimo di età […] l'attribuzione e il rispetto di alcuni diritti fondamentali di libertà ed eguaglianza, implicanti prestazioni di fare o di non fare da parte dello Stato apparato; il regime giuridico della proprietà e l'intervento dello Stato apparato nel mercato"; secondo L. PEGORARO, S*istemi costituzionali*, Giappichelli, Torino, 2020, rileverebbero i criteri del rapporto tra economia e diritto, delle finalità perseguite dallo Stato, dei principi che ispirano il rapporto tra Stato e società civile, della titolarità e della legittimazione del potere politico, della garanzia dei diritti di libertà, dell'esistenza o meno di una Costituzione; secondo G. AMATO, F. CLEMENTI, *Forme di Sato e forme di governo*, il Mulino, Bologna, 2012, rileverebbero i criteri della repressione delle condotte antisociali, dell'allocazione dei beni e dei servizi, della legittimazione e distribuzione del potere pubblico, della garanzia dei diritti e delle libertà.

ni di libertà dell'individuo e delle formazioni sociali), che si risolve nello "stato-ordinamento".

Non essendo questa la sede privilegiata per approfondire con il dovuto rigore scientifico il problema della forma di stato, si ritiene tuttavia utile, nella prospettiva dell'oggetto specifico di questo contributo, fare un passo indietro e soffermarsi brevemente sulle nozioni di autorità e libertà e sulla relazione che intercorre tra esse.

L'autorità, da un punto di vista statico, può essere intesa come quella dimensione ordinante e necessaria che emerge dall'aggregazione degli individui in forme organizzate. L'essenza ordinante dell'autorità si manifesta funzionalmente nel potere, quale, in un primo stadio, capacità materiale di imporre la propria volontà[2] ma limitata dal fine, originario e autonomo, a cui la stessa emersione necessitata dell'autorità risponde e, per questa via, traendone un fondamento legittimante. Invero, quando da queste aggregazioni sorge un'organizzazione sociale (popolo) dotata dei caratteri di permanenza, stabilità e stanzialità (territorio), «implicando la soddisfazione di bisogni individuali e collettivi, che finiscono per atteggiarsi come fini sociali»[3], la dimensione ordinante dell'autorità e dei relativi poteri (sovranità) assume, parallelamente e secondo l'insegnamento tradizionale, una forma istituzionale, quindi ordinamentale, che coincide, da Westfalia a oggi, con la categoria di stato, i cui poteri, secondo l'insegnamento tradizionale e nelle trame del tessuto di diritto qual è l'ordinamento inteso come categoria, trasmodano nella capacità unilaterale di determinare effetti giuridici nella sfera giuridica dei soggetti.

La libertà, di contro e apparentemente, è quella condizione di assenza del potere, di negazione del potere; quella dimensione individuale che si realizza nella capacità attiva del soggetto di autodeterminarsi, compiere scelte e agire per realizzare fini da esso stesso determinati. Nondimeno, la libertà, in questa ricostruzione concettuale, partecipa degli stessi caratteri dell'autorità appena sopra circoscritti: come l'autorità, la libertà può solo nascere nel contesto di un'aggregazione di individui in forme organizzate, non essendoci, diversamente, una dimensione ontologica dalla, nella e attraverso la quale possa realizzarsi l'autodeterminazione dell'individuo;

[2] Elemento questo che, seppur in forme più sofisticate, rimane una delle pietre d'angolo su cui si fonda il principio d'autorità degli stati moderni; cfr. G.U. RESCIGNO, *Diritto pubblico*, Zanichelli, Bologna, 2022, pp. 10 e ss., nella disamina dello stato quale ente monopolizzatore della forza legittima.

[3] G. DE VERGOTTINI, T.E. FROSINI, *Diritto pubblico*, Cedam, Padova, 2021, p. 3.

al pari dell'autorità, la libertà è potere[4], inteso come volontà che si realizza immediatamente, dunque in assenza di mediazioni, imponendosi nella dimensione oggettiva e soggettiva del reale, nel presupposto di una innata e intima forza espansiva dell'individuo[5]; analogamente all'autorità, anche la libertà è una volontà autonoma e originaria, e non eteronoma, il cui fine, la cui direzione, è da essa stessa impressa.

È quest'ultimo rilievo in ordine ai caratteri logici di cui si compongono l'autorità e la libertà in relazione all'autonomia del fine che esse si pongono che, invero, attualizza dinamicamente il contrasto fra questi due termini, la cui composizione è l'essenza stessa della forma di stato. L'autorità e la libertà si muovono, infatti, in un rapporto conflittuale (ad es. nell'esperienza dello stato autocratico) o sinergico (ad es. nell'esperienza dello stato costituzionale), in una continua tensione i cui i diversi punti di caduta definiscono l'una o l'altra forma di stato. Non a caso, l'evoluzione storica delle diverse forme di stato che si sono avvicendate possono leggersi nel quadro dell'elaborazione di strumenti di limitazione del potere in funzione delle libertà[6], declinandosi nelle forme di «una tecnica della libertà contro il potere arbitrario»[7], dove arbitrario è il potere che non conosce altra direzione della volontà diversa da quella che essa stessa si imprime. Infatti, nel tentativo di aggiungere un tassello a questa preliminare impostazione, è di particolare evidenza l'idea per cui il tema dell'autorità, non può essere utilmente trattato senza fare riferimento al potere quale autonoma categoria concettuale, proiezione dell'autorità ma allo stesso tempo sostanza della stessa, nella misura in cui il potere è tale «in quanto esiste, e, per ciò, la determinazione della essenza del potere si risolve nella determinazione del potere nel suo esistere»[8]. In altre parole, la forma, il contenuto e i limiti dell'autorità radicano la loro esistenza, in rapporto alla libertà, nella forma, nei contenuti e nei limiti del potere. Ciò chiarito, allora, l'idea appena cennata della libertà come tecnica di limitazione del potere deve essere correttamente intesa: prima ancora che limite esterno all'esercizio dell'autorità, la libertà è una categoria che agisce sulla morfologia del potere, negandone in radice la concentrazio-

[4] Cfr. V. Angiolini, *Studi in onore di Giorgio Berti*, Jovene, Napoli, 2005, pp. 97 e ss.

[5] Il riferimento alla perdurante forza espansiva dell'individuo evoca F. Nietzsche, *La volontà di potenza*, (in Italia e più di recente per) Bompiani, Milano, 2021.

[6] Cfr. P. Ridola, *Il principio di libertà nello stato costituzionale. I diritti fondamentali in prospettiva storico-comparativa*, Giappichelli, Torino, 2018.

[7] N. Matteucci, *Organizzazione del potere e liberta. Storia del costituzionalismo moderno*, il Mulino, Bologna, 2016, p. 20.

[8] P. Biondi, *Studi su potere*, Giuffrè, Milano, 1965, p., 33.

ne come modo di essere dello stesso e predicandone invece la divisione, quale migliore garanzia a tutela della libertà.

Volendo qui trattare le criticità della relazione fra una specifica forma di stato e l'emersione dei nuovi poteri digitali, è appena il caso di notare come, alla luce e con gli strumenti fin qui dipanati, la forma di stato costituzionale di matrice liberal-democratica abbia, per certi versi, risolto l'espressione di questa dinamica conflittuale. Se è vero, infatti, che autorità e libertà partecipano degli stessi tre caratteri logici già visti (contesto originario, volontà come potere, autonomia del fine), la grande "rivoluzione" rappresentata dallo stato costituzionale di matrice liberal-democratica è stata quella di disinnescare il conflitto logico e storico fra queste due espressioni di potere, e la loro relazione antagonistica, attraverso l'attribuzione eteronoma del fine perseguito dall'autorità: il fondamento e il principio ordinante e operativo dell'autorità risiede nella miglior tutela e garanzia della libertà nella sua espressione più ampia e plurale, non avendo altro fine se non il fine stesso che la libertà si pone che, nei termini del fondamento dei poteri in cui si esplica, e si traduce «non già nella contraddittoria autolimitazione unilaterale dell'unico potere dominante, ma nella accettazione contrattuale di limiti legali da parte del potere sovrano determinata dalla presenza e volontà di altro e diverso potere, posto e riconosciuto a sua volta come autonomo»[9]; in definitiva, nella centralizzazione del soggetto titolare del potere-libertà, ossia l'individuo. Lo stato, allora, «è libertà, nel senso che deve pensarsi fondato sulla libertà, perché il suo compito e la sua stessa struttura interna appariscano giustificati. Libertà è svolgimento progressivo della personalità nell'azione; è direzione costante e inflessibile del volere […] Tale affermazione soddisfa a un'esigenza più imperiosa: quella di considerare la realizzazione della convivenza ordinata, di cui il soggetto individuale è elemento e fattore, come celebrazione della sua libertà»[10].

Di conseguenza, il naturale precipitato, sulla base del quale si imposta questo contributo, è quello per cui ogni problema di libertà è una questione che ha a che vedere con il potere; ogni problema di potere è una questione di libertà.

[9] P. BIONDI, *Studi sul potere*, cit., p. 42.

[10] G. PERTICONE, *Stato (teoria generale)*, in *Novissimo Digesto Italiano*, vol. XVII, p. 252; in senso analogo G. BERTI, *Sovranità*, in *Enciclopedia del diritto, Annali I*, Giuffrè, Milano, 2007, p. 1089, per il quale «non avrebbe ragione di essere la sovranità se essa non significasse riconoscimento e tutela delle libertà dei membri di un determinato popolo».

2. *Piattaforme digitali e autorità*

La circostanza di fatto per cui, oggi, le nuove piattaforme digitali concentrino una quantità smisurata di potere e di poteri è indiscussa. Vale la pena indagare, tuttavia, se questa concentrazione di potere si innesta in quella relazione di potere fra autorità e libertà appena vista e se, per questa via, esistono degli elementi per parlare di una de-formazione dello stato costituzionale di matrice liberal-democratica[11], tenendo a memoria l'argomento prima sviluppato, approdo del costituzionalismo liberale, che ritrova nella divisione del potere l'unica dimensione morfologica compatibile nell'orizzonte della libertà.

Le piattaforme digitali «offrono servizi informativi, interattivi, di condivisione di file, s*treaming* e comunicazione multimediale. La parte essenziale di qualsiasi piattaforma digitale è la comunità che interagisce con essa»[12]. Tuttavia, definizioni di piattaforme digitali assunte dal punto prospettico dei servizi offerti, forse, non colgono la vera essenza che si trae dall'osservazione empirica del fenomeno, soprattutto nella sua evoluzione più recente. Invero, le piattaforme digitali hanno creato un nuovo spazio di esistenza, a-specifico e non settoriale, in cui possano esprimersi una gamma progressivamente più ampia delle interazioni umane e sociali: in altre parole, le piattaforme digitali costituiscono un ordinamento a carattere sempre più generale che, per l'effetto, si giustappone all'ordinamento generale per eccellenza e fino ad oggi (ieri?) il solo concepibile, ossia lo stato[13]. I confini, sempre più mobili e lontani, di questo nuovo spazio digitale dell'esistenza, al quale non a caso il legislatore europeo si riferisce con la locuzione ecosistema, si trovano in un processo di costante ridefinizione poietica, grazie all'infinita capacità demiurgica dell'algoritmo, nella loro sempre più accelerata ibridazione con la realtà materiale.

Il respiro di generalità a questo nuovo ordinamento si è avuto sotto il segno della costruzione progressiva di una partecipazione sempre più estesa a questa nuova realtà, di una soddisfazione sempre più ampia dei bisogni del singolo e, parzialmente, della collettività all'interno dello

[11] Significativamente, si rileva come ormai appaiono correnti espressioni che si riferiscono alle nuove piattaforme digitali nei termini della sovranità; v. ad es. A. Celotto, *"Sudditi". Diritti e cittadinanza nella società digitale*, Giuffrè, Milano, 2023, e F. Paruzzo, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, ESI, Napoli, 2022.

[12] R. Bocchini (a cura di), *Le piattaforme digitali. e-Agorà*, Giappichelli, Torino, 2025, p. 17.

[13] S. Romano, *L'ordinamento giuridico*, Sansoni, Firenze, 1977, *passim*.

spazio digitale, di una incessante evoluzione tecnica e tecnologica, anche grazie ai progressi in materia di AI, nell'architettura delle piattaforme. In effetti, la trasversalità (*rectius* generalità) che oggi caratterizza queste piattaforme è ben evidenziata dal profluvio di provvedimenti normativi che hanno offerto una cornice regolatoria nei settori più disparati del diritto, quindi alle più varie interazioni sociali selezionate dal traffico giuridico, in questo nuovo ecosistema digitale: per fare solo qualche esempio, nell'arco degli ultimi dieci anni, il legislatore europeo è intervenuto in materia di dati con il Reg. (UE) 2016/679, c.d. GDPR, nella prospettiva della tutela delle persone fisiche, il Reg. (UE) 2016/680, nella prospettiva dell'attività realizzate dalle autorità competenti in materia penale, il Reg. (UE) 2022/868, c.d. Data Governance Act nella prospettiva della *governance* dei dati, il Reg. (UE) 2023/2854, c.d. Data Act, nella prospettiva dell'equo accesso ai dati; in materia di tutela della concorrenza e del mercato nell'ecosistema digitale con il Reg. (UE) 2022/1925, c.d. Digital Markets Act; in materia, per alcuni profili, di qualità del processo democratico e della regolazione del c.d. *hate speech* e, più ampiamente, della moderazione dei contenuti *online* con il Reg. (UE) 2022/2065, c.d. Digital Services Act; in materia di tutela del consumatore digitale con la Direttiva (UE) 2019/770 e via discorrendo. Nonostante l'approccio regolatorio del legislatore, fino ad oggi, si sia caratterizzato per profili di settorialità nella regolazione del fenomeno, non sfugge come gli ambiti del traffico giuridico ed economico più variamente toccati da queste normative possano ricomporsi, come tessere di un mosaico, in un quadro, appunto, di (tendenziale) generalità di questo nuovo ordinamento.

Senonché, la regolazione normativa pare essere insufficiente, se non inefficace, nel tentativo di attrarre e confondere nell'ordinamento generale statuale il nuovo ordinamento costituito dalle piattaforme digitali. Questo perché il diritto, quale trama del tessuto dell'ordinamento statuale, non è la categoria ordinante nel e dell'ecosistema digitale, il quale, invece, dispone di un altro strumento di architettura ordinamentale: l'algoritmo. Questo ordinamento, invero, può essere definito, utilizzando una espressione particolarmente calzante, come l'*ordine giuridico dell'algoritmo*[14]: così come «la norma giuridica crea i cassetti nei quali inserire i continui accadimenti, nell'infinito produrre di azioni umane grazie alla tecnica, l'algoritmo mette ordine e rende accessibili contenuti che la mente da sola non riuscirebbe a gestire. C'è però un passaggio che merita

[14] A. STERPA (a cura di), *L'ordine giuridico dell'algoritmo*, in Collana Tiresia, Quad. 1, Editoriale Scientifica, Napoli, 2024.

attenzione: mentre il diritto pubblico crea un ordinamento giuridico nel quale l'individuo è in grado, grazie al costituzionalismo democratico e liberale, di governare l'assetto regolatorio che impone a sé stesso e all'ambiente, così non accade nell'ordine posto dall'algoritmo»[15]. Avviene, così, che se nell'ordinamento generale statuale il diritto, quale manifestazione del potere, a sua volta attributo dell'autorità, agisce nel perseguimento del fine proprio della libertà, la norma algoritmica sfugge a questo circuito, rivelando tutta l'attualità del conflitto fra autorità e libertà che nel nuovo spazio digitale si manifesta, se, come si vedrà, si considerano l'ampiezza dei poteri in capo ai titolari delle piattaforme digitali e lo spettro delle libertà che oggi si esplicano in questo nuovo ecosistema.

Ma vi è di più. La norma giuridica opera nel mondo del *dover essere*, eventualmente predisponendo strumenti sanzionatori e repressivi o proattivi e incentivanti che possono comportare effetti conformativi nei confronti dei destinatari di una norma, ma non per questo in grado di imporsi direttamente sull'espressione del reale. Di contro, la norma algoritmica agisce sull'*essere* delimitando con precisione e nettezza i confini del possibile, disegnano l'azione materiale (e digitale) che può o non può essere realizzata dall'individuo e lo stesso contesto in cui questa azione si inscrive. La norma algoritmica non si limita a indicare ciò che è consentito o vietato, ma struttura l'ambiente digitale, orienta le possibilità di scelta, filtra le informazioni accessibili e determina in modo automatico priorità, visibilità e percorsi decisionali. In questo senso, la sua forza normativa non deriva dalla prescrizione esplicita, bensì dalla capacità di modellare la realtà operativa dell'individuo, influenzandone i comportamenti in maniera spesso invisibile e preventiva. La normatività algoritmica, allora, non si manifesta come comando rivolto alla volontà del soggetto, ma come organizzazione tecnica del contesto entro cui quella volontà si forma ed esercita.

I poteri dei creatori di questo nuovo ordinamento (tendenzialmente) generale, dunque, affondano le loro radici nella dimensione di questo nuovo potere demiurgico del reale, di modellazione del possibile, ponendosi per questa via il primo conflitto logico fra autorità e libertà nel nuovo ecosistema digitale dal quale tutto il resto discende: «la forma unitaria del potere la si riscontra esclusivamente nelle teorie relative alla creazione del mondo e alla onnipotenza di un soggetto supremo (quale può essere un Dio) allorché nel momento in cui il potere si afferma (nel suo primo

[15] A. Sterpa, *L'ordine giuridico dell'algoritmo: un uovo ordinamento giuridico*, in A. Sterpa (a cura di), *L'ordine giuridico dell'algoritmo*, cit., p. 13.

ed unico caso) lo fa in forma pura e in modo istantaneo ed unitario. Solo in quell'istante il potere mantiene una dimensione unitaria che non giustifica alcuna relazione né con i destinatari né con altri poteri»[16]; il potere della creazione, dunque, è un potere che per sua intima struttura non conosce limiti se non quello della volontà della creazione, non potendo emergere il conflitto dinamico con altro potere e, segnatamente, con la libertà. È da questo primo postulato, poi, che partono le diramazioni analitiche dei poteri dei nuovi "sovrani" digitali: il potere economico, se si ha riguardo al ruolo di *gatekeepers*, secondo la terminologia del c.d. DMA, che oggi queste piattaforme ricoprono, decidendo se e a che condizioni ammettere la trasversalità degli operatori economici all'interno di questa piattaforma; il potere infrastrutturale, il quale si lega a doppio filo con la normatività algoritmica e con la capacità demiurgica di questi nuovi attori, plasmando la circolazione del valore e il traffico sociale; il potere politico e informazionale, nella sua ulteriore articolazione in potere di comunicazione, potere politico diretto (ossia la capacità di influenzare i processi di formazione dell'opinione pubblica) e potere politico indiretto (attraverso la moderazione dei contenuti); il potere biopolitico, quale forma di potere capace di incidere sulla formazione della soggettività di individui e gruppi sociali[17]. Ancora, per effetto «dell'adozione di regole interne di controllo da parte delle piattaforme […], si sono sviluppati poteri di regolazione e di attuazione delle regole, nonché appositi apparati con funzioni che potrebbero definirsi almeno giustiziali, se non giurisdizionali in senso proprio»[18-19], suggerendo in termini quasi forzati una lettura, come più volte offerta in questo contributo, di questo nuovo ordinamento (tendenzialmente) generale in termini analogici a quegli or-

[16] A. STERPA, *La frammentazione del processo decisionale e l'equilibrio costituzionale tra i poteri*, in *federalismi.it*, n. 23/2019, p. 5.

[17] Questa rapida rassegna riprende la lucida ricostruzione dei poteri digitali offerta da I. DE VIVO, *Il contesto tecnologico e sociale della comunicazione*, in M.E. BUCALO, M. CAPORALE, A. STERPA (a cura di), *Diritto pubblico di internet*, Editoriale Scientifica, Napoli, 2024, pp. 52 e ss.

[18] L. TORCHIA, *Lo Stato digitale*, il Mulino, Bologna, 2023, p. 34.

[19] Il caso più noto è quello del *Facebook's Oversight Board*, organo chiamato ad adottare decisioni, su sollecitazione dell'interessato, sulle determinazioni assunte da Facebook o Instagram in materia di moderazione e/o rimozione dei contenuti. Le condizioni contrattuali prevedono esplicitamente che Facebook e Instagram debbano adeguarsi a quanto deciso dal Comitato, il quale svolge la sua attività in condizioni di "neutralità", "indipendenza" e "imparzialità". Non sfugge la funzione giurisdizionale rimessa a questa Comitato in una materia che coinvolge un rosa diversificata di diritti e libertà fondamentali quali, fra gli altri, il diritto di difesa e la la libertà di espressione.

dinamenti giuridici dotati di potere normativo, potere esecutivo e potere giurisdizionale che chiamiamo stati.

A questo punto, recuperando questa suggestione proposta che giustappone l'ordinamento generale statuale a questo nuovo ordinamento (tendenzialmente) generale, è inevitabile chiedersi quale sia il fondamento giuridico che legittima l'esercizio di poteri di tale vastità nei confronti di individui, gruppi sociali, operatori economici, popoli: se nello stato costituzionale di matrice liberal-democratica è la costituzione, nell'*ordine giuridico dell'algoritmo* è il contratto. Simmetricamente, allora, nell'ecosistema digitale, il titolo d'accesso a questa nuova dimensione del reale, la patente di esistenza dell'individuo, anche nell'espressione delle proprie libertà, è un negozio privato. Peraltro, non il contratto inteso come paritaria composizione degli interessi coinvolti, ma il contratto nella sua dimensione giuridica asimmetrica, ossia i termini e le condizioni d'uso, quale contratto d'adesione in cui i termini del rapporto sono definiti interamente, in questo caso, dai titolari della piattaforma e all'individuo/utente è rimessa la scelta, e v'è da chiedersi se libera in senso sostanziale, di aderirvi o no. Pare impresa ardua non rilevare la forte distonia fra la cornice regolatoria privatistica e l'assetto di poteri che promana dal combinato disposto della norma algoritmica e dei termini e condizioni d'uso in capo ai titolari di queste nuove architetture digitali, tenuto conto del grado di incisione degli stessi sullo spettro delle libertà. In effetti, potrebbe dirsi che l'ordinamento (tendenzialmente) generale che oggi costituiscono le piattaforme digitali è il risultato di una somma di contratti individuali che si traducono in atti di sottoposizione all'autorità che le piattaforme digitali manifestano; circostanza questa che, nonostante il tratto semantico in comune, si conceda l'ironia, poco ha a che vedere con la teoria contrattualistica del giustapposto ordinamento generale statuale.

Invero, non può sottacersi la pressante «necessità, propria del moderno costituzionalismo, di procedere ad una limitazione dei poteri digitali che muova nel segno di una rinnovata centralità dell'uomo […] apparendo non più procrastinabile l'esigenza di oltrepassare una visione privatistica della rete»[20], traendo insegnamento dal costituzionalismo liberale al fine di ricostituire efficacemente il rapporto fra autorità e libertà, come compendiato nella forma di stato costituzionale di stampo liberal-democratico, attraverso l'attribuzione al potere del fine della celebrazione dell'individuo nella dimensione assiologica delle libertà.

[20] C. Cipolloni, *Persona, poteri privati e Stato nella rivoluzione internettiana*, Giappichelli, Torino, 2024, p. 75.

3. Piattaforme digitali e libertà

Analizzati nel paragrafo precedente e per sommi capi i termini in cui si declina la categoria di *autorità* nell'ecosistema digitale, è questa la sede per trattare il problema della *libertà*, non potendosi prescindere, allo scopo, dall'individuo quale punto di partenza. Il tema della libertà all'interno delle piattaforme digitali viene non di rado assorbito dall'analisi d'impatto della nuova realtà digitale sulla libertà di manifestazione del pensiero, anche nei suoi riflessi di libertà informazionali, venendo in gioco l'art. 21, Cost., ma anche, e forse soprattutto, alla luce della nuova costruzione normativa dell'ecosistema digitale europeo, l'art. 11, Carta di Nizza e l'art. 10, CEDU (Carta che, come è noto, è parte dell'*acquis* eurounionale; v. art. 6, par. 3, TUE). Tuttavia, la gamma delle libertà coinvolte è ben più ampia, potendosi annoverare, a titolo esemplificativo, la libertà di riunione, il diritto di associazione nonché il diritto d'accesso e partecipazione. Peraltro, in questo nuovo contesto, «rimane problematico separare le diverse libertà, dovendosi giungere, semmai, a un modello olistico di libertà: d'altronde, chi accede a internet si esprime, corrisponde, naviga, si unisce e si riunisce, in forme variabili e lasciate alla scelta individuale»[21].

Ciò detto, l'orizzonte più ampio in cui deve inscriversi il problema della libertà all'interno dell'ecosistema digitale è lo stesso che perimetra lo spazio di esistenza dello stato costituzionale di matrice liberal-democratica: prima ancora che le singole libertà, la *libertà* dell'individuo quale fondamento assiologico dell'autorità e dei relativi poteri. Questo per tre ordini di ragioni: da un lato, perché, nonostante si assista oggi ad una espansione dell'*ordine giuridico dell'algoritmo* verso un ordinamento ai confini della generalità, in concorrenza allo stato, la relazione fra l'individuo e il potere rimane organizzata secondo questo principio, la cui negazione lo stato costituzionale non ammette; dall'altro, poiché, come segnalato a più riprese, il digitale non può più essere considerato quale mezzo attraverso il quale si esercitano le libertà, in ottica strumentale, ma deve essere correttamente inteso come spazio entro il quale esistono le libertà e, anzi, si ridisegnano; infine, con un afflato di sintesi fra le prime due ragioni, poiché pare ravvisarsi un rapporto circolare tra la realtà fisica e il virtuale, ormai parte di un'unica grande infosfera che confonde i piani attraverso plurime interazioni tra l'analogico e il digitale, che sì

[21] T.E. FROSINI, *Liberté, egalité, internet*, Editoriale Scientifica, Napoli, 2023, p. 89.

modifica la realtà in cui si esprime, ma non altera il dogma che presiede alla relazione fra autorità e libertà.

Ora, offrire una definizione esaustiva e soddisfacente del principio di libertà rischia di rimanere esercizio vano; non per questo non è inefficace procedere per prime approssimazioni. Il principio di libertà che legittima e innerva l'autorità e il potere, così come i diversi diritti di libertà, ne assume una nozione di "autodeterminazione, autonomia, per la quale esser libero significa non essere determinati da altri, non dipendere da altri nelle proprie decisioni, volere senza che altri diriga la nostra volontà"[22]. Questa idea di libertà, nell'ordinamento italiano, è illuminata dal principio personalista di cui all'art. 2, Cost., che pone al centro l'individuo e il suo pieno sviluppo nei termini da essa stessa determinati, offrendo il crisma di laica sacralità al patrimonio inesauribile di espressione della persona quale principio ordinatore delle aggregazioni sociali nella loro dimensione politica. Il principio personalista nella sua accezione di principio assiologico di libertà può considerarsi allora la matrice di tutte le libertà, anche costituzionali: se le libertà «appartengono all'uomo come essere libero» (Corte cost., sent. n. 11/1956), la condizione di libertà dell'uomo è precisamente il presupposto, la garanzia e l'elemento di legittimazione e funzionalizzazione del potere preziosamente racchiuso nell'art. 2, Cost.

Tutto ciò premesso, è già nelle trame degli artt. 2 e 3, Cost. (quando in quest'ultimo si fa riferimento alla rimozione degli ostacoli di natura giuridica, economica e sociale) che il pieno sviluppo della persona, quindi la libertà nella sua accezione fondante, è modellata dai «contesti materiali [che] influenzano la soggettività e plasmano la personalità»[23]. È fin troppo facile allora, arrivati a questo punto, concludere con una domanda: come e in che misura, prima ancora che le libertà, le nuove piattaforme digitali plasmano la libertà?

3.1. La costruzione interna della libertà

Come appena chiarito, la libertà di cui qui si tratta è quello «*status libertatis* quale bene-presupposto costituzionalmente implicito (come il bene della vita, ad esempio) che abbraccia non tanto forme espressive specifiche della libertà individuale, quanto il complesso delle manifesta-

[22] D. Nocilla, *Libertà*, in S. Cassese, *Dizionario di diritto pubblico*, Giuffrè, Milano, 2006, p. 3499.

[23] C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quaderni Costituzionali*, XLIII (3), p. 549.

zioni che si riassumono in tale stato. Occorre pertanto, innanzitutto, che il singolo possa effettivamente essere libero di compiere azioni senza che la realtà circostante lo influenzi oltre un certo grado e pertanto presuppone il diritto di autodeterminarsi»[24].

Le piattaforme digitali, oggi, incidono sulla libertà di autodeterminarsi dell'individuo sotto due profili connessi ma distinti: da un lato, la disinformazione; dall'altro, la profilazione. In relazione al primo profilo, la circolazione rapida e spesso incontrollata di «quelle notizie che sono intenzionalmente e verificabilmente false e potrebbero trarre in inganno chi vi si imbatte»[25], favorita dalla norma algoritmica che seleziona preferibilmente contenuti sensazionalistici o emotivamente coinvolgenti, amplificando così fenomeni di polarizzazione e manipolazione collettiva, compromettono la libertà di autodeterminazione dell'individuo in tanto in quanto le determinazioni dell'Io non si fondano più su informazioni corrette e consapevoli, ma su contenuti alterati o costruiti strategicamente. Non a caso, infatti, il ricorso a veicoli di informazioni false, quali i *bot* all'interno dello spazio digitale, è oggi parte della strategia geopolitica delle democrazie illiberali per destabilizzare i sistemi costituzionali di matrice liberal-democratica nel contesto più ampio della "guerra cognitiva"[26]. L'individuo, allora, nella sua dimensione costitutiva e quale fondamento e fine della forma di stato costituzionale, diventa l'obiettivo privilegiato di un'azione di contrasto che tenta di raggiungerlo, manipolandolo. A complicare ulteriormente lo scenario, poi, vi è la considerazione per cui il tema delle *fake news* si pone sulla linea di confine sfumata con la libertà di espressione, rappresentando uno sforzo erculeo, se non vano, il tentativo di inscrivere in una cornice epistemologica adeguata il tema della verità dell'informazione. In quest'ultimo senso, sono state sollevate critiche ai più recenti interventi del legislatore europeo sul punto (DSA, DMA e *Media Freedom Act*) ponendosi il rischio che «norme eccessivamente vaghe o ampie si traducano in una compressione arbitraria del diritto alla libertà di espressione, nonché del correlato diritto a un'informazione libera, pluralista e di qualità»[27].

[24] A. GATTI, *Profilazione e diritti fondamentali. Modelli a confronto: Europa, Usa, America Latina*, Editoriale Scientifica, Napoli, 2026, p. 288.

[25] M.E. BUCALO, M. CAPORALE, A STERPA (a cura di), *Diritto pubblico di internet*, cit., p. 261.

[26] A. STERPA, *La difesa della democrazia dalle minacce ibride. Teoria della comunità, dell'autorità, del potere e delle migrazioni: elementi per un'analisi strategica della "guerra tiepida"*, Editoriale Scientifica, Napoli, 2025.

[27] S. SASSI, A. STERPA (a cura di), *Minacce ibride alla sicurezza nazionale. Disinformazione e migrazioni*, Editoriale Scientifica, Napoli, 2025, p. 42.

In relazione al secondo profilo, è noto che il funzionamento delle piattaforme digitali poggi sul processo di raccolta e analisi dei dati personali di un individuo per creare un profilo delle sue caratteristiche, preferenze o comportamenti, favorendo così la creazione delle cc.dd. *filter bubbles*, bolle create all'interno dello spazio digitale dentro le quali l'individuo è esposto continuativamente a contenuti rafforzativi delle proprie convinzioni ed opinioni per come ricavate dall'algoritmo. Ora, in questo scenario, si afferma una frammentazione della rappresentazione del reale, diversa per ciascun individuo, che mette in crisi la tutela del libero sviluppo della personalità individuale, ossia della sua coscienza. Di conseguenza, nel nuovo ecosistema digitale in cui parte delle libertà dell'individuo si realizzano in uno spazio sottratto allo stato, si assiste a una trasformazione qualitativa del rapporto tra autorità e libertà. Se nello stato la libertà di autodeterminazione dell'individuo è garantita per effetto dall'astensione dello stato o di un suo intervento positivo al fine di un "pieno sviluppo della personalità umana", i poteri digitali agiscono una etero-direzione invisibile della volontà dell'individuo, mai manifesta come coercizione esplicita, attraverso la strutturazione preventiva e, quantomeno, parziale dei dati reali funzionali alla determinazione dell'Io, con l'obiettivo di trattenere l'individuo all'interno di questa nuova dimensione del reale; in altre parole, forse, un modello di conservazione di un potere autonomo nel fine che rievoca la conflittualità logica, storica e assiologica fra autorità e libertà, annichilendo quest'ultima attraverso la negazione del suo presupposto, ossia la libera autodeterminazione del volere dell'individuo.

3.2. La proiezione esterna delle libertà

Avendo voluto più ampiamente trattare la sorte della libertà nella sua dimensione assiologica all'interno dell'ecosistema digitale e non essendo questa la sede per un approfondimento ulteriormente dettagliato, un doveroso cenno, comunque, deve essere rivolto all'idea per cui le piattaforme digitali rappresentino, sotto alcuni aspetti, uno dei principali fattori di espansione delle libertà fondamentali. Sul versante passivo, in un sistema decentralizzato che disintermedia lo spazio fisico, attraverso queste piattaforme è oggi possibile una circolazione delle informazioni più rapida, accessibile e potenzialmente svincolata dai tradizionali centri di controllo politico ed economico, ampliando le possibilità di accesso alla conoscenza e di espressione individuale. Sul versante attivo, gli individui possono produrre, condividere e ricevere contenuti su scala globale,

partecipando in modo diretto al dibattito pubblico e favorendo dinamiche di pluralismo informativo, di diffusione associativa e di possibilità di mobilitazione. Ancora, le libertà economiche sono state rafforzate dalla riduzione delle barriere all'ingresso tradizionalmente connesse ai costi di intermediazione, alla localizzazione geografica e all'asimmetria informativa, favorendo l'emersione di nuovi modelli imprenditoriali fondati sul commercio elettronico, sulle piattaforme digitali e sull'economia dei dati. Dunque, coerentemente al quadro costituzionale di riferimento, per alcuni aspetti «le tecnologie hanno rappresentato e continuano a rappresentare uno sviluppo delle libertà; anzi, le libertà si sono potute notevolmente accrescere ed espandere verso nuove frontiere dell'agire umano proprio grazie al progresso tecnologico»[28].

Nondimeno, l'esercizio di queste libertà, potenziate nella loro proiezione esterna dalle piattaforme digitali, si scontrano, sotto un primo aspetto, con l'esercizio dei poteri dei titolari delle piattaforme digitali. Un esempio su tutti: la c.d. *hard moderation* prevista dal c.d. DSA. Per effetto dell'artt. 3 e 16, Reg. (UE) 2022/2065 le piattaforme digitali hanno il potere-dovere di rimuovere i contenuti illeciti, ai sensi della normativa nazionale, ma anche i contenuti leciti ma non conformi ai termini e alle condizioni d'uso o a non meglio definiti *standard* della *community*. Ebbene, se si tiene conto che tutti i contenuti immessi nella piattaforma rappresentano un esercizio di una libertà fondamentale quale quella di manifestazione del pensiero, pare configurarsi allora una delega a un potere privato, peraltro non diversamente legittimato se non da un atto di adesione contrattuale, di un difficile bilanciamento fra diritti fondamentali e altri beni giuridici. Rischia di non essere peregrina allora l'affermazione secondo la quale, così facendo, «mutano attraverso l'azione di un soggetto privato i paradigmi di giustizia elaborati da livello interno come internazionale e si traspone su un piano nuovo quel rischio di evaporazione dei diritti fondamentali che le Costituzioni della seconda metà del Novecento avevano consegnato al bilanciamento di soggetti pubblici e che qui, in un *deficit* di rappresentanza democratica e nella piena discrezionalità di cosa sottoporre a decisione, sono rimessi all'autorità di privati che si auto-legittimano»[29].

[28] T. E. FROSINI, *Liberté, egalité, internet*, cit., p. 92.

[29] F. PARUZZO, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, cit., p. 134.

FORMA DI STATO E GUERRA COGNITIVA: LA DIFESA DELLE DEMOCRAZIE LIBERALI NELL'ERA DELLE MINACCE IBRIDE

Antonio Teti[*]

1. *La mutazione del conflitto: dalla guerra industriale alla guerra cognitiva*

Per comprendere la portata della guerra cognitiva nel contesto contemporaneo, è necessario collocarla all'interno di una traiettoria evolutiva più ampia che ha trasformato la natura stessa del conflitto. Ogni fase storica ha prodotto una specifica forma di guerra: la guerra pre-moderna, caratterizzata da scontri limitati e territorialmente circoscritti; la guerra industriale, fondata sulla mobilitazione totale delle risorse; la guerra fredda, dominata dalla deterrenza nucleare e dalla competizione ideologica. La fase attuale, tuttavia, introduce un elemento di discontinuità radicale. La guerra non è più soltanto un evento, ma una condizione permanente, poiché non è più confinata a specifici teatri operativi, ma permea l'intero spazio sociale. Essa non si limita all'uso della forza, ma include strumenti informativi, tecnologici e cognitivi, ed è in questo contesto che il dominio cognitivo emerge come il nuovo baricentro strategico. Esso non sostituisce gli altri domini, ma li integra e li attraversa. La dimensione fisica, quella cibernetica e quella informativa convergono in un unico spazio operativo, in cui la mente umana diventa il principale obiettivo. Questa trasformazione può essere interpretata come il passaggio da una logica di distruzione a una logica di influenza. Se nella guerra tradizionale, l'obiettivo era neutralizzare le capacità dell'avversario, in quella cognitiva,

[*] Responsabile del settore sistemi informativi e innovazione tecnologica di Ateneo nell'Università degli Studi di Chieti-Pescara "Gabriele D'Annunzio".

l'obiettivo è modificarne il comportamento. Oggigiorno il successo non si misura in termini di territori conquistati, ma di decisioni influenzate.

2. *Il dominio cognitivo: definizione e implicazioni strategiche*

Il dominio cognitivo può essere definito come lo spazio in cui si formano le percezioni, le convinzioni e le decisioni degli individui e delle collettività. Esso include dimensioni psicologiche, culturali, sociali e simboliche, e rappresenta il livello più profondo della competizione strategica. A differenza degli altri domini, quello cognitivo presenta caratteristiche peculiari. In primo luogo, è intrinsecamente soggettivo: ciò che conta non è la realtà oggettiva, ma la sua rappresentazione. In secondo luogo, è altamente dinamico in quanto le percezioni possono cambiare rapidamente in risposta a stimoli informativi. Infine, è difficilmente controllabile: non esistono confini chiari né strumenti di difesa tradizionali. Queste caratteristiche rendono il dominio cognitivo particolarmente adatto a operazioni di influenza, e gli attori ostili possono intervenire in modo mirato, sfruttando vulnerabilità psicologiche e sociali, per orientare le decisioni senza ricorrere alla forza. Un aspetto fondamentale è quello che insiste sulla relazione tra informazione e potere. Nella società contemporanea, il controllo dei flussi informativi equivale al controllo delle dinamiche sociali. Chi riesce a influenzare ciò che le persone percepiscono, riesce indirettamente a influenzare ciò che esse fanno. La forma di Stato rappresenta un elemento determinante nella configurazione delle vulnerabilità cognitive. Le democrazie liberali, in particolare, presentano una struttura che le rende contemporaneamente resilienti e fragili, e la loro forza risiede nella capacità di adattamento, nella pluralità delle fonti e nella libertà di espressione. Tuttavia, questi stessi elementi possono essere sfruttati per introdurre instabilità. In altri termini, il punto centrale è quello del rapporto tra apertura e controllo. Nei sistemi democratici, l'informazione circola liberamente, senza un filtro centralizzato, se ciò favorisce la trasparenza, nel contempo rende difficile il contrasto alla diffusione di contenuti manipolativi. La guerra cognitiva sfrutta questa straordinaria "vulnerabilità" per infiltrarsi nel tessuto informativo. Non si tratta, quindi, di una tipologia di attacco diretto, ma di un processo di contaminazione progressiva, in cui elementi di disinformazione vengono introdotti e amplificati fino a diventare parte del discorso pubblico. Va evidenziato che uno degli elementi più rilevanti della guerra cognitiva è la crisi della verità. Nella società con-

temporanea, la distinzione tra vero e falso diventa sempre più difficile, a causa della moltiplicazione delle fonti e della velocità della comunicazione, fenomeno che può essere descritto come una frammentazione epistemica, in cui diverse comunità costruiscono versioni alternative della realtà. In assenza di un quadro condiviso, il consenso diventa fragile e instabile. La guerra cognitiva si inserisce in questo contesto, amplificando la frammentazione e rendendo sempre più difficile la costruzione di una narrativa comune. Il risultato è una società divisa, in cui le decisioni collettive diventano più complesse.

La guerra cognitiva si sviluppa attraverso una serie di livelli interconnessi, che vanno dalla produzione di contenuti alla loro diffusione e amplificazione. A livello superficiale, si collocano le operazioni di disinformazione, che consistono nella diffusione di informazioni false o manipolate. Tuttavia, queste rappresentano solo una parte del fenomeno. A un livello più profondo, si colloca la costruzione di narrative. Le narrative non sono semplici storie, ma strutture interpretative che orientano la percezione della realtà, e che definiscono ciò che è rilevante, ciò che è credibile e ciò che è accettabile. Un ulteriore livello è rappresentato dalla manipolazione algoritmica. Le attuali piattaforme digitali utilizzano algoritmi che sono in grado di determinare la visibilità dei contenuti. Intervenire su questi algoritmi significa influenzare ciò che le persone vedono e, di conseguenza, ciò che pensano.

3. Casi di guerra cognitiva e scenari operativi

Se per secoli, la guerra è stata definita dalla conquista dello spazio fisico, con l'avvento dell'era digitale, il conflitto si è spostato nei *bit* del cyberspazio, mutando in maniera più profonda e insidiosa lo scenario del conflitto bellico. La "*cognitive warfare*" rappresenta l'ultima frontiera dello scontro umano, un ambito in cui l'obiettivo non è più distruggere l'arma o il corpo dell'avversario, ma "*hackerare*" il suo approccio psicologico e comportamentale. A differenza della guerra psicologica tradizionale o della semplice propaganda, la dimensione cognitiva sfrutta l'integrazione tra scienze comportamentali, neuroscienze e intelligenza artificiale per agire direttamente sui processi decisionali. Non si limita quindi ad influenzare "*cosa"* le persone pensano, ma mira a modificare il "*modo"* in cui il cervello elabora le informazioni. In questo particolare momento storico, stiamo già osservando come diversi Paesi stiano conducendo conflitti in cui all'uso delle armi si abbinano attività di condizio-

namento psicologico mediante l'utilizzo di quelle tecnologie digitali che utilizziamo quotidianamente.

Vale come esempio la Federazione Russa, che ha sviluppato un approccio sofisticato alla guerra cognitiva basato sulla creazione di confusione e ambiguità, una metodologia che si potrebbe definire con il termine "*disinformazione sistemica*". L'obiettivo di questa tecnica non è quello di convincere, bensì di destabilizzare. Nel caso delle elezioni statunitensi del 2016, le operazioni russe hanno dimostrato la capacità di utilizzare i *social media* come strumenti di influenza, attraverso la creazione di *account* falsi e la diffusione di contenuti polarizzanti che hanno reso possibile l'amplificazione delle divisioni interne. Nel conflitto ucraino, questa strategia è stata ulteriormente sviluppata. La narrativa russa ha cercato di giustificare l'intervento militare, mentre parallelamente venivano diffuse informazioni contraddittorie per generare incertezza. L'approccio russo si basa su un principio fondamentale: non imporre una verità alternativa, ma moltiplicare le versioni della realtà. L'obiettivo è creare confusione, erodere la fiducia e rendere impossibile distinguere tra vero e falso. Attraverso l'utilizzo di *bot*, *troll farm* e piattaforme digitali, attori legati all'intelligence russa hanno costruito reti di influenza capaci di raggiungere milioni di utenti. Le campagne non si limitano a diffondere contenuti falsi, ma sfruttano temi sensibili per amplificare divisioni preesistenti.

Nel conflitto in Ucraina, questa strategia è stata ulteriormente sviluppata. La narrativa russa ha cercato di legittimare l'intervento militare attraverso una rappresentazione distorta degli eventi, mentre parallelamente venivano condotte operazioni di disinformazione a livello globale. L'Ucraina rappresenta un caso opposto, in cui la dimensione cognitiva è stata utilizzata come strumento di difesa. Fin dalle prime fasi del conflitto, Kiev ha sviluppato una strategia comunicativa estremamente efficace, basata su trasparenza, velocità e autenticità. La figura del presidente Zelensky ha svolto un ruolo centrale, diventando simbolo della resistenza ucraina. I suoi interventi, spesso diffusi attraverso i social media, hanno contribuito a costruire una narrativa coerente e credibile.

La Cina ha invece preferito orientarsi verso lo sviluppo di un modello basato sul controllo centralizzato dell'informazione. La dottrina delle "*Three Warfares*"[1] rappresenta un esempio di integrazione tra dimensione psicologica, mediatica e legale, poiché consente di mantenere una

[1] La dottrina delle "*Three Warfares*" una strategia ufficiale adottata dalla Commissione Militare Centrale della Repubblica Popolare Cinese e dal Partito Comunista Cinese (PCC) nel 2003. Essa mira a integrare le operazioni politiche, psicologiche e di informa-

coerenza narrativa interna e di esercitare un'influenza crescente a livello globale. Nel contesto delle proteste di Hong Kong, Pechino ha utilizzato una combinazione di censura interna e campagne informative esterne per controllare la narrativa globale. Parallelamente, l'espansione delle infrastrutture digitali cinesi ha consentito al Paese di esercitare un'influenza crescente sui flussi informativi internazionali.

Altro esempio è quello dell'Iran, che utilizza una combinazione di operazioni *cyber* e campagne di disinformazione sfruttando dei "*leak* selettivi", o divulgazione intenzionale di notizie e dati riservati, confidenziali o sensibili, orchestrata per influenzare l'opinione pubblica. Nel corso degli ultimi anni l'Iran ha sviluppato una strategia che combina operazioni *cyber* e campagne di disinformazione. Gruppi legati ai Pasdaran hanno creato reti di siti e *account social* destinati a diffondere contenuti favorevoli agli interessi iraniani. In diversi casi, tali operazioni sono state accompagnate da attacchi informatici finalizzati all'esfiltrazione di dati sensibili, successivamente utilizzati per operazioni di *leakage* selettivo, con l'obiettivo di influenzare l'opinione pubblica.

Nel conflitto israelo-palestinese, la dimensione cognitiva ha assunto un ruolo centrale, poiché le operazioni militari sono accompagnate da campagne informative, volte a influenzare la percezione globale. Israele rappresenta un modello avanzato di integrazione tra operazioni militari, intelligence e comunicazione. Durante i conflitti con Hamas, la dimensione cognitiva è stata gestita in modo coordinato, attraverso una narrativa coerente e l'utilizzo di strumenti digitali per influenzare l'opinione pubblica internazionale. L'uso di tecnologie avanzate per l'analisi dei dati ha consentito di monitorare in tempo reale le dinamiche informative, adattando le strategie comunicative in funzione dell'evoluzione del contesto.

4. *Intelligenza artificiale, intelligence e dominio cognitivo: dalla raccolta informativa alla modellazione della realtà*

L'evoluzione della guerra cognitiva ha profondamente trasformato anche il ruolo dell'intelligence. Tradizionalmente orientata alla raccolta, analisi e interpretazione delle informazioni, essa si trova oggi a operare in un contesto in cui il confine tra informazione e percezione risulta sempre più sfumato. Non è più sufficiente conoscere i fatti: è necessa-

zione per conseguire obiettivi strategici, in particolare nel Mar Cinese Meridionale e nei confronti di Taiwan, senza la necessità di ricorrere a un conflitto armato aperto.

rio comprendere come tali fatti vengano percepiti, interpretati e narrati. In questo senso, l'intelligence contemporanea si configura sempre più come una disciplina orientata alla modellazione della realtà cognitiva. Le tradizionali discipline intelligence – HUMINT[2], SIGINT[3], IMINT[4] – si affiancano oggi a nuove dimensioni, tra cui la *Social Media Intelligence* (SOCMINT) e quella che sempre più frequentemente viene definita *Cognitive Intelligence* (COGINT). Quest'ultima non si limita a raccogliere dati, ma mira a comprendere i processi mentali e decisionali degli individui e delle collettività. L'analisi dei flussi informativi digitali consente di individuare *pattern* comportamentali, dinamiche di polarizzazione e segnali precoci di operazioni di influenza. In questo senso, l'intelligence assume una funzione predittiva, orientata non solo a descrivere il presente, ma ad anticipare evoluzioni future. Tuttavia, questa trasformazione introduce anche nuove criticità. L'utilizzo massivo di dati e algoritmi solleva questioni etiche e giuridiche, soprattutto nelle democrazie liberali, dove la tutela dei diritti individuali rappresenta un valore fondamentale. Uno degli sviluppi più significativi degli ultimi anni è rappresentato dall'emergere dell'*Open Source Intelligence* come strumento centrale nella competizione cognitiva. Ad esempio, nel conflitto tra Russia e Ucraina, le comunità OSINT hanno dimostrato la capacità di analizzare immagini satellitari, video e dati pubblici per ricostruire eventi in tempo reale, elemento che ha contribuito a contrastare la disinformazione e a costruire una narrativa basata su evidenze verificabili. Il ruolo dell'OSINT, di con-

[2] La HUMINT (*HUMan INTelligence*) è una branca dell'intelligence che raccoglie informazioni attraverso contatti umani diretti e fonti umane, distinguendosi dai metodi tecnologici come SIGINT o IMINT. Rappresenta la forma più antica di spionaggio, utilizzata per comprendere intenzioni, piani e tattiche avversarie, spesso classificata in attività aperte (Overt), sensibili o clandestine.

[3] Il termine SIGINT sta per *Signals Intelligence* (spionaggio di segnali elettromagnetici). È l'attività di raccolta e analisi di informazioni ottenute intercettando segnali elettronici. Si suddivide solitamente in due sottocategorie: COMINT (*Communications Intelligence)* ovvero l'intercettazione di comunicazioni tra persone, come chiamate telefoniche, email o messaggi radio; ELINT (*Electronic Intelligence*) che fa riferimento all'intercettazione di segnali elettronici che non sono comunicazioni dirette, come le emissioni dei radar o dei sistemi d'arma.

[4] IMINT è l'acronimo di *IMagery INTelligence* (intelligence d'immagine) e si riferisce alla disciplina dell'intelligence che consiste nella raccolta e nell'analisi di informazioni ottenute tramite la rappresentazione visiva di oggetti, persone o aree geografiche. Queste immagini vengono acquisite attraverso diversi sensori e supporti: fotografie aeree (da aerei o droni), immagini satellitari e sensori a terra, radar, sensori all'infrarosso, laser e apparati elettro-ottici.

seguenza, introduce una dinamica nuova: la democratizzazione dell'intelligence. Attori non statali, come analisti indipendenti e comunità online, diventano parte attiva nel processo di produzione della conoscenza, un fenomeno che rafforza la resilienza delle democrazie, ma al tempo stesso aumenta la complessità del sistema informativo, poiché la moltiplicazione delle fonti rende più difficile distinguere tra informazione affidabile e manipolazione.

Anche l'Intelligenza Artificiale (IA) sta assumendo un ruolo centrale e uno straordinario fattore di accelerazione della guerra cognitiva, poiché la sua capacità di generare contenuti realistici e analizzare dati consente di progettare e condurre operazioni altamente sofisticate ed efficaci. Se le piattaforme digitali rappresentano oggi l'infrastruttura principale attraverso cui si sviluppano le operazioni cognitive, gli algoritmi, che regolano la visibilità dei contenuti, possono svolgere un ruolo determinante nel definire ciò che viene percepito come rilevante. Questi sistemi sono progettati per massimizzare l'*engagement*, privilegiando contenuti emotivi e polarizzanti.

Le aree in cui l'IA può assumere particolare rilevanza sono:

- *Profilazione e micro-targeting psicometrico*. L'IA può analizzare enormi quantità di dati dai *social media* per creare profili psicologici dettagliati di intere popolazioni, agendo sulla vulnerabilità (individuando paure, desideri e pregiudizi specifici), e sul piano dell'azione (ad esempio, invia messaggi personalizzati che colpiscono il "*punto debole*" di ogni singolo utente, massimizzando le probabilità di cambiare la sua opinione o il suo comportamento).
- *Generazione di contenuti sintetici.* L'IA generativa permette di creare prove visive e testuali false ma indistinguibili dalla realtà come i *deepfake* (ad esempio, video o audio di leader politici che dicono cose mai dette per scatenare rivolte o crolli finanziari), e generazione massiva di articoli di notizie, *post* e commenti che simulano un consenso popolare inesistente (*astroturfing*), soffocando le voci reali in un oceano di "*rumor*" sintetico.
- *Automazione del discorso (bot intelligenti).* A differenza dei vecchi "*bot*"[5] che ripetevano frasi fatte, i moderni LLM[6] (*Large Lan-*

[5] In ambito informatico, il termine *bot* (abbreviazione di "*robot*") si riferisce a un *software* progettato per eseguire compiti automatizzati e ripetitivi su internet molto più velocemente di quanto farebbe un essere umano.

[6] I *Large Language Models* (LLM) sono sistemi di intelligenza artificiale avanzata

guage Models) possono interagire in modo fluido e convincente, poiché possono partecipare a discussioni online, rispondere a obiezioni in tempo reale e manipolare emotivamente le persone all'interno di gruppi chiusi o *forum* e gestire migliaia di conversazioni simultanee, dando l'impressione che una certa idea sia condivisa dalla maggioranza.

- *Sfruttamento dei bias cognitivi tramite algoritmi.* Gli "*algoritmi di raccomandazione*" delle piattaforme *social* sono già progettati per massimizzare l'*engagement*, spesso favorendo contenuti polarizzanti. L'IA può essere usata per "*ingannare*" gli algoritmi di distribuzione, spingendo contenuti divisivi nei *feed* di persone indecise (*echo chambers*), ma può essere utilizzata anche per bombardare l'utente con versioni contrastanti della realtà, inducendolo in uno stato di confusione e apatia che lo porta a non credere più a nulla (nichilismo informativo).

Mentre la propaganda tradizionale poteva essere identificata come uno strumento che adottava la tecnica del "*bombardamento a tappeto*", l'IA permette un attacco chirurgico, ovverosia colpisce la mente della vittima esattamente dove è più fragile, spesso senza che questa si accorga nemmeno di essere sotto attacco. Di conseguenza, la disinformazione tende a diffondersi più rapidamente rispetto alle informazioni verificate. La guerra cognitiva sfrutta queste dinamiche, intervenendo sui meccanismi di amplificazione attraverso l'utilizzo di *bot*, *account* coordinati e tecniche di manipolazione algoritmica. Il controllo delle piattaforme diventa quindi un elemento strategico. Le grandi aziende tecnologiche si trovano in una posizione ambigua, tra responsabilità sociale e interessi economici.

Anche l'avvento dei *deepfake*[7] rappresenta una delle innovazioni più dirompenti nel campo della guerra cognitiva. La possibilità di generare contenuti audiovisivi altamente realistici mette in discussione il concetto stesso di evidenza. Se in passato, immagini e video costituivano prove

progettati per comprendere, analizzare e generare testo in linguaggio naturale. Rappresentano l'evoluzione dei modelli linguistici tradizionali, potenziati da una scala massiccia di dati e parametri.

[7] Il *deepfake* è una tecnica per la sintesi dell'immagine umana fondata sull'intelligenza artificiale, usata per combinare e sovrapporre immagini e video esistenti con video o immagini originali con una tecnica di apprendimento automatico, conosciuta come rete antagonista generativa.

difficilmente contestabili, attualmente ogni contenuto può essere manipolato, generando una condizione di incertezza generalizzata. Questa trasformazione produce un effetto paradossale: non solo è possibile diffondere contenuti falsi, ma diventa anche possibile negare la veridicità di contenuti autentici. Questo fenomeno, noto come "*liar's dividend*", rappresenta una delle principali minacce per la stabilità informativa e le piattaforme di intelligenza artificiale sono in grado di analizzare enormi quantità di dati per costruire profili psicologici dettagliati che possono essere utilizzati per personalizzare i messaggi in modo estremamente preciso. La tecnica del "*micro-targeting*"[8] rappresenta una delle tecniche più efficaci della guerra cognitiva contemporanea perché, a differenza delle campagne tradizionali che si rivolgono a un pubblico ampio, essa consente di veicolare contenuti specificatamente progettati per influenzare particolari individui o comunità. La combinazione tra dati comportamentali e modelli predittivi consente di identificare vulnerabilità cognitive e sfruttarle in modo mirato, e ciò consente di comprendere come le guerre cognitive si vadano a collocare al confine tra neuroscienze e tecnologia. Va evidenziato che la possibilità di influenzare direttamente i processi cognitivi attraverso stimoli mirati apre scenari inediti, e sebbene molte di queste applicazioni siano ancora in fase sperimentale, esse indicano una direzione chiara: la progressiva integrazione tra tecnologia e mente umana.

5. Verso un modello di difesa multi-dominio e sicurezza integrata

Gli scenari futuri evidenziano come la difesa non possa più essere vista con un approccio di "*compartimentazione*". Il futuro della difesa viaggia inequivocabilmente verso il concetto di Difesa Multi-Dominio (MDO), dove le forze terrestri, navali ed aeree operano in simbiosi costante con le capacità *cyber* e spaziali. Lo spazio diventa il "sistema nervoso" della difesa, poiché senza una governance spaziale solida, le comunicazioni e la navigazione GPS (essenziali per la vita civile e militare) sono vulnerabili. Un altro pilastro fondamentale si basa sulla difesa civile non armata. La *governance* del futuro dovrà investire nella "*resilienza cognitiva*" della popolazione per contrastare le minacce ibride, come le campagne di disin-

[8] Il *microtargeting* è una strategia di marketing e comunicazione che utilizza l'analisi di grandi quantità di dati personali (*Big Data*) per identificare segmenti di pubblico estremamente specifici e inviare loro messaggi iper-personalizzati

formazione volte a destabilizzare le istituzioni democratiche dall'interno. In un mondo sempre più caratterizzato dal "tecno-nazionalismo" di Stati Uniti e Cina, l'Europa deve delineare un modello di governance basato sulla sovranità strategica. Ciò implica necessariamente:

Indipendenza tecnologica. Ridurre la dipendenza da catene di approvvigionamento critiche (semiconduttori, terre rare).

Difesa comune. L'evoluzione della Cooperazione Strutturata Permanente (PESCO) verso un'integrazione operativa reale, superando le diversità di vedute, soprattutto sul piano geopolitico, dei singoli paesi e la frammentazione dei singoli eserciti nazionali.

Standardizzazione dei dati. La creazione di un *Data Governance Framework* europeo che permetta la libera circolazione dei dati sicuri tra gli alleati, garantendo al contempo la *privacy* dei cittadini.

Il concetto di difesa sta evolvendo da una logica basata sul presidio dei confini fisici a una focalizzata sulla protezione delle interconnessioni vitali. Nel prossimo decennio, la sovranità di uno Stato si misurerà sulla capacità di governare e proteggere i "*Global Commons*" (cyberspazio, spazio extra-atmosferico e cavi sottomarini), di conseguenza la *governance* non sarà più un esercizio statico di amministrazione, ma una funzione dinamica di resilienza sistemica, capace di assorbire shock tecnologici, energetici e informativi in tempo reale. L'integrazione dell'intelligenza artificiale nei processi di comando e controllo (C2) sta portando alla nascita della cosiddetta "*Governance* Algoritmica" incentrata su:

Accelerazione del Ciclo OODA[9]*.* L'obiettivo della Strategia della Difesa IA 2026[10] è garantire la superiorità decisionale riducendo drasticamente i tempi tra l'osservazione di una minaccia e l'azione di risposta.

IA Agentica e Autonoma. Prevede il passaggio da strumenti di analisi a "*agenti*"[11] capaci di operare in autonomia per il triage delle minacce informatiche o la gestione della logistica complessa, con tassi di precisione superiori al 98%.

[9] Il ciclo OODA (Osservare, Orientare, Decidere, Agire) è un modello decisionale rapido sviluppato dal colonnello John Boyd, pilota USAF. È una strategia militare focalizzata sulla velocità: superare l'avversario completando il ciclo più velocemente, disorientandolo e forzandolo a reagire alle proprie azioni.

[10] Strategia della difesa in materia di intelligenza-artificiale, in difesa.it

[11] L'IA agentica (Agentic AI) rappresenta un'evoluzione dell'intelligenza artificiale, passando dalla generazione di contenuti all'azione autonoma. Questi sistemi intelligenti pianificano, decidono e utilizzano strumenti per completare attività complesse multi-fase verso un obiettivo specifico con supervisione umana minima, distinguendosi per proattività, memoria e capacità di adattamento

Regolamentazione e Etica. Con l'entrata in vigore delle norme di governance dell'IA (agosto 2025), la sfida sarà bilanciare l'automazione con il controllo umano (*human-in-the-loop*), specialmente per i sistemi ad alto rischio.

Per quanto concerne le forze armate, dal 2030 opereranno in un ambiente dove terra, mare, aria, spazio e cyber sono fusi in un'unica architettura digitale basata su:

Sincronizzazione in Real-Time. La NATO sta definendo quadri dottrinali per orchestrare attività militari e non militari simultaneamente, generando effetti convergenti istantanei.

Il Dominio Spaziale. Lo spazio diventa il pilastro della navigazione e comunicazione. Progetti come l'European Space Shield (previsto dalla Roadmap 2030 dell'UE) mirano a proteggere le infrastrutture satellitari da attacchi fisici o *cyber.*

Quantum Sensing e Navigazione. Per contrastare il jamming (disturbo del segnale), si stanno sviluppando sensori quantistici che permettono la navigazione precisa anche in assenza di segnale GPS (*GPS-denied environments*).

L'Unione Europea ha tracciato un percorso verso l'autonomia strategica attraverso documenti chiave come il Libro Bianco *Defence Readiness 2030* che prevede: *ReArm Europe,* ovvero un piano ambizioso per stimolare la produzione industriale della difesa su vasta scala, riducendo le dipendenze esterne; *iniziative flagship,* la creazione di scudi aerei e droni comuni (*European Air Shield, Drone Defence Initiative*) per uniformare la risposta alle minacce asimmetriche; *integrazione civile-militare,* basata sul trasferimento tecnologico tra settore militare e civile sarà essenziale per lo sviluppo di scuole e ospedali digitalmente protetti.

In definitiva, i modelli di difesa e governance del futuro saranno definiti dalla loro versatilità e agilità di adattamento agli scenari che saranno in grado di esprimere nel tempo. Le strutture gerarchiche e rigide del passato stanno lasciando il posto a modelli a rete, capaci di riconfigurarsi rapidamente di fronte a minacce asimmetriche. La sfida non sarà più solo "*vincere*" un conflitto, ma mantenere la stabilità di un sistema globale interconnesso in cui il collasso di un nodo (economico, digitale o ambientale) può compromettere l'intera struttura. Il futuro della guerra cognitiva sarà caratterizzato da una crescente integrazione tra intelligenza artificiale, realtà virtuale e ambienti digitali immersivi. Il metaverso, in particolare, potrebbe diventare un nuovo spazio di competizione, in cui le operazioni cognitive assumono forme ancora più sofisticate.

6. Conclusioni

La guerra cognitiva rappresenta una sfida esistenziale per le democrazie liberali, poiché essa colpisce il cuore del sistema, mettendo in discussione la fiducia, la coesione e la capacità decisionale. La risposta non può essere la rinuncia ai valori fondamentali, ma il loro rafforzamento. Le democrazie devono sviluppare strumenti di difesa che siano coerenti con i principi di libertà e pluralismo. In ultima analisi, la guerra cognitiva non è soltanto una questione di sicurezza, ma di identità. Essa richiede una riflessione profonda sul significato stesso della democrazia nel XXI secolo e rappresenta una sfida esistenziale per le democrazie liberali, poiché mette in discussione non solo la sicurezza, ma la natura stessa del sistema democratico. La risposta non può essere la rinuncia ai propri valori, ma il loro rafforzamento. In questo senso, la resilienza cognitiva diventa il fondamento della sicurezza nel XXI secolo.

ELEMENTI DI RIFLESSIONE PER UNA LETTURA NORMATIVA DELLA GUERRA COGNITIVA

Claudia Capasso[*]

SOMMARIO: 1. La mente quale dominio del conflitto. – 2. L'evoluzione concettuale dalla guerra psicologica alla guerra cognitiva. – 3. Una prima proposta di lettura normativa del fenomeno. – 3.1. Il livello costituzionale: guerra cognitiva e ordinamento italiano. – 3.2. L'ordinamento europeo. – 3.3 Il quadro internazionale. – 4. Riflessioni conclusive.

1. *La mente quale dominio del conflitto*

Il conflitto, persino nella sua accezione tradizionale, ha pressoché sempre contenuto una dimensione nascosta, invisibile ai più. Accanto agli scontri più fisici, concreti quanto i materiali e la carne che costituiscono infrastrutture e individui, esso si è corredato di una battaglia per il controllo della percezione[1]. Cosa fosse accaduto, chi ne fosse il responsabile, quale fosse il futuro possibile o, meglio ancora, desiderabile. Ciò che sembrerebbe radicalmente mutare nell'epoca contemporanea non è dunque la presenza di una simile dimensione, ovverosia il terreno cognitivo oggetto del presente volume collettaneo, bensì la sua centralità strategica e la sofisticazione degli strumenti impiegati per coltivarla.

Del resto, l'accesso sostanzialmente illimitato all'informazione, lungi da produrre una società più consapevole, ha invece reso la verità stessa un terreno conteso. L'iperproduzione di contenuti, la c.d. "infodemia"[2], non solo non semplifica l'accesso alla conoscenza da parte dell'individuo, ma lo complica, annegando l'informazione rilevante in un flusso caotico e difficilmente accertabile, in cui il falso e il vero si confondo-

[*] Ricercatrice in Dritto costituzionale e pubblico nell'Università degli Studi della Tuscia.

[1] Sul ruolo storico della dimensione psicologica nei conflitti, a partire dagli strateghi militari cinesi del 2070 a.C. fino a Sun Tzu, cfr. Y. CHUNG, *Allusion, reasoning and luring in Chinese psychological warfare*, in *International Affairs*, v. 97, n. 4, 2021.

[2] Dal vocabolario Treccani *online*, si tratta della «circolazione di una quantità eccessiva di informazioni, talvolta non vagliate con accuratezza, che rendono difficile orientarsi su un determinato argomento per la difficoltà di individuare fonti affidabili».

no con simile credibilità[3]. La manipolazione dell'informazione, dunque, non richiede più una mera soppressione della verità, poiché è sufficiente saturare lo spazio cognitivo con una mole insostenibile di alternative plausibili per giungere all'esito destabilizzante sperato. I *media,* nuclei di questa trasformazione, da tradizionali veicoli di notizie si evolvono sotto la spinta del digitale. Nascono piattaforme ibride che, pur rispondendo alle logiche del diritto privato, sono tanto necessarie alla formazione dell'opinione pubblica da divenire, *de facto*, irriducibili piazze virtuali[4]. È soprattutto in questi luoghi (o *non-luoghi*, come il cyberspazio di irtiana memoria[5]) che le logiche dell'informazione e quelle della disinformazione si intrecciano in modo tale da rendere arduo distinguere l'una dall'altra, persino agli sguardi più attenti e istruiti[6]. Come già le prime teorie dei *media studies* avevano intuito, fin dall'*Agenda-setting theory* di McCombs e Shaw alla *Cultivation theory* di Gerbner, ma anche alla *Social learning theory* di Bandura, i *media* non si limitano a rispecchiare fedelmente la realtà. Essi contribuiscono attivamente a costruirla., selezionando ciò che merita attenzione e modellando le lenti attraverso cui l'opinione pubblica interpreta il mondo davanti a sé[7]. Una capacità di orientare (e disorientare) la percezione collettiva che, come è noto, non è esente da applicazioni belliche.

D'altronde, il contesto del conflitto è per sua natura terreno fertile per la disinformazione; l'emotività, la paura e la tensione collettiva tipiche dello stato di ostilità indeboliscono la capacità critica, rendendo le collettività, ma anche i singoli individui, più permeabili alla manipolazione. Eppure, come si è detto, la novità non risiede nel ricorso alla menzogna,

[3] M. CALIGIURI, A. PAGANI, *Disinformare: ecco l'arma. L'emergenza educativa e democratica del nostro tempo*, Rubbettino, Soveria Mannelli, 2024, p. 66.

[4] Si consenta il riferimento a A. STERPA, C. CAPASSO, *Empty squares, empty billboards, empty dashboards, and semi-empty ballots: the "political" European elections in the global election year*, in T. CERRUTI, F. SAVASATANO (a cura di), *The European Parliament Elections in 2024,* Giappichelli, Torino, 2024.

[5] N. IRTI (2007), voce *Geodiritto*, in *Enciclopedia Italiana – VII Appendice*, disponibile su www.treccani.it.

[6] Cfr., *infra,* il contributo di Silvia Sassi, *La sfida della disinformazione nell'ecosistema digitale europeo*. Ma si v. anche ID., *Il ruolo della disinformazione nelle moderne strategie di guerra*, in E.A. IMPARATO, G. GIORGINI PIGNATIELLO (a cura di), *La libertà di espressione nel diritto comparato tra stato di diritto e stati di emergenza*, Giappichelli, Torino, 2024, *passim.*

[7] M. GOMBAR, *Algorithmic Manipulation and Information Science: Media Theories and Cognitive Warfare in Strategic Communication*, in *European Journal of Communication and Media Studies*, v. 4, n. 2, 2025, p. 1 e ss.

pratica tanto antica quanto lo stesso concetto di guerra poiché capace di destabilizzare l'avversario senza ricorrere alla forza fisica e, pertanto, senza i costi umani e politici che essa comporta; la trasformazione si insidia nel fatto che essa sia divenuta tanto strutturale e dirompente da rendere la mente, prima ancora che il campo, teatro di conflitto[8].

Nella appena delineata cornice concettuale possiamo dunque introdurre le c.d. minacce ibride, azioni condotte «da attori statali o non statali, il cui obiettivo è quello di minare o danneggiare un *target* ricorrendo a mezzi militari e non militari, sia palesi sia occulti»[9]. In un contesto internazionale sempre più caratterizzato da dinamiche conflittuali non convenzionali, le società democratiche si trovano particolarmente esposte a questo genere di minacce; sfruttando l'apertura fisiologica dei sistemi democratici, fondati sulla libertà di espressione, sulla pluralità informativa e sull'accesso libero allo spazio digitale, vi si possono iniettare più facilmente contenuti manipolatori o deliberatamente falsi. Al contrario, i regimi autoritari, «chiusi nelle loro monadi, dove lo spazio digitale coincide con quello fisico»[10] possono impiegare con maggiore efficacia la disinformazione come strumento sistemico di potere. In tali regimi l'adulterazione dell'informazione non è più un effetto collaterale, bensì parte integrante della strategia del governo, il quale non la utilizza solamente per mascherare decisioni impopolari o controverse in una popolazione non del tutto manipolata come talvolta accade nelle democrazie, ma anche come strumento finalizzato al «completo riordinamento della tessitura fattuale» per costruire una realtà alternativa coerente con quella ufficiale del potere[11]. Questo processo potrebbe trovare una possibile interpretazione anche sul piano neurologico. Secondo il modello del *predictive coding*, il sistema nervoso tenderebbe a generare continuamente delle previsioni sulla realtà, che vengono poi confermate oppure modificate sulla base degli stimoli sensoriali in arrivo[12]. Va però sottolineato che, nonostante i progressi delle neuroscienze, la comprensione del funzionamento del cervello resta ancora parziale e in molti aspetti incerta; di conseguenza, è

[8] Cfr. S. Sassi, *Il ruolo della disinformazione nelle moderne strategie di guerra*, cit.

[9] Così il Centro europeo di eccellenza per la lotta contro le minacce ibride, https://www.hybridcoe.fi/.

[10] S. Sassi, *Il ruolo della disinformazione nelle moderne strategie di guerra*, cit., p. 239.

[11] *Ibidem*. La citazione «completo riordinamento della tessitura fattuale», così come riportato da Silvia Sassi, è di V. Sorrentino, *Il segreto e la menzogna in politica: Hannah Arendt*, in *Studium*, n. 6, 1995, p. 894.

[12] Stato Maggiore della Difesa, *Cognitive Warfare. La competizione nella dimensione cognitiva*, 2023, p. 38.

consigliabile considerare ciò che segue quale chiave di lettura plausibile, ma non definitiva[13]. Secondo detto modello, chiunque voglia manipolare l'informazione non dovrebbe necessariamente impiantare credenze false, poiché sarebbe sufficiente interferire con il meccanismo anticipatorio, saturandolo di stimoli incoerenti o orientandolo verso previsioni favorevoli agli obiettivi dell'operazione[14]. In questo senso, la disinformazione contemporanea non costituirebbe soltanto un problema di contenuti, ma di architettura cognitiva, agendo sui modi in cui il cervello costruisce la realtà, prima ancora che sulla sua percezione della realtà. Ne consegue un ruolo ancor più preminente dell'opinione pubblica nella dinamica del conflitto. Come è noto, se la percezione collettiva ritiene che i propri *leader* siano nel torto, diviene estremamente complesso sostenere uno sforzo bellico efficace, venendo infatti meno il consenso necessario alla legittimazione dell'azione militare[15]. Non è dunque casuale che la manipolazione cognitiva si rivolga sempre più non ai soldati nemici, ma alle popolazioni civili e alle loro istituzioni; esse sono divenute, del resto, un vero e proprio centro di gravità strategico.

In sintesi, la riflessione alla quale viene chiamato il giurista è duplice. Da un lato, quella della qualificazione giuridica del fenomeno della guerra cognitiva; ciò significa capire *se* e *quando* un atto ad essa riconducibile possa costituire un illecito sul piano internazionale, ma anche quali siano i confini di costituzionalità dello stesso. Dall'altro, quella della risposta normativa; vale a dire, comprendere quale strumentario giuridico sia disponibile e adeguato a fronteggiarla, evitando che la cura possa rivelarsi peggiore del male da curare, comprimendo le stesse libertà che si intende proteggere. Il presente contributo intende muovere un primo passo in questa direzione, pur non avendo pretese di esaustività; ci si confronta, infatti, con fenomeni in trasformazione nel dominio cognitivo e informativo, la cui evoluzione, anche in relazione allo sviluppo dell'intelligenza artificiale, presenta profili di significativa complessità e incertezza.

2. *L'evoluzione concettuale dalla guerra psicologica alla guerra cognitiva*

Prima di affrontare le questioni di natura normativa, appare opportuno definire con maggiore precisione l'oggetto dell'analisi. Il concetto

[13] Cfr. G. MAIRA, *Il cervello è più grande del cielo*, Solferino, Milano, 2019.
[14] Stato Maggiore della Difesa, *Cognitive Warfare*, cit., p. 38.
[15] M. CALIGIURI, A. PAGANI, *Disinformare: ecco l'arma*, cit., p. 13.

di guerra cognitiva, infatti, non si configura come una nozione isolata o estemporanea, bensì come l'esito di un'annosa evoluzione teorica che trae origine dalle pratiche di guerra psicologica del Novecento e si sviluppa progressivamente attraverso l'integrazione delle tecnologie digitali, fino ad assumere caratteristiche qualitativamente nuove. In questa sede, una simile ricostruzione ha una funzione prevalentemente introduttiva e di inquadramento concettuale, volta a delineare i presupposti necessari per la successiva trattazione. Un'analisi più approfondita, tecnica e specialistica delle dinamiche proprie della guerra cognitiva sarà infatti oggetto di altri contributi presenti nel volume, ai quali si rinvia per un'esposizione più articolata e competente del tema.

Già in epoche remote è possibile rintracciare una precoce consapevolezza della rilevanza della dimensione psicologica nei conflitti. Le tradizioni strategiche cinesi, sin dal II millennio a.C., valorizzavano infatti l'idea di un attacco diretto alla sfera interiore dell'avversario, concepito come una forma di «guerra di attacco al cuore»; una prospettiva che troverà poi una sistematizzazione più compiuta nel pensiero di Sun Tzu, il quale sottolineava la centralità dell'inganno, della disinformazione e della manipolazione delle percezioni quale via privilegiata per conseguire la vittoria[16]. È, tuttavia, nel contesto novecentesco che dette intuizioni destano l'interesse accademico. Negli anni Venti del Novecento, J. F. C. Fuller coniò l'espressione "guerra psicologica", in cui il conflitto tende progressivamente a svincolarsi dall'impiego diretto della forza militare e dal controllo territoriale, per configurarsi come uno scontro eminentemente immateriale, in cui l'obiettivo principale diviene l'erosione della capacità cognitiva e morale dell'avversario. In questo quadro, la vittoria non deriva tanto dalla distruzione fisica, quanto dalla disgregazione della volontà collettiva, ottenuta con costi umani e materiali significativamente ridotti[17].

È dunque in questa cornice che si colloca il concetto di guerra cognitiva, oggi definita dallo Stato Maggiore della Difesa come «un'operazione multidominio (o parte di essa) che impiega mezzi, azioni e strumenti attraverso le connessioni tra i domini classici – terrestre, aereo, navale –, i domini spazio e *cyber*, l'ambiente informativo e lo spettro elettromagnetico, influenzando il comportamento umano e generando effetti nella dimensione cognitiva, con l'obiettivo di ottenere un vantaggio sull'avver-

[16] Y. Chung, *Allusion, reasoning and luring in Chinese psychological warfare*, cit.

[17] S. Narula, *Psychological Operations (PSYOPs): A Conceptual Overview*, in *Strategic Analysis*, v. 28, n. 1, 2004 p. 178.

sario»[18]. In termini più sintetici, essa può essere intesa come l'impiego sistematico di tecnologie e strategie volte ad alterare i processi mentali del *target*, spesso in modo non percepito, incidendo sulla capacità di interpretare la realtà e di assumere decisioni autonome[19]. A differenza delle forme tradizionali di guerra informativa, la guerra cognitiva non si limita a intervenire sul contenuto dell'informazione, ma mira direttamente ai meccanismi attraverso cui essa viene elaborata dal cervello umano; per queste ragioni, l'effetto cognitivo non rappresenta una mera conseguenza indiretta dell'azione, bensì il suo fine strategico primario. Essa si configura dunque come un'estensione delle minacce ibride, integrando strumenti cibernetici e tecniche di influenza psicologica per sfruttare *bias* cognitivi, generare distorsioni percettive e condizionare i processi decisionali individuali e collettivi[20]. Daniel Kahneman, nel suo celebre studio sui meccanismi decisionali umani, ha teorizzato un duplice sistema del pensiero umano, di cui uno veloce, intuitivo e soggetto a *bias* e uno lento, analitico e deliberato[21]. La guerra cognitiva agirebbe prevalentemente sul primo sistema, sfruttando euristiche e scorciatoie cognitive per orientare percezioni e decisioni prima ancora che il pensiero critico possa intervenire. Questa dimensione è oggi pienamente riconosciuta dagli apparati militari, tanto che la guerra cognitiva potrebbe essere qualificata come un attacco alla razionalità stessa e non semplicemente alla correttezza delle informazioni circolanti[22].

Logicamente, l'evoluzione tecnologica contribuisce in modo significativo a rafforzare le dinamiche descritte. Un esempio particolarmente efficace è rappresentato dallo sviluppo di interfacce neurali, che consentono forme di comunicazione diretta tra cervello umano e dispositivi digitali. Sebbene possano offrire potenzialità operative considerevoli, esse introducono al contempo nuove vulnerabilità, esponendo l'operatore al rischio di interferenze esterne, quali l'iniezione di *malware* o la manipo-

[18] STATO MAGGIORE DELLA DIFESA, *Cognitive Warfare. La competizione nella dimensione cognitiva*, cit., p. III.

[19] B. CLAVERIE, F. DU CLUZEL, *"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare*, in B. CLAVERIE, B. PREBOT, N. BUCHLER, F. DU CLUZEL (a cura di), *Cognitive Warfare: The Future of Cognitive Dominance*, NATO Collaboration Support Office, 2022.

[20] *Ibidem*.

[21] D. KAHNEMAN, *Thinking, fast and slow,* Farrar, Straus and Giroux, New York, *passim.*

[22] *Cognitive Warfare: Strenghtening and Defending the Mind*, pubblicato il 5 aprile 2023 su www.act.nato.int.

lazione dei segnali sensoriali. Emerge, infatti, la prospettiva del cosiddetto "*hacking cognitivo*", ossia la possibilità di alterare le rappresentazioni mentali del soggetto attraverso l'induzione di percezioni distorte della realtà. Intervenendo sui precedentemente citati meccanismi anticipatori del cervello, è possibile generare un disallineamento tra percezione e realtà oggettiva, con effetti potenzialmente rilevanti tanto sul piano operativo quanto su quello psicofisico[23]. Un recente sviluppo, di notevole rilevanza per la trattazione, è l'evoluzione cinese verso le cosiddette *Cognitive Domain Operations (CDO),* che combinano la tradizionale guerra psicologica con le operazioni *cyber* per condizionare i comportamenti e i processi decisionali dell'avversario. Questo approccio è stato monitorato con crescente attenzione dalla comunità intelligence statunitense, che in alcune valutazioni della minaccia ha documentato l'evoluzione della dottrina militare cinese in questa direzione[24]. La dottrina cinese delle "Tre Guerre" (psicologica, dell'opinione pubblica e giuridica) ne rappresenta il quadro concettuale di riferimento, attribuendo centralità crescente al dominio cognitivo come capacità di influenzare l'avversario attraverso mezzi intangibili quali la coesione sociale, il morale e la percezione collettiva[25]. Nel 2019, la Cina ha introdotto ufficialmente nel Libro Bianco della Difesa il concetto di «Guerra Intelligente», puntando al «dominio mentale» come nucleo strategico delle nuove forme di conflitto, anche attraverso l'uso di piattaforme digitali come Tiktok per influenzare l'opinione pubblica, sfruttare i dati degli utenti e creare *bias* cognitivi[26].

Per comprendere appieno la portata della guerra cognitiva, è infine necessario considerare il suo rapporto con le operazioni psicologiche (*PsyOps*), tradizionalmente definite come attività pianificate volte a influenzare percezioni, atteggiamenti e comportamenti di specifici pubbli-

[23] Stato Maggiore della Difesa, *Cognitive Warfare. La competizione nella dimensione cognitiva*, cit., pp. 35 e ss.

[24] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, pubblicato il 5 febbraio 2024.

[25] M. Raska, *Hybrid Warfare with Chinese Characteristics*, in *RSIS Commentary*, 2015. Il concetto delle "Tre Guerre", approvato nel 2003 dalla Commissione Militare Centrale (CMC), ha fornito il quadro concettuale guida per le operazioni informative dell'Esercito Popolare di Liberazione (PLA). Esso si basa su tre strategie tra loro complementari: operazioni psicologiche strategiche coordinate, manipolazione mediatica, sia palese che occulta, e guerra giuridica, finalizzata a influenzare le percezioni, le politiche di difesa e le strategie dei Paesi bersaglio. Queste componenti agiscono sinergicamente per creare un effetto cumulativo di pressione cognitiva sull'avversario

[26] I. Pujol, Q. Dinh, *The Battle for the Mind: Understanding and Addressing Cognitive Warfare and its Enabling Technologies*, IE CGC, 2024, p. 7 e ss.

ci[27]. Una distinzione fondamentale tra *PsyOps* e guerra cognitiva riguarda il *target* e l'approccio comunicativo, in quanto le operazioni psicologiche si rivolgono prevalentemente a soggetti ostili in contesti bellici, mentre la guerra cognitiva agisce anche in tempo di pace, colpendo l'intera infrastruttura sociale, civile e istituzionale di uno Stato[28]. Inoltre, se le *PsyOps* si basano su contenuti attribuiti apertamente al mittente ("bianchi"), attribuiti a terzi ("grigi") o attribuiti falsamente a fonti ostili ("neri"), la guerra cognitiva predilige i contenuti "grigi", sfruttandone l'elevato grado di verosimiglianza e negabilità per massimizzare l'effetto manipolativo[29]. Una distinzione ulteriore riguarda il *target* delle operazioni in quanto, mentre le *PsyOps* si rivolgono tradizionalmente a pubblici militari o a gruppi ostili, la guerra cognitiva, come detto poc'anzi, tende a colpire infrastrutture sociali e istituzioni civili, mirando a destabilizzare la coesione interna di una nazione. Nonostante ciò, varie definizioni ufficiali di *PsyOps* includono anche *target* neutrali o amichevoli, suggerendo una sovrapposizione operativa che giustifica l'inclusione delle operazioni psicologiche nel dominio più ampio della guerra cognitiva[30]. Alla luce di queste considerazioni, possiamo considerare la guerra cognitiva come un concetto ombrello, capace di inglobare al suo interno le operazioni psicologiche, la guerra informativa e altri strumenti di influenza, riconfigurandoli in chiave contemporanea[31]. In sintesi, pur condividendo finalità analoghe, le due nozioni divergono sotto diversi profili. Le *PsyOps* operano prevalentemente in contesti bellici e si rivolgono a *target* specifici, mentre la guerra cognitiva si estende anche al tempo di pace e coinvolge l'intero tessuto sociale e istituzionale. Inoltre, essa privilegia forme di comunicazione indiretta e difficilmente attribuibili, sfruttando contenuti ambigui e verosimili per massimizzare l'efficacia manipolativa. Il lettore avrà forse notato il potenziale paradosso nell'uso del termine "guerra" anche in tempi di pace. È infatti opportuno precisare che l'espressione

[27] «Attività psicologiche pianificate che utilizzano metodi di comunicazione e altri mezzi diretti a un pubblico approvato per influenzare le percezioni, gli atteggiamenti e i comportamenti, influendo sul raggiungimento di obiettivi politici e militari», Strategic Communications Centre of Excellence della NATO, www.stratcomcoe.org

[28] F. IBRAHIM, S. RHODE, M. DASEKING, *A systematic review of cognitive and psychological warfare*, in *The defence horizon journal*, 2023.

[29] A. BERNAL, C. CARTER, I. SING, K. CAO, O. MADREPERLA, *Cognitive Warfare. An attack on truth and thought*, NATO Innovation Hub, 2020, p. 7.

[30] F. IBRAHIM, S. RHODE, M. DASEKING, *A systematic review of cognitive and psychological warfare*, cit.

[31] *Ibidem.*

"guerra cognitiva" può indurre, soprattutto in lingua italiana, a una lettura immediatamente riconducibile alla nozione tradizionale di "guerra" quale conflitto armato formalmente dichiarato. Tuttavia, essa costituisce la traduzione dell'inglese "*cognitive warfare*"; il termine "*warfare*" presenta un'accezione più ampia e sfumata rispetto a "*war*", in quanto non si riferisce necessariamente a uno stato giuridico di guerra, bensì all'insieme delle pratiche, strategie e modalità operative attraverso cui il conflitto viene condotto, anche al di sotto della soglia della violenza armata. Ciò significa che la guerra cognitiva non coincide necessariamente con la guerra in senso stretto, ma designa piuttosto una forma di competizione strategica continua, che può dispiegarsi tanto in tempo di pace quanto in contesti di crisi, incidendo in modo pervasivo sulla dimensione cognitiva degli individui e delle collettività.

3. Una prima proposta di lettura normativa del fenomeno

L'evoluzione teorica sin qui ripercorsa consente di comprendere perché la guerra cognitiva ponga al giurista sfide qualitativamente diverse rispetto alle forme di conflitto tradizionali e, forse, persino rispetto alla guerra cibernetica. Essa non distrugge infrastrutture, non viola frontiere fisiche, non produce vittime immediatamente riconoscibili come tali, bensì agisce in profondità, riscrivendo le premesse cognitive su cui si fondano il consenso democratico, la fiducia nelle istituzioni e la coesione sociale. È precisamente questa invisibilità strutturale, e dunque non soltanto la novità tecnologica, a rendere urgente e insieme complesso il compito di una sua lettura normativa. Le attività di influenza cognitiva, intese come interventi finalizzati a orientare percezioni, emozioni e decisioni attraverso la manipolazione dell'informazione e l'impiego di tecnologie neuro-psicologiche, interpellano almeno tre livelli di analisi: quello costituzionale, quello europeo e quello internazionale. Ciascuno di essi offre strumenti parziali; nessuno, allo stato attuale, sembrerebbe fornire una risposta esaustiva.

3.1 Il livello costituzionale: guerra cognitiva e ordinamento italiano

Il primo nodo interpretativo riguarda la collocazione della guerra cognitiva all'interno del quadro costituzionale italiano. Non si può non iniziare la riflessione dall'art. 11 Cost., secondo cui «*l'Italia ripudia la guerra come strumento di offesa alla libertà degli altri popoli e come mezzo*

di risoluzione delle controversie internazionali», letto in combinato disposto con l'art. 52 Cost., che sancisce il dovere inderogabile del cittadino di difesa della Patria[32]. La questione che si pone è se la guerra cognitiva, in questo caso al pari di quella cibernetica, con cui condivide la natura non convenzionale e l'uso di strumenti digitali, possa essere ricondotta alla nozione di «guerra» ai sensi dell'art. 11, oppure se le operazioni difensive in questo dominio siano sussumibili nell'obbligo di difesa di cui all'art. 52.

Come noto, le difficoltà interpretative non sono nuove; esse erano già emerse con riferimento alla guerra cibernetica, sebbene la guerra cognitiva le amplifichi ulteriormente. La dottrina costituzionale prevalente sembrerebbe ritenere che l'art. 11 della Costituzione consenta l'uso della forza esclusivamente per finalità difensive, escludendo pertanto qualsiasi forma di guerra di aggressione; restano tuttavia aperte le cosiddette «zone grigie», tra cui la legittimità costituzionale della partecipazione a sistemi di difesa collettiva come il Patto Atlantico e il concetto di «soccorso difensivo»[33]. Sebbene lo Stato italiano, attraverso il proprio *position paper* sull'applicazione del diritto internazionale al ciberspazio, abbia ribadito l'operatività dei principi fondamentali del diritto internazionale anche nel dominio digitale[34], una riflessione costituzionale specificamente dedicata alla dimensione cognitiva appare ancora assente. Un primo orientamento è comunque tracciabile per via analogica. Se la guerra cibernetica offensiva, volta a danneggiare reti o infrastrutture di altri Stati, appare costituzionalmente incompatibile con l'art. 11 Cost. in quanto contraria alla finalità di promozione della pace, una difesa cibernetica attiva finalizzata alla tutela della sicurezza nazionale può invece ricondursi al dovere sancito dall'art. 52 Cost.[35]. Le medesime considerazioni possono essere estese, con gli opportuni adattamenti, alle operazioni cognitive. Una condotta

[32] Sul combinato disposto degli artt. 11 e 52 Cost. con riferimento ai conflitti non convenzionali cfr. A. GATTI, M. GIANNELLI, *Presupposti per la configurazione e la dichiarazione di guerra cibernetica*, in *DPCE Online*, v. 63, n. speciale 1, 2024, p. 462.

[33] Ivi, p. 462. Per una lettura dell'art. 11 Cost. come «invalicabile baluardo» del sistema costituzionale cfr. C. DE FIORES, *Il principio costituzionale pacifista, gli obblighi internazionali e l'invio di armi a paesi in guerra*, in G. AZZARITI (a cura di), *Il costituzionalismo democratico moderno può sopravvivere alla guerra?*, Editoriale Scientifica, Napoli, 2022. Per la ricostruzione dell'articolo nell'ambito dell'Assemblea Costituente cfr. L. CARLASSARE, *L'art. 11 Cost. nella visione dei Costituenti,* in *Costituzionalismo.it*, n. 1, 2013.

[34] Repubblica Italiana, *Italian Position Paper on 'International Law and Cyberspace',* pubblicato il 4 novembre 2021.

[35] A. GATTI, M. GIANNELLI, *Presupposti per la configurazione e la dichiarazione di guerra cibernetica*, cit., p. 463 e ss.

cognitiva offensiva di uno Stato, diretta a destabilizzare le istituzioni o l'opinione pubblica di un altro, apparirebbe incompatibile con il dettato *ex* art. 11 Cost.; al contrario, misure di contrasto e resilienza cognitiva adottate in funzione difensiva potrebbero collocarsi nell'alveo dell'art. 52 Cost. Tale estensione analogica richiede, tuttavia, un particolare livello di cautela, per via della natura ancora non pienamente esplorata dei meccanismi cognitivi umani e delle implicazioni etiche che qualsiasi intervento su di essi comporta[36].

Un aspetto che merita approfondimento specifico, nel quadro della lettura costituzionale della guerra cognitiva, è la tensione strutturale tra l'esigenza di contrastare la disinformazione e la tutela della libertà di manifestazione del pensiero *ex* art. 21 Cost. Il punto non è meramente teorico, in quanto qualsiasi misura normativa volta a contenere le operazioni cognitive in rete, sia essa il controllo diretto dei contenuti, l'obbligo di rimozione o i sistemi di etichettatura, si espone al rischio di comprimere le stesse libertà che si intende proteggere, producendo effetti paradossali rispetto agli obiettivi perseguiti. Interventi percepiti come arbitrari o sproporzionati possono generare un diffuso sentimento di sfiducia verso le istituzioni e, per questa via, agevolare la stessa propaganda ostile che le politiche di contrasto intendono neutralizzare[37]. Il caso nepalese del settembre 2025 è emblematico, poiché illustra con nitidezza i rischi di questo scivolamento. Il governo ha infatti tentato di bloccare l'accesso alle principali piattaforme *social* adducendo la necessità di contrastare la diffusione di *fake news* e contenuti d'odio. La misura, di carattere generalizzato e sproporzionato, ha inciso in modo particolare sulle generazioni più giovani, per le quali lo spazio digitale costituisce il principale veicolo di partecipazione alla sfera pubblica. La reazione sociale che ne è scaturita sembra aver disvelato la reale finalità dell'intervento, ovverosia non tanto la tutela della collettività dalla disinformazione, bensì la repressione del dissenso nei confronti di fenomeni radicati di corruzione e malagestione. La successiva *escalation*, culminata in atti di violenza contro sedi istituzionali e dimore dei membri dell'esecutivo, dimostra come la restrizione illegittima di una libertà fondamentale possa innescare una grave crisi di legittimità dello Stato e minare l'ordine costituzionale stesso. Sul versante opposto, la dottrina aveva già individuato nella libertà di informazione

[36] G. Maira, *Il cervello è più grande del cielo*, cit.

[37] Cfr. S. Sassi, A. Sterpa, *La Corte costituzionale della Romania difende la democrazia liberale dalla disinformazione. Prime note sulla sentenza n. 32 del 6 dicembre 2024*, in *federalismi.it*, n. 4, 2025, pp. 164 e ss.

una risorsa difensiva intrinseca. Carlo Esposito osservava che l'esercizio della libertà di manifestazione del pensiero non costituiva un «pericolo generale per la saldezza degli istituti», poiché le esternazioni «pericolose» sarebbero state confutate da altre capaci di «porne in luce la pericolosità eliminandola»; vale a dire che la «propaganda delle idee sovversive» sarebbe stata «vinta da quella delle idee costruttive» e «la verità avrebbe illuminato sé stessa e l'errore»[38]. La libertà di informazione possiederebbe dunque «validi anticorpi in grado di bloccare la disinformazione»[39], e il compito dell'ordinamento non sarebbe quello di sostituirsi al dibattito pubblico, bensì preservarne le condizioni di funzionamento.

3.2. L'ordinamento europeo

Il livello di analisi del quadro regolatorio europeo tocca due ambiti distinti ma convergenti, ovverosia la disciplina dell'intelligenza artificiale in contesto militare e la regolazione delle piattaforme digitali come vettori di disinformazione.

Quanto al primo ambito, il Regolamento europeo sull'Intelligenza Artificiale, detto AI Act (Reg. UE 2024/1689), esclude espressamente dal proprio campo di applicazione i sistemi di IA destinati alla difesa, alla sicurezza nazionale o a fini militari[40]. L'esenzione opera secondo due modalità. La prima riguarda i sistemi immessi sul mercato o utilizzati esclusivamente per scopi militari o di sicurezza nazionale, indipendentemente dall'entità che li impiega; la seconda esonera i sistemi non immessi sul mercato nell'Unione, purché il loro utilizzo nel territorio sia limitato agli scopi medesimi. Ne consegue che i sistemi di IA impiegati nelle operazioni cognitive a fini militari, dai generatori di *deepfake* alle piattaforme di amplificazione automatizzata dei contenuti, restino al di fuori dell'armonizzazione normativa europea e sono rimessi alla competenza esclusiva degli Stati membri. Si tratta, certamente, di una scelta dettata dalla necessità di preservare l'esclusività della sovranità statale in ambiti quali la difesa e la sicurezza nazionale, per cui una regolazione sovranazionale vincolante in materia militare avrebbe sollevato questioni di legittimità costituzionale in numerosi ordinamenti. Nondimeno, essa determina una significativa asimmetria regolatoria, in quanto le medesime tecnologie di

[38] C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, Milano, 1958.

[39] *Ibidem*.

[40] Art. 2, co. 3, del Regolamento (UE) 2024/1689.

IA che, impiegate in contesti civili, sono soggette a stringenti requisiti di trasparenza, valutazione del rischio e supervisione umana, restano prive di un quadro armonizzato non appena il loro utilizzo si collochi nel dominio della difesa, con la conseguenza che proprio i contesti a più elevato potenziale lesivo rimangono i meno presidiati sul piano normativo europeo. Sul piano internazionale, alcuni Stati hanno sottoscritto la "Dichiarazione politica sull'uso militare responsabile dell'Intelligenza Artificiale e dell'autonomia", con cui si impegnano a promuovere un consenso internazionale sull'impiego responsabile di tali tecnologie[41]. La dichiarazione ha però natura meramente programmatica e non vincolante e, soprattutto, tra i firmatari sono assenti proprio gli attori statuali più attivamente coinvolti nello sviluppo e nell'uso operativo di tecnologie belliche avanzate, ovverosia la Repubblica Popolare Cinese, la Federazione Russa, l'India, la Repubblica Islamica dell'Iran. Un accordo internazionale sull'IA militare che non include le principali potenze militari del mondo ha, inevitabilmente, un valore segnaletico più che regolatorio.

Il secondo ambito è quello della regolazione delle piattaforme digitali. Il *Digital Services Act* (Regolamento UE 2022/2065) rappresenta forse lo strumento europeo più avanzato in materia. Esso impone alle piattaforme di grandi dimensioni obblighi di trasparenza sui sistemi di raccomandazione, di valutazione dei rischi sistemici, tra cui quelli legati alla disinformazione, nonché di accesso ai dati per i ricercatori[42]. Tuttavia, il DSA presenta un limite strutturale nel contesto della guerra cognitiva, poiché si applica in tempo di pace e nelle giurisdizioni dell'Unione, mentre le operazioni cognitive più rilevanti sono condotte da attori esterni, attraverso piattaforme che operano su scala globale. Come emerge con chiarezza da alcuni studi, i ricercatori al di fuori dell'UE non possono avvalersi dei diritti di accesso ai dati che il DSA garantisce ai ricercatori europei, con conseguenze significative sulla capacità di monitorare e contrastare il fenomeno[43]. Il DSA è dunque uno strumento utile, ma insufficiente a regolare un fenomeno che per definizione non conosce confini giurisdizionali.

Due aspetti recenti arricchiscono il contesto fin qui delineato, meri-

[41] *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, proposta dagli Stati Uniti il 16 febbraio 2023, nel contesto del *summit* sull'AI responsabile nel dominio militare tenutasi presso L'Aia.

[42] Art. 40 del Regolamento (UE) 2022/2065 (Digital Services Act).

[43] K. Allen, C. Nehring, *AI-Generated Disinformation in Europe and Africa – Use Cases, Solutions and Transnational Learning*, Konrad-Adenauer-Stiftung e.V., 2025, p. 18.

tando particolare attenzione in virtù dell'indirizzo politico che sembrano portare con loro.

Il primo è l'*European Democracy Shield*, presentato congiuntamente dalla Commissione europea e dall'Alto Rappresentante il 12 novembre 2025. Si tratta del più ambizioso intervento europeo in materia di contrasto alle ingerenze straniere nell'ecosistema informativo. È articolato su tre pilastri, vale a dire la salvaguardia dell'integrità dello spazio informativo, il rafforzamento delle istituzioni e dei processi elettorali e il potenziamento della resilienza sociale. Lo *Shield* prevede, tra l'altro, l'istituzione di un *European Centre for Democratic Resilience*, destinato a fungere da centro di coordinamento tra istituzioni europee, Stati membri e società civile per anticipare, rilevare e rispondere alle minacce ibride, con particolare riguardo alle campagne di manipolazione informativa di origine straniera. È inoltre in corso la definizione di un protocollo di crisi nell'ambito del DSA per garantire reazioni coordinate e tempestive di fronte a operazioni informative su larga scala.

Il secondo strumento è la Dichiarazione per la sovranità digitale europea, una dichiarazione extra-europea adottata dagli Stati membri e dall'Unione europea stessa il 18 novembre 2025. Pur avendo anch'essa natura non cogente, la Dichiarazione cristallizza a livello politico l'ambizione europea di rafforzare la propria autonomia strategica nel dominio digitale; il documento esprime un impegno condiviso a consolidare la sovranità digitale europea a sostegno della resilienza economica, della prosperità sociale, della competitività e della sicurezza, prevedendo al contempo di continuare a trarre vantaggio dalla collaborazione con i *partner* globali attraverso un mercato aperto. Nel contesto della guerra cognitiva, la Dichiarazione assume un rilievo che va oltre la dimensione infrastrutturale cui è principalmente rivolta. Essa sancisce, perlomeno sul piano politico e degli intenti, che il controllo sulle infrastrutture digitali, dai *data center* ai sistemi di *cloud computing*, fino alle architetture di IA, sia una questione di sicurezza nazionale e di sovranità e non soltanto di competitività economica. La dipendenza dell'Unione europea da piattaforme e infrastrutture extraeuropee non sarebbe dunque un mero problema di mercato, ma una vulnerabilità strategica che gli attori ostili potrebbero sfruttare per condurre operazioni cognitive difficilmente contrastabili dall'interno dei sistemi che esse stesse controllano.

Considerati congiuntamente, lo *Shield* e la Dichiarazione segnalano una progressiva presa di coscienza europea della natura sistemica della guerra cognitiva. Rimane tuttavia aperta la questione centrale. Entrambi gli strumenti operano al di fuori del confine del diritto vincolante, in

un'area in cui l'enunciazione di intenti politici è ben lontana dalla costruzione di obblighi giuridicamente cogenti. Il passaggio dall'intenzione alla norma e, dunque, dalla norma all'*enforcement*, resta il nodo irrisolto del quadro europeo.

3.3. Il quadro internazionale

Sul piano del diritto internazionale, la guerra cognitiva incide principalmente su tre distinti aspetti, ovverosia il divieto dell'uso della forza (*ex* art. 2, par. 4, della Carta ONU), il principio di non intervento negli affari interni degli Stati e le norme del diritto internazionale umanitario applicabili in contesto bellico.

Quanto al primo profilo, non esiste nel diritto internazionale una definizione o una soglia precisa che consenta di stabilire con certezza quando un'operazione cognitiva integri l'«uso della forza» vietato dalla Carta. Lo Stato italiano ha adottato, con riferimento alle operazioni cibernetiche, il principio dell'«equivalenza cinetica»; un'operazione *cyber* condotta da uno Stato nei confronti di un altro costituisce uso della forza «quando la sua portata e i suoi effetti sono paragonabili a quelli di un uso convenzionale della forza, con conseguenti danni fisici a proprietà, lesioni o perdite di vite umane»[44]. Secondo un documento redatto da un gruppo internazionale di esperti convocato dalla NATO sull'applicazione del diritto internazionale alla guerra *cyber*, il Manuale di Tallinn 1.0, le operazioni psicologiche non distruttive, il cui scopo esclusivo sia minare la fiducia in un governo o in un'economia, non si qualificherebbero come uso della forza; lo farebbero invece, ad esempio, la fornitura a un gruppo organizzato di *malware* e della formazione necessaria per condurre attacchi cibernetici contro un altro Stato[45]. Il trasferimento di questo criterio alle operazioni cognitive apre però scenari di notevole incertezza, poiché le campagne di manipolazione cognitiva su larga scala, pur non producendo danni fisici diretti, potrebbero causare effetti destabilizzanti di portata paragonabile a quella di un'azione militare convenzionale.

Il secondo istituto rilevante è il principio di non intervento negli affari interni degli Stati. Secondo la Regola 66 del Manuale di Tallinn 2.0, «uno Stato non può intervenire, anche con mezzi informatici, negli affari interni o esterni di un altro Stato»; il divieto comprende, tra l'altro,

[44] *Italian position paper on 'International Law and Cyberspace'*, cit., p. 8.

[45] Regola 11 del M.N. Schmitt (a cura di), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013.

l'alterazione dei voti elettronici per condizionare elezioni, ma anche la coercizione di uno Stato finalizzata a modificare la propria legislazione in materia di ciberspazio[46]. Affinché un'operazione integri tale divieto, essa deve avere natura coercitiva. La coercizione, pur non essendo chiaramente definita nel diritto internazionale, è intesa nel Manuale di Tallinn 2.0 come un atto volto a privare uno Stato della sua libertà di scelta, costringendolo ad agire, o non agire, in modo involontario, attraverso pressioni che lo obbligano a modificare il proprio comportamento interno[47]. La maggioranza degli esperti redigenti il Manuale ritiene che la coercizione sia condizione necessaria ma non sufficiente: l'intervento deve essere altresì diretto a influenzare decisioni o esiti interni dello Stato *target*[48]. Una minoranza di Autori ritiene invece sufficiente che lo Stato sia privato del controllo su un proprio affare interno, indipendentemente dall'intento di condizionarne le scelte[49].

Il terzo profilo è quello del diritto internazionale umanitario, applicabile nei contesti di conflitto armato. Esso ammette il ricorso a «stratagemmi di guerra»[50], che includono la diffusione di notizie false, i mascheramenti e le operazioni simulate, purché non configurino perfidia e non violino i diritti dei civili[51]. Ciò significa che una certa dose di manipolazione informativa è considerata lecita anche nel diritto dei conflitti armati. Il confine, tuttavia, è segnato dal divieto di atti il cui scopo principale sia diffondere terrore tra la popolazione civile; strumenti come i *deepfake*, qualora impiegati per indurre falsamente alla resa o alla fuga, si porrebbero in aperta violazione di tale divieto[52]. Più in generale, la disinformazione in situazioni emergenziali può alimentare tensioni, generare psicosi collettive e disarticolare il sistema decisionale statale, configuran-

[46] Regola 66, M.N. SCHMITT (a cura di), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, cit., 2017.

[47] *Ibidem.*

[48] *Ibidem.* Ad esempio, una campagna *cyber* che colpisce un gruppo etnico interno a un altro Stato, in un momento di tensioni interne, ma non mira a condizionare la politica dello Stato sul tema, non sarebbe considerata un intervento illecito; lo diventerebbe qualora mirasse a determinare un cambiamento di posizione dello Stato medesimo.

[49] *Ibidem.*

[50] Art. 37, co. 2, della IV Convenzione di Ginevra del 1949 relativa alla protezione delle persone civili in tempo di guerra.

[51] Artt. 51 e 57 della IV Convenzione di Ginevra del 1949.

[52] M. MEZZANOTTE, *Fake news, deepfake e sovranità digitale nei periodi bellici,* in *federalismi.it*, n. 33, 2022, pp. 57 e ss.

do una minaccia alla sicurezza nazionale e alla stabilità democratica che il diritto fatica ancora a nominare con precisione[53].

Infine un ostacolo strutturale all'applicazione del diritto internazionale alla guerra cognitiva è il cosiddetto «gap di attribuzione», ossia la difficoltà, spesso insuperabile, di ricondurre con certezza un'operazione cognitiva a uno Stato determinato. La negabilità è, come si è visto, una caratteristica intrinseca delle operazioni cognitive, che prediligono i contenuti «grigi» proprio perché non attribuibili con certezza al loro committente. In assenza di attribuzione, il meccanismo della responsabilità internazionale dello Stato non può operare e le norme esistenti rimangono inapplicabili. Questo problema, già acuto nel dominio cibernetico, si acuisce ulteriormente in quello cognitivo, dove la catena causale tra l'operazione e i suoi effetti è ancora più difficile da ricostruire.

4. Riflessioni conclusive

Le riflessioni svolte nelle pagine precedenti si collocano consapevolmente in una fase ancora preliminare dell'analisi giuridica di un fenomeno che, per complessità, sfugge alle categorie consolidate del diritto. La guerra cognitiva interpella in modo radicale non soltanto le tradizionali categorie della scienza giuridica, ma anche i presupposti epistemologici su cui essa si fonda, come l'identificabilità del soggetto agente e la delimitazione temporale e spaziale del conflitto.

Il percorso analitico condotto ha consentito di individuare, nei tre livelli normativi esaminati, alcuni agganci interpretativi che, pur non essendo stati concepiti per rispondere alle specificità della guerra cognitiva, possono offrire una base da cui muovere riflessioni. Il progressivo consolidamento di strumenti come l'European Democracy Shield e la Dichiarazione per la sovranità digitale europea testimonia, sul piano politico, una crescente consapevolezza istituzionale delle implicazioni del fenomeno, pur mancando l'aspetto cogente. In questo senso, il contributo che la riflessione giuridica può offrire in questa fase è forse quello di affinare un lessico condiviso e categorie interpretative sufficientemente duttili da accompagnare, senza pretesa di anticiparli, gli sviluppi normativi che il contesto geopolitico renderà progressivamente necessari. Si tratta, forse, di un invito alla cautela metodologica, poiché la complessità del feno-

[53] Per un'analisi del rapporto tra terrore e istituzioni democratiche si veda anche P. Bonetti, *Terrorismo, emergenza e costituzioni democratiche*, il Mulino, Bologna, 2006.

meno esige strumenti d'analisi adeguati, la cui elaborazione potrebbe richiede tempo, confronto interdisciplinare e una disponibilità a rivedere assunti consolidati che è, essa stessa, una forma di rigore scientifico.

FROM BATTLEFIELDS TO BROWSERS: AI, NEUROSCIENZE E GUERRA SOCIO-COGNITIVA

Arije Antinori[*]

1. *Introduzione*

La guerra cognitiva viene spesso trattata o come categoria talmente ampia da assorbire quasi ogni forma di influenza, oppure come mero adattamento della disinformazione allo scenario contemporaneo. Una ricostruzione più rigorosa richiede invece di distinguere con chiarezza il *target* cognitivo, il contesto conflittuale e i mezzi tecnologici utilizzati, evitando così che il concetto venga dilatato fino a perdere capacità esplicativa[1].

Qui si propone l'introduzione del concetto di "guerra socio-cognitiva", e non soltanto di guerra cognitiva, per evidenziare una trasformazione decisiva del conflitto contemporaneo. Se la nozione di guerra cognitiva mette correttamente a fuoco l'obiettivo finale dell'azione ostile, ossia percezione, attenzione, emozione, memoria, giudizio e decisione, essa rischia tuttavia di apparire ancora eccessivamente individualizzata, come se la mente fosse colpita in modo diretto e separabile dal contesto in cui opera. L'espressione "guerra socio-cognitiva" intende invece specificare che, nell'ecosistema cyber-sociale – ciò che continuiamo riduttivamente a chiamare internet e social media – la cognizione non è mai isolata. Essa

[*] Docente di Criminologia alla Sapienza Università di Roma.

[1] C. DEPPE, G.S. SCHAAL, *Cognitive warfare: a conceptual analysis of the Nato Act cognitive warfare exploratory concept*, in *Frontiers in Big Data*, vol. VII, 2024.

è continuamente modellata da piattaforme, *feed* algoritmici, metriche di visibilità, logiche di *engagement*, comunità digitali, pratiche memetiche e dinamiche di validazione sociale. In tal senso, la guerra cognitiva contemporanea è inevitabilmente anche *social*, quindi sociale, perché colpisce la mente agendo sulle infrastrutture relazionali, simboliche e tecnologiche entro cui la mente forma credenze, emozioni, appartenenze e disponibilità all'azione. Parlare di guerra socio-cognitiva consente dunque di cogliere più precisamente il fatto che, nel passaggio dai *battlefields* ai *browsers*, la manipolazione del giudizio individuale si è fusa con la manipolazione delle condizioni sociali della percezione, del senso e della credibilità[2].

Tale impostazione consente di compiere un ulteriore passo analitico. La guerra socio-cognitiva non va letta soltanto attraverso i suoi effetti osservabili come: disorientamento, polarizzazione, erosione della fiducia o frammentazione del dibattito pubblico, ma attraverso le condizioni strutturali che rendono una collettività cognitivamente vulnerabile. Il *target* non è semplicemente ciò che una società conosce e/o crede, bensì l'insieme dei criteri, delle aspettative e delle architetture di senso attraverso cui essa costruisce conoscenza, attribuisce significato agli eventi e conserva una rappresentazione coerente di sé e del proprio futuro. In questo senso, la guerra socio-cognitiva non agisce soltanto sulle opinioni, ma sulle invarianti che permettono a una società di restare cognitivamente coerente, tra cui: verità, valori, identità, fiducia e futuro.

Ciò non indica quindi soltanto che il conflitto entra nello spazio digitale, ma che questo si sposta nelle condizioni stesse della formazione del giudizio. Il *target* non è più soltanto il territorio, né soltanto l'infrastruttura informativa, ma la capacità di una società di orientare l'attenzione, attribuire significato, discriminare tra vero e plausibile, mantenere fiducia nelle istituzioni e decidere sotto pressione. L'ecosistema cyber-sociale rende questa trasformazione strutturale, poiché intreccia dimensione psicologica, digitale e fisica in un unico spazio-tempo operativo, nel quale media, piattaforme, algoritmi, immagini, *meme*, *chatbot* e interazioni automatizzate concorrono a modellare il comportamento collettivo.

Il punto non è, dunque, aggiungere al lessico della guerra cognitiva un semplice inventario di "strumenti", come ad esempio *AI/MUAI*, *meme*, *FIMI, CIB* o attori *proxy*, ma chiarire il meccanismo che li rende efficaci nell'ecosistema cyber-sociale. Tali strumenti operano perché intercettano e amplificano vulnerabilità neurocognitive specifiche tra cui:

[2] B.C. TAYLOR, H. BEAN, *The handbook of communication and security*, Routledge, Londra, 2019.

attenzione, salienza, emozione, memoria, identità e decisione, attraverso architetture di piattaforma fondate su visibilità, ingaggio, replicabilità e validazione sociale. È in questa saldatura tra processi neurocognitivi e infrastrutture socio-digitali che la guerra cognitiva assume una forma propriamente socio-cognitiva.

Pertanto, la guerra cognitiva, letta nel quadro delle minacce ibride e delle minacce convergenti, deve essere compresa come pressione socio-cognitiva esercitata nel dominio cyber-sociale, secondo una prospettiva che consente di collegare influenza, disinformazione, *cyber*, radicalizzazione e vulnerabilità democratiche all'interno di un'unica architettura di rischio strategico. Quest'ultima non sostituisce sicurezza nazionale, sicurezza pubblica o *cybersecurity*, ma le integra. Difendere le infrastrutture digitali senza comprendere ad esempio i processi di radicalizzazione è insufficiente, tanto quanto proteggere le istituzioni senza capire come si generino sfiducia, polarizzazione e mobilitazione ostile; contrastare la manipolazione informativa senza considerare emozioni, *meme*, contenuti sintetici e dinamiche di piattaforma risulta altrettanto insufficiente[3].

2. *Dalla guerra dell'informazione alla guerra sul giudizio*

Per essere utile sul piano analitico, la guerra cognitiva deve essere distinta da concetti che si possono definire vicini. L'*Information Warfare* (IW) ha come baricentro il controllo, l'interruzione o la manipolazione del flusso informativo. La propaganda tradizionale mira a orientare opinioni e comportamenti collettivi attraverso messaggi relativamente identificabili. Le *Psychological Operations* (PsyOps) ricercano effetti psicologici e/o comportamentali su *target* selezionati. La guerra cognitiva, invece, assume come oggetto diretto il modo in cui il *target* trasforma l'informazione in percezione, comprensione, senso e soprattutto decisione. Il contenuto informativo, in tale prospettiva, è solo il vettore, mentre il vero obiettivo è il processo di elaborazione[4]

La distinzione decisiva tra guerra informativa e guerra socio-cogniti-

[3] L. Danley, B. Colder, *The building resilience to cognitive warfare technical exchange meeting*, MITRE, 2023; L. Huang, Q. Zhu, *Cognitive security: A system-scientific approach*, Springer, Berlino, 2023.

[4] A. Bernal, C. Carter, I. Singh, K. Cao, O. Madreperla, *Cognitive warfare: An attack on truth and thought,* 2020; B. Claverie, F. Du Cluzel, *The cognitive warfare concept*, 2022.

va non consiste quindi soltanto nel tipo di messaggio impiegato, ma nel livello dell'attacco. La prima agisce prevalentemente sulla disponibilità, sulla veridicità o sulla circolazione del contenuto informativo. La seconda agisce sulle strutture interpretative che rendono quel contenuto credibile, minaccioso, irrilevante, moralmente vincolante e desiderabile. Per questo la guerra socio-cognitiva è più profonda della disinformazione: non mira solo a far credere qualcosa di falso, ma a modificare le condizioni attraverso cui una collettività stabilisce che cosa possa essere considerato vero, affidabile e condivisibile.

Una delimitazione operativa particolarmente utile consiste nell'individuare tre elementi ricorrenti:

a. una finalità più ampia di quella immediatamente visibile;

b. una natura diffusa, concatenata e spesso difficilmente attribuibile dell'azione;

c. un *target* propriamente cognitivo, rivolto a dubbio, interpretazione, percezione della minaccia, volontà e decisione.

Tale tripartizione evita sia l'inflazione concettuale che la riduzione della guerra cognitiva a singoli episodi comunemente definiti *fake news* e/o propaganda occasionale. Oggi minacce ibride, disinformazione, *Foreign Information Manipulation and Interference* (FIMI), *Coordinated Inauthentic Behaviour* (CIB), radicalizzazione e sabotaggio vengono sempre più spesso associate alla guerra cognitiva. Il lessico cambia, ma la finalità operativa resta la stessa, ossia colpire la capacità di orientamento del *target*, generando sfiducia, incertezza, attrito decisionale e, in modo più esteso, vulnerabilità sistemica.

Ogni ecosistema cyber-sociale si regge su criteri condivisi di verità, gerarchie di valore, confini identitari, architetture di fiducia e immagini del futuro che pertanto non sono soggette ad alterazioni. Tali invarianti non sono semplici opinioni diffuse, ma le strutture che permettono a una collettività di restare cognitivamente coerente, di riconoscersi come soggetto unitario e di adattarsi al mutamento senza dissolvere la propria continuità. La guerra socio-cognitiva mira precisamente a queste strutture. Infatti, non si limita a immettere contenuti tossici, divisivi, nello spazio informativo, ma tenta di alterare le condizioni attraverso cui ogni contenuto viene interpretato[5].

Pertanto, la vulnerabilità cyber-sociale può essere letta secondo cinque livelli:

[5] F. KOROBEYNIKOV, A. DAVYDIUK, V. MOKHOR, *Ontological foundations of cognitive warfare,* NATO Cooperative Cyber Defence Centre of Excellence, 2026.

- epistemico – riguarda i criteri attraverso cui una comunità distingue vero, falso, plausibile e manipolato;
- assiologico – relativo alle gerarchie di valore che stabiliscono ciò che è giusto, intollerabile e/o sacrificabile;
- identitario – concerne i confini tra "Noi" e "Loro";
- fiduciario-istituzionale – riguarda l'affidabilità attribuita a procedure, esperti, media, autorità e fonti;
- teleologico – concerne il fine ultimo, l'immagine condivisa del futuro.

Colpire uno di questi livelli significa produrre effetti sugli altri, perché nell'ecosistema cyber-sociale verità, valori, identità, fiducia e futuro non operano separatamente.

Tale prospettiva consente anche di leggere l'ecosistema cyber-sociale come una rete stratificata, composta da più livelli di relazione sovrapposti. Gli stessi soggetti, gruppi e istituzioni sono simultaneamente connessi da relazioni informative, affettive, identitarie, valoriali, istituzionali e simboliche. La vulnerabilità nasce proprio da questa stratificazione, in quanto un attacco che appare inizialmente confinato al piano informativo può propagarsi al piano della fiducia, dell'identità, della memoria collettiva e della visione del futuro. La guerra socio-cognitiva sfrutta dunque i connettori tra strati diversi, generando effetti a cascata che non sarebbero spiegabili attraverso una lettura monodimensionale[6].

3. Neuroscienze della vulnerabilità cognitiva

La guerra socio-cognitiva non controlla magicamente la mente, ma sfrutta tendenze ricorrenti e relativamente stabili della cognizione umana. Queste sono ad esempio la selettività dell'attenzione, la maggiore salienza degli stimoli percepiti come minacciosi, la forza delle emozioni morali – indignazione, disgusto, rabbia o senso di ingiustizia – nel trasformare un'informazione in giudizio e disponibilità all'azione, la capacità della ripetizione di rendere messaggi, immagini e frame più familiari, memorabili e credibili, il peso dell'identità di gruppo e la dipendenza da euristiche quando il soggetto è esposto a sovraccarico informativo, scarsità di tempo o stress decisionale[7].

[6] F. Korobeynikov, A. Davydiuk, V. Mokhor, *Ontological foundations of cognitive warfare,* cit.

[7] M. Fitzduff, *Our brains at war: the neuroscience of conflict and peacebuilding*, Ox-

La dimensione neuroscientifica consente di evitare due errori opposti. Il primo è costituito da una lettura puramente tecnologica della guerra cognitiva, attribuendo la responsabilità della manipolazione unicamente a piattaforme digitali e AI; mentre il secondo è in una lettura puramente psicologica, come se la vulnerabilità fosse una proprietà individuale separata dall'ambiente in cui si sviluppa. Il punto centrale è invece la convergenza, poiché AI, piattaforme, *meme* e attori asimmetrici sfruttano vulnerabilità neurocognitive specifiche -attenzione, salienza, emozione, memoria, identità e decisione – all'interno di architetture sociali progettate per visibilità, ingaggio, replicabilità e validazione tra pari.

Il *target* primario è quindi l'attenzione. In ambienti ad alta densità informativa, tutto ciò che interrompe, sorprende, scandalizza o minaccia tende a prevalere. *Feed*, notifiche, immagini forti, *short-form content* e *meme* competono per risorse attentive limitate, e l'ecosistema cybersociale premia strutturalmente i contenuti più salienti. Ciò rende l'attenzione una superficie di attacco decisiva che può essere catturata, saturata o dispersa fino a rendere meno disponibile la capacità di selezione critica[8].

In tale quadro, *emotional warfare* e *narrative warfare* sono concetti utili, ma non devono essere trattati come guerre parallele o autonome rispetto alla guerra cognitiva. Essi vanno piuttosto compresi come dimensioni interne della guerra socio-cognitiva. La prima ne descrive l'energia affettiva: paura, rabbia, indignazione, umiliazione e disgusto sono vettori di attivazione, polarizzazione e mobilitazione. La seconda ne descrive la forma simbolica: *frame* di vittimizzazione, minaccia, tradimento, redenzione e scontro esistenziale organizzano gli stimoli emotivi dentro una struttura di senso comprensibile, condivisibile e mobilitante. La guerra socio-cognitiva è quindi affettiva e narrativa al tempo stesso. È affettiva perché sfrutta il fatto che l'emozione orienta attenzione, memoria e disponibilità all'azione. Inoltre, è anche narrativa perché trasforma l'esperienza in una sequenza di ruoli, colpe, minacce e finalità. Paura e rabbia forniscono energia, mentre la narrazione fornisce direzione. Senza attivazione emotiva, il messaggio resta debole, così come senza forma narrativa, l'emozione resta dispersa. La forza della pressione socio-cognitiva deriva precisamente dalla saldatura tra questi due livelli.

Il secondo *target* è dunque il sistema di elaborazione della minaccia. In condizioni di tensione o pericolo percepito, i circuiti associati alla ri-

ford University Press, Oxford, 2021; HUANG, Q. ZHU, *Cognitive security: A system-scientific approach*, cit.

[8] *Ibidem.*

sposta rapida alla minaccia tendono a prevalere su quelli associati alla valutazione deliberativa. Ne deriva che paura, rabbia, disgusto, indignazione morale e umiliazione rendono più probabile il ricorso a scorciatoie interpretative, segnali di gruppo e/o cornici morali dicotomiche. La saturazione emotiva riduce il campo del giudizio e aumenta la reattività[9].

Il terzo *target* è la memoria. *Meme, slogan*, immagini traumatiche, archetipi e figure dell'inimicizia funzionano perché comprimono complessità in unità rapidamente memorizzabili. La ripetizione produce scorciatoie cognitive e disponibilità mnemoniche che possono essere riattivate nelle crisi successive. La guerra socio-cognitiva non persuade solo nel presente: sedimenta, lascia tracce, costruisce repertori simbolici e morali a cui sarà facile attingere in futuro.

Un ulteriore meccanismo cruciale riguarda status e *belonging*. Le motivazioni profonde del conflitto non si riducono alle ideologie che lo giustificano, ma spesso le precedono. Ricerca di appartenenza, riconoscimento, lealtà, protezione del gruppo e timore dell'esclusione costituiscono potenti motori della mobilitazione. Le ideologie, le religioni e le narrazioni politiche rendono questi impulsi socialmente intelligibili e moralmente nobili. Per tale ragione, radicalizzazione e polarizzazione non possono essere lette solo come adesione ideologica, ma rappresentano anche risposte a bisogni di appartenenza e posizionamento che l'ecosistema cyber-sociale amplifica e rinforza[10].

Infine, la guerra cognitiva non punta sempre a convincere; spesso mira a confondere, rallentare, dividere, destabilizzare il giudizio. Il sovraccarico informativo, l'ambiguità, la saturazione emotiva e la pressione sociale favoriscono l'uso di euristiche, segnali "tribali" e semplificazioni morali. Il problema non è solo la falsità dei contenuti, ma l'integrità delle condizioni entro cui individui e istituzioni decidono[11]

4. *Dal campo di battaglia al* browser*:* AI*,* MUAI *e attori asimmetrici*

Il passaggio dai *battlefields* ai *browsers* ha prodotto un effetto strutturale, ridistribuendo le capacità offensive. Operazioni di influenza che in passato richiedevano apparati statali, filiere mediali e competenze

[9] M. Fitzduff, *Our brains at war: the neuroscience of conflict and peacebuilding*, cit.

[10] M. Martin, *Why we fight,* Hurst, Londra, 2018.

[11] L. Danley, B. Colder, *The building resilience to cognitive warfare technical exchange meeting*, cit.; Huang, Q. Zhu, *Cognitive security: A system-scientific approach*, cit.

molto specifiche possono oggi essere imitate, scalate e/o decentralizzate grazie a piattaforme globali, sistemi di automazione, servizi digitali pronti all'uso e contenuti generati sinteticamente. Il *Malicious Use of AI* (MUAI) – l'impiego di tecnologie su base AI per finalità dannose, non etiche e/o illecite, con effetti potenzialmente destabilizzanti sull'ecosistema cyber-sociale – amplifica questa trasformazione, riducendo il costo di produzione, aumentando la velocità di adattamento e rendendo più accessibile la manipolazione conversazionale, audiovisiva e narrativa[12]. I sistemi di *Machine Learning* (ML) sono spesso fragili, opachi, dipendenti da dati imperfetti e vulnerabili al *poisoning*, bias e manipolazione del *training set* [13]. Tuttavia, proprio perché non sostituiscono l'umano ma lo potenziano, essi agiscono come moltiplicatore di forza, accelerando classificazione, *targeting*, generazione di contenuti, adattamento tattico e produzione di verosimiglianza. L'*AI*, quindi, non elimina l'incertezza strategica poiché gli attori continuano a decidere in condizioni di informazione incompleta, opacità dei sistemi, errore, manipolazione e imprevedibilità delle reazioni sociali. Essa tende però a comprimere i tempi entro cui tale incertezza deve essere interpretata e gestita, e ad ampliarne la scala, perché consente di automatizzare analisi, selezione dei bersagli, produzione di contenuti e adattamento delle operazioni a una velocità e con una granularità difficilmente raggiungibili da operatori umani[14].

Il *browser* favorisce così l'ingresso degli attori asimmetrici nella guerra cognitiva. Estremisti, hacktivisti, gruppi criminali, reti/attori proxy e operatori opportunistici possono sfruttare lo stesso ambiente informativo-comunicativo, cioè lo stesso ecosistema, lo stesso ecosistema, delle grandi potenze, anche se con obiettivi e capacità differenti. Considerando questa capacità, ciò che conta non è solo la quantità di risorse, ma la capacità di sfruttare partecipazione distribuita, mimetismo, viralità, simulazione di autenticità e difficoltà di attribuzione.

In aggiunta a ciò, una trasformazione particolarmente rilevante ri-

[12] A. ANTINORI, *Cyber-Social Threats: How AI Fuels Modern Radicalisation*. EU Knowledge Hub on Prevention of Radicalisation of the European Commission, 2025; A. ANTINORI, *Malicious Use of Artificial Intelligence (MUAI): l'uso malevolo dell'Intelligenza Artificiale nell'ecosistema cyber-sociale*, in *Sicurezza e scienze sociali*, 13(2), 2025; J. JOHNSON, *Artificial intelligence and the future of warfare: the USA, China, and strategic stability,* Manchester University Press, Manchester, 2021.

[13] A. ANTINORI, *Artificial Inte[Glitch]Ence. Una minaccia sistemica alla sicurezza nazionale in prospettiva futura*, in *Gnosis. Rivista italiani di intelligence*, 2/2019.

[14] J. JOHNSON, *Artificial intelligence and the future of warfare: the USA, China, and strategic stability*, cit.

guarda il linguaggio stesso. Nella sicurezza digitale contemporanea, il linguaggio non è più soltanto veicolo di *social engineering*, ma diviene esso stesso superficie di attacco. *Email*, SMS, *chatbot*, *deepfake* vocali, videoconferenze fraudolente, *landing page* credibili e messaggi generati da *Large Language Model* (*LLM*) consentono livelli di personalizzazione, persuasione e seduzione che prima erano molto più difficili da raggiungere[15]. In estrema sintesi, il passaggio dall'*exploit* tecnico a quello discorsivo rende l'ecosistema cyber-sociale una matrice di attacco al contempo semantica, socio-relazionale e predittiva.

5. AI *e operazioni informative: modelli strategici comparati*

In questa transizione, l'integrazione tra AI e guerra informativa non è uniforme. Le grandi potenze la incorporano secondo tradizioni strategiche, culture organizzative e priorità diverse, anche sulla base dei modelli organizzativi e catene di responabilità individuate. In prospettiva comparata, si osservano almeno tre traiettorie:

x. una maggiore enfasi su *detection*, analisi e supporto decisionale;

y. una su controllo informativo, gestione dell'opinione e monitoraggio sociale;

z. una su operazioni offensive, polarizzazione, *deepfake*, bot e sfruttamento delle fratture dell'avversario.

La comparazione tra Stati Uniti, Cina e Russia mostra che l'AI entra in modo ormai organico nelle operazioni informative, sia come strumento di difesa cognitiva sia come moltiplicatore offensivo[16].

Particolarmente rilevante è la concezione che sembra avere la Cina del dominio cognitivo come spazio permanente di *shaping*. In questa prospettiva, la battaglia cognitiva non appartiene solo alla guerra dichiarata, ma attraversa pace, crisi e conflitto, operando come attività continua di modellamento delle percezioni, delle narrative e della volontà politica dell'avversario. Il dominio cognitivo viene così dilatato nello

[15] A. Antinori, *Strategic Communications against the Malicious Use of AI*, in The Hub. Insights, Strategic Communication and Artificial Intelligence, EU Knowledge Hub on Prevention of Radicalisation, 2026.

[16] L.Y Hunter, C.D. Albert, J. Rutland, K. Topping, C. Hennigan, *Artificial intelligence and information warfare in major power states: How the US, China, and Russia are using artificial intelligence in their information warfare and influence operations*, in Defense & Security Analysis, 2024.

spazio e nel tempo, non è un teatro circoscritto, ma un ambiente permanente di influenza e condizionamento. Da qui derivano l'approccio *whole-of-government*, la ricerca di superiorità narrativa, l'occupazione delle "alture" della moralità e della legalità percepite nonché la fusione tra componenti militari, civili e tecnologiche. L'informazione diventa munizionamento, le piattaforme campi di battaglia invisibili, la tecnologia infrastruttura di modellamento della volontà[17].

6. FIMI, CIB *e grammatica operativa dell'interferenza*

Le categorie di *FIMI* e *CIB* permettono di nominare con precisione la grammatica operativa della guerra cognitiva nel contesto europeo e italiano. La minaccia ibrida viene descritta come attività coordinata, negabile e difficilmente attribuibile, modellata sulle vulnerabilità sistemiche dei *target* e spesso collocata sotto la soglia dell'aperto conflitto armato.

La nozione di "sottosoglia" deve essere intesa, in questa sede, non come sinonimo di bassa intensità, ma come modalità di azione strategica calibrata per produrre effetti politici, psicologici e sociali senza oltrepassare immediatamente i limiti, le soglie tradizionali della risposta militare, giuridica o politica. Proprio per questo, *FIMI* e *CIB* sono strumenti particolarmente adatti alla guerra socio-cognitiva in quanto permettono di alterare visibilità, credibilità e consenso apparente senza presentarsi come aggressione manifesta.

Dette categorie sono essenziali perché mostrano che la guerra cognitiva non si esaurisce nella produzione di contenuti falsi. Essa coinvolge la costruzione artificiale rispettivamente di visibilità, credibilità e consenso apparente. L'obiettivo non è soltanto cambiare ciò che viene detto, ma alterare ciò che appare condiviso, legittimo, urgente, maggioritario e/o prioritario, talvolta in senso esistenziale. In termini cognitivi, il *target* non è solo l'opinione, ma sempre più la percezione del contesto sociale entro cui l'opinione si forma.

Tale dinamica risulta particolarmente rilevante perché agisce anche sulle invarianti epistemiche e fiduciario-istituzionali dell'ecosistema democratico. La simulazione di consenso, spontaneità o autenticità non produce solo disinformazione, ma altera i criteri attraverso cui una comunità valuta ciò che appare credibile, condiviso e socialmente legitti-

[17] J. BAUGHMAN, *How China wins the cognitive domain*, China Aerospace Studies Institute, 2023.

mo. In tal modo, *FIMI* e *CIB* non colpiscono esclusivamente i contenuti, ma l'ambiente cognitivo che rende alcuni contenuti percepiti come veri, urgenti o inevitabili[18]. Proprio per questo, il ricorso alla creazione di reti *CIB* riconducibili ad attori internazionali quali Cina, Iran e Russia conferma che automazione, account inautentici, mimetismo mediatico e contenuti sintetici tendono ormai a convergere in campagne di influenza sempre più credibili, pervasive e difficili da individuare. Il caso delle reti filorusse e del cosiddetto ecosistema di trollaggio pro-*Kremlin* mostra in modo particolarmente evidente la persistenza, l'adattabilità e la continuità operativa di tali infrastrutture di manipolazione[19].

7. Memetic warfare *e propaganda partecipativa*

Nella complessità dinamica dello scenario qui rappresentato, il *memetic warfare* non è un sottoprodotto folklorico e *low-cost* della guerra cognitiva, ma una delle sue forme più efficaci. Il meme cattura l'attenzione, attiva emozioni immediate, condensa una narrazione multidimensionale e sancisce appartenenza. Per questo si colloca precisamente nell'intersezione tra neuroscienze, piattaforme e influenza, rendendo virale ciò che è apparentemente semplice, identificabile, emotivamente saliente e socialmente condivisibile.

La *memetic warfare*, ossia la forma di conflitto informazionale/cognitivo in cui meme, *dark irony*, simboli digitali e micro-narrazioni virali vengono impiegati come vettori di influenza, radicalizzazione e mobilitazione ostile, rappresenta il punto in cui le dimensioni emotiva e narrativa della guerra socio-cognitiva si fondono con maggiore evidenza. Sul piano emotivo, il meme attiva rapidamente paura, rabbia, scherno, umiliazione, indignazione o disgusto. Sul piano narrativo, esso comprime in una forma minima un frame di vittimizzazione, minaccia, tradimento, redenzione o scontro esistenziale. La sua forza deriva proprio da questa doppia compressione: massima intensità affettiva e massima semplicità simbolica.

La logica memetica è strettamente legata alla partecipazione dell'au-

[18] A. Antinori, *Strategic Communications against the Malicious Use of AI*, cit.; A. Antinori, *Radicalisation and FIMI in the Western Balkans Cyber-Social Ecosystem*, in A. Antinori, J. Nijenhuis, *How FIMI Fuels Polarisation and Radicalisation in the Western Balkans*, Institute of Communication Studies, 2026.

[19] L. Gyori, C. Molnar, P. Kreko, P. Szicherle, *The Kremlin's troll network never sleeps*, Political Capital, 2022.

dience. Ciò in quanto la propaganda contemporanea non si limita a persuadere destinatari passivi, ma sfrutta *audience* che commentano, rilanciano, reinterpretano, desiderano e amplificano. La partecipazione non neutralizza la propaganda, al contrario, spesso la rende più efficace, perché la radica all'interno di pratiche ordinarie di condivisione, ironia o meglio *dark irony*, appartenenza e riconoscimento reciproco[20].

Per gli attori asimmetrici, il meme è particolarmente vantaggioso in quanto economico, adattabile, dotato di *plausible deniability*, attraversa facilmente piattaforme sociomediali differenti sia *mainstream* che *fringe*, e consente all'attaccante di abbassare significativamente la soglia di accettabilità di contenuti ostili, il che genera un effetto propagazione e normalizzazione estremamente preoccupante, soprattutto per gli *screenagers*, adolescenti e preadolescenti ormai non più solo iperconnessi, ma sempre più identitariamente connettivi. Quando viene potenziato dalla Generative *AI* (*GenAI*), inoltre, il memetic warfare acquisisce maggiore volume, velocità e capacità di personalizzazione, configurandosi come una delle applicazioni socio-cognitive più rilevanti del *MUAI*[21]. Esso agisce simultaneamente su attenzione, emozione, memoria, appartenenza e decisione. La sua efficacia non deriva soltanto dalla viralità, ma dal fatto che trasforma la narrazione in gesto partecipativo, nel condividere, "remediare" e/o commentare un *meme* significa spesso prendere posizione, dichiarare appartenenza e contribuire alla normalizzazione di un *frame*.

8. *Dal sottosoglia al sopra soglia: il* continuum *della pressione socio-cognitiva*

L'espressione "sottosoglia" non indica semplicemente una forma attenuata o minore di conflitto, ma una modalità strategica di azione che mira a produrre effetti rilevanti senza oltrepassare immediatamente le soglie tradizionali della risposta militare, giuridica o politica. Le minacce ibride operano precisamente in tale spazio, combinando strumenti militari e non, azioni manifeste e operazioni occulte e/o difficilmente

[20] A. ANTINORI, *The Incel Phenomenon: Structures, Narratives, and Interations,* EU Knowledge Hub on Prevention of Radicalisation Newsletter, 2026; R. BURDA, *Cognitive warfare as part of society: Never-ending battle for minds*, The Hague Centre for Strategic Studies, 2023.

[21] A. ANTINORI, *Malicious Use of Artificial Intelligenc (MUAI): l'uso malevole dell'Intelligenza Artificiale nell'ecosistema cyber-sociale*, cit.

attribuibili, disinformazione, cyberattacchi, pressione economica, sabotaggio, attori proxy, manipolazione informativa e interferenza politica. Tutto questo rende incerta la distinzione tra pace e guerra e complicando attribuzione e risposta. In questa prospettiva, il sottosoglia non è un'area di pericolosità, ma di un regime di ambiguità strategica. La sua efficacia deriva dal fatto che ogni singola azione può apparire insufficiente a giustificare una risposta forte, mentre la loro combinazione produce effetti cumulativi su fiducia, coesione, percezione della minaccia e capacità decisionale.

A questo riguardo, nel quadro della guerra socio-cognitiva, si individuano almeno quattro soglie, come di seguito indicato:

- soglia giuridica, punto oltre il quale un'azione può essere qualificata come uso della forza, aggressione armata o conflitto armato. Molte attività ibride restano al di sotto di questa linea, pur producendo effetti significativi;
- soglia politica, punto oltre il quale un governo o un'alleanza ritiene necessario rispondere pubblicamente e in modo coordinato;
- soglia attributiva, relativa alla possibilità di identificare autore, intenzione, catena di comando e responsabilità dell'azione ostile;
- soglia cognitiva, il punto oltre il quale una società riconosce un evento non come disfunzione isolata, crisi spontanea o conflitto ordinario, ma come parte di una pressione strategica ostile. La guerra socio-cognitiva opera soprattutto su questa quarta soglia, perché è tanto più efficace quanto meno viene percepita come attacco.

Del resto, la guerra socio-cognitiva opera in modo privilegiato sottosoglia perché i suoi effetti principali non sono immediatamente cinetici. Essa non mira necessariamente a distruggere infrastrutture, occupare territori o produrre vittime fisiche, ma a modificare il contesto entro cui una collettività interpreta gli eventi. Un contenuto manipolativo, una rete di *account* inautentici, un *meme* ostile, un *deepfake*, una campagna di delegittimazione o una sequenza di micro-narrazioni polarizzanti possono apparire, se osservati in modo isolato, come fenomeni comunicativi ordinari. Tuttavia, se coordinati, amplificati e ripetuti, essi possono alterare progressivamente fiducia istituzionale, percezione della realtà, coesione sociale e disponibilità all'azione. In questo senso, la guerra socio-cognitiva deve essere considerata una tecnologia di soglia poiché può mantenersi sotto la soglia dell'uso della forza, sotto la soglia dell'attribuzione certa e sotto la soglia della percezione pubblica dell'aggressione, pur producendo effetti strategici.

Qui, il sottosoglia non è separato dal soprasoglia. Gli strumenti cyber-sociali e informativi possono preparare, accompagnare e prolungare spionaggio, sabotaggio, pressione politica e conflitti convenzionali. Nel contesto della guerra russo-ucraina, ad esempio, la centralità del dominio cibernetico e informativo mostra come la pressione cognitiva possa agire prima, durante e dopo l'impiego manifesto della forza. L'effetto cognitivo non è accessorio rispetto alla dimensione cinetica, ma contribuisce a orientarne la percezione, la legittimazione e l'efficacia strategica. La guerra socio-cognitiva non è dunque soltanto prebellica, né meramente alternativa al conflitto armato. Essa costituisce una dimensione trasversale, preparatoria, concomitante e successiva rispetto all'uso della forza. Il sottosoglia rende più porosa la distinzione tra minaccia esterna, vulnerabilità interna e ordine pubblico. La stessa pressione cognitiva può colpire simultaneamente fiducia istituzionale, coesione sociale, integrità del dibattito pubblico, sicurezza delle infrastrutture digitali e resilienza delle istituzioni e delle infrastrutture critiche, senza oltrepassare immediatamente i confini simbolici della guerra aperta. È qui che emerge la necessità del paradigma di sicurezza cyber-sociale. La risposta non può essere solo militare, solo cibernetica o solo comunicativa, ma deve integrare capacità di prevenzione, attribuzione, protezione infrastrutturale, monitoraggio dell'ecosistema informativo, resilienza cognitiva e misure politiche di tutela dell'ordine democratico. Il sottosoglia, quindi, è il luogo in cui sicurezza nazionale, sicurezza pubblica e *cybersecurity* cessano di essere domini separati e diventano componenti di una medesima architettura di difesa democratica.

9. Radicalizzazione socio-cognitiva mediata da piattaforma

L'estremismo rappresenta uno degli ambienti cyber-sociali in cui la guerra socio-cognitiva si lascia osservare con maggiore chiarezza. Esso si sviluppa sempre più spesso all'interno di comunità decentralizzate e dinamiche, popolate anche da soggetti molto giovani, segnate da vulnerabilità psicologiche e generazionali, da legami transnazionali mediati da piattaforme di messaggistica ormai funzionalmente assimilabili ai social media, da forme di ibridazione ideologica e pseudo-ideologica, da crescente nichilismo violento e dalla diffusione di una "cultura della violenza". In tali ambienti, strumenti di *AI* possono essere impiegati per propaganda, assistenza alla pianificazione, manipolazione realistica dei contenuti e ricognizione delle vulnerabilità a fini operativi e la prospettiva trova conferma

anche nell'analisi del rapporto tra FIMI, polarizzazione e radicalizzazione nell'ecosistema cyber-sociale dei Balcani occidentali, dove interferenza informativa, fratture identitarie, piattaforme digitali e vulnerabilità socio-politiche si combinano in processi di pressione cognitiva e mobilitazione ostile[22]. Tali processi di "radicalizzazione socio-cognitiva mediata da piattaforma" non dipendono pertanto da una singola idea tossica, ma dalla convergenza di esposizione narrativa, salienza emotiva, validazione reciproca, compressione memetica, ritualità cyber-sociale e disponibilità di repertori simbolici di violenza[23]. Ne deriva che il *browser* non è più soltanto mezzo di trasmissione, ma ambiente di (ri-)formattazione identitaria e di formazione della minaccia[24]. La dinamica identitaria è qui decisiva. Quando status, appartenenza, riconoscimento e valori percepiti, talvolta come sacri, si combinano con un ecosistema che rinforza paura, senso di assedio e purezza del gruppo, la soglia tra narrazione, disponibilità all'azione e attivazione comportamentale si abbassa. La radicalizzazione, quindi, non è solo un problema di contenuti, ma sempre più una questione di architetture cognitive, algoritmico-relazionali e affettive che rendono certi contenuti esistenzialmente persuasivi e capaci di mobilitare reazioni[25].

10. Sicurezza cyber-sociale e difesa democratica

Se la cognizione è divenuta superficie di attacco, la risposta non può essere settoriale. La sicurezza cyber-sociale – in quanto naturalmente socio-cognitiva – offre una cornice integrata che tiene insieme infrastrutture informative, processi cognitivi collettivi, relazioni di fiducia e resilienza democratica. Nei sistemi *human-cyber-physical*, la vulnerabilità umana non è un elemento esterno alla sicurezza, ma una sua componente strutturale. Per tale ragione la difesa democratica deve combinare educazione, progettazione socio-tecnica, monitoraggio, capacità analitiche, *policy* e strumenti *AI-enabled* orientati alla protezione di attenzione, decisione e *sensemaking*[26].

[22] A. Antinori, *The Incel Phenomenon: Structures, Narratives, and Interations*, cit.

[23] A. Antinori, *Radicalisation and FIMI in the Western Balkans Cyber-Social Ecosystem*, cit.

[24] A. Antinori, *Cyber-Social Threats: How AI Fuels Modern Radicalisation*, cit.

[25] M. Fitzduff, *Our brains at war: the neuroscience of conflict and peacebuilding*, cit.; M. Martin, *Why we fight*, cit.

[26] Huang, Q. Zhu, *Cognitive security: A system-scientific approach*, cit.

Questa integrazione diventa particolarmente urgente nelle dinamiche sottosoglia. Quando l'azione ostile non si presenta come attacco manifesto, ma come sequenza di anomalie informative, incidenti *cyber*, polarizzazioni sociali, contenuti virali, sabotaggi limitati o crisi apparentemente spontanee, la risposta settoriale tende a fallire. Ogni amministrazione vede solo una porzione del fenomeno. Infatti, la cybersicurezza osserva l'incidente tecnico, l'ordine pubblico osserva la mobilitazione, l'*intelligence* osserva l'interferenza, la comunicazione istituzionale osserva la narrativa ostile. La sicurezza cyber-sociale serve precisamente a ricomporre questi frammenti in un'unica diagnosi strategica.

Tale impostazione impone di superare una concezione meramente reattiva della difesa cognitiva. La correzione dei contenuti falsi, la segnalazione delle fonti problematiche e/o la rimozione dei messaggi manipolativi restano strumenti necessari, ma intervengono spesso quando il contesto cognitivo è già stato "vulnerabilizzato". La sicurezza cyber-sociale deve invece operare anche sulle condizioni che rendono certi contenuti più visibili, più credibili e più capaci di aggregare comunità interpretative chiuse. Ciò significa osservare la distribuzione della visibilità, i sistemi di raccomandazione, le traiettorie di circolazione dei contenuti, la formazione di *cluster* narrativi reciprocamente ostili e i meccanismi attraverso cui alcune comunità digitali consolidano criteri autonomi di validazione della realtà. In questa prospettiva, la resilienza cognitiva non è soltanto passiva, cioè orientata a contenere gli effetti già manifesti della manipolazione, ma attiva, in quanto capacità pubblica di comprendere e proteggere l'ecosistema socio-cognitivo prima che la frammentazione della realtà condivisa comprometta il conflitto democratico stesso.

La sicurezza cyber-sociale deve inoltre confrontarsi con un limite ordinario, non patologico, della cognizione umana: gli individui non verificano ogni informazione ricevuta, non ricostruiscono ogni fonte e non sottopongono ogni contenuto a un'analisi approfondita. In condizioni di sovraccarico, scarsità di tempo e risorse cognitive limitate, essi tendono a ricorrere a scorciatoie, euristiche e strumenti esterni di supporto. L'uso dell'AI per riassumere testi, produrre connessioni, ordinare informazioni o delegare segmenti del ragionamento rappresenta una forma contemporanea di cognitive *offloading*: può aumentare efficienza e accessibilità, ma può anche ridurre la vigilanza epistemica se sostituisce stabilmente il giudizio critico. Per questa ragione, la difesa cognitiva non può limitarsi a *debunking*, *prebunking* e *debiasing*, pur necessari. Deve prima costruire una cultura della sicurezza cognitiva, capace di rendere percepibile il rischio della delega non governata del giudizio e di promuovere un

uso dell'AI orientato all'assistenza, non alla sostituzione, delle funzioni cognitive critiche[27].

La sicurezza cyber-sociale deve inoltre essere intesa come protezione delle invarianti cognitive e relazionali che permettono a una società democratica di restare coerente sotto pressione. In questa prospettiva, reti, piattaforme, dati e infrastrutture non sono separabili da criteri di verità, architetture di fiducia, appartenenze collettive, gerarchie di valore e immagini del futuro. Proteggere l'ecosistema cyber-sociale significa quindi preservare la possibilità stessa di un giudizio collettivo condiviso[28].

Ne deriva che la resilienza cognitiva non coincide con la semplice capacità di smentire contenuti falsi o neutralizzare campagne informative ostili. Essa consiste, più profondamente, nella capacità di un sistema di mantenere coerenza interpretativa sotto pressione, ossia: continuare a distinguere il vero dal manipolato, preservare gerarchie di valore condivise, evitare la frammentazione identitaria, mantenere fiducia nelle procedure legittime e conservare un'immagine praticabile del futuro. La sicurezza cyber-sociale può essere intesa, in questo senso, come infrastruttura di protezione delle invarianti cognitive di una democrazia.

Questa impostazione impone anche di superare il paradigma puramente reattivo della rilevazione, attribuzione e risposta. Tale modello presuppone un evento ostile identificabile, una catena causale ricostruibile e un attore attribuibile. Ma la pressione socio-cognitiva opera spesso attraverso mutamenti lenti, distribuiti e apparentemente endogeni. La sicurezza cyber-sociale deve quindi spostarsi da una logica di risposta all'incidente a una logica di preservazione della coerenza. Il che significa proteggere criteri di verità, architetture di fiducia, continuità identitarie, gerarchie di valore e immagini condivise del futuro prima che diventino irreversibilmente vulnerabili.

In tale quadro, la nozione di *cognitive security* aiuta anche a evitare una lettura puramente "militarizzata" del problema. Essa insiste sul fatto che la difesa del dominio cognitivo riguarda non solo contesti di guerra e/o intelligence, ma una vasta gamma di missioni pubbliche, ove il target è costituito dalla capacità di giudicare, decidere, mantenere fiducia,

[27] E.F. Risko, S.J. Gilbert, *Cognitive offloading*, in *Trend in Cognitive Sciences*, 20 (9), 2016, pp. 676-688; S. Lewandowsky, S. Van Der Linden, *Countering misinformation and fake news through inoculation and prebunking*, in *European Review of Social Psychology*, 32 (2), 2021.

[28] F. Korobeynikov, A. Davydiuk, V. Mokhor, *Ontological foundations of cognitive warfare,* cit.

e percepire il desiderio. In tale quadro, la misurazione degli effetti, la costruzione di comunità interdisciplinari, lo sviluppo di *measures of effectiveness* e la *digital force protection* diventano priorità, proprio perché la semplice denuncia della minaccia non produce automaticamente resilienza[29].

La difesa democratica richiede però anche un criterio normativo. Non tutte le pratiche di influenza cognitiva sono eticamente equivalenti. La distinzione rilevante passa per il rapporto tra verità, attribuzione, trasparenza, inganno e rispetto dell'autonomia del soggetto bersaglio. Una democrazia liberale non può difendere l'autonomia politica dei cittadini mediante strumenti che ne riproducono la logica manipolativa o che ne compromettono stabilmente la capacità di giudizio. Da qui la rilevanza della distinzione tra forme occulte, ambigue e trasparenti di influenza cognitiva: le prime fondate su inganno, occultamento della fonte e manipolazione del vero; le seconde collocate in una zona intermedia di opacità e pressione strategica; le terze compatibili, almeno in linea di principio, con criteri di attribuibilità, veridicità, proporzionalità e rispetto della dignità umana. Il richiamo a dignità umana e autonomia politica consente così di fissare il limite oltre il quale la difesa cognitiva delle democrazie rischia di trasformarsi in una pratica incompatibile con i propri stessi presupposti normativi[30].

11. Conclusioni

Il passaggio dai *battlefields* ai *browsers* ha trasformato la guerra contemporanea in almeno cinque modi. Ha spostato il *target* verso le condizioni del giudizio. Ha reso il conflitto intrinsecamente cyber-sociale. Ha abbassato le barriere d'ingresso, favorendo attori asimmetrici e non-statali. Ha reso il *memetic warfare* una grammatica trasversale della mobilitazione ostile. Ha fatto dell'AI non solo un moltiplicatore tecnico, ma un acceleratore di profiling, simulazione, automazione e attacco linguistico.

Le neuroscienze sono essenziali perché spiegano perché la guerra cognitiva funzioni: perché alcuni stimoli catturino attenzione più di altri, perché la minaccia emotiva polarizzi, perché la ripetizione sedimenta

[29] L. DANLEY, B. COLDER, *The building resilience to cognitive warfare technical exchange meeting*, cit.

[30] A. HENSCKE, *Cognitive warfare: Grey matters in contemporary political conflict*, Routledge, Londra, 2024.

memoria in questa prospettiva, perché il gruppo rinforzi il messaggio, perché il sovraccarico degradi la decisione e perché status e *belonging* siano spesso più mobilitanti di quanto dicano le ideologie esplicite.

Tuttavia, il rischio ultimo della guerra socio-cognitiva non è solo la diffusione di false credenze, ma la frammentazione del quadro comune entro cui una società distingue il vero dal falso, il legittimo dall'illegittimo, il dissenso dalla delegittimazione e la crisi dall'aggressione. Una società può continuare a disporre di istituzioni, media, procedure, infrastrutture e competenze tecniche, ma perdere progressivamente la capacità di interpretarli dentro un quadro comune. In questa condizione, i singoli segmenti del sistema possono ancora funzionare localmente, mentre viene meno la possibilità di una percezione condivisa della realtà, di una risposta coordinata e di una trasformazione adattiva coerente. La decoerenza cognitiva è dunque una forma di disintegrazione interna senza collasso apparente[31].

Per tale ragione, la risposta non può limitarsi né alla protezione delle reti né alla sola smentita dei contenuti falsi. Deve assumere la forma di una politica di *sicurezza cyber-sociale*, capace di proteggere insieme infrastrutture, processi cognitivi collettivi, autonomia politica, relazioni di fiducia e resilienza democratica. Se il *browser* è divenuto un campo di battaglia, allora la sicurezza delle democrazie dipende anche dalla capacità di difendere gli ambienti in cui oggi percezione, significato, appartenenza e comportamento vengono prodotti, condivisi e contesi[32]. Difendere il browser come campo di battaglia significa dunque difendere le invarianti che rendono possibile la coerenza democratica, ossia: criteri di verità, gerarchie di valore, appartenenze plurali ma non distruttive, fiducia minima nelle procedure e immaginazione condivisa, in quanto comunità, del e nel futuro. In assenza di queste invarianti, il pluralismo può trasformarsi in paralisi, il dissenso in delegittimazione reciproca e la libertà informativa in vulnerabilità sistemica.

[31] F. Korobeynikov, A. Davydiuk, V. Mokhor, *Ontological foundations of cognitive warfare,* cit.

[32] A. Henscke, *Cognitive warfare: Grey matters in contemporary political conflict*, cit.; Huang, Q. Zhu, *Cognitive security: A system-scientific approach*, cit.

OLTRE IL CAMPO DI BATTAGLIA: LA WEAPONIZZAZIONE DEL CYBERSPAZIO E LA PROTEZIONE DEI CIVILI NEL DIRITTO INTERNAZIONALE UMANITARIO

Anna Calabrese[*]

1. *Introduzione*

Il paradigma della guerra ibrida rappresenta oggi la chiave interpretativa principale dell'evoluzione della conflittualità contemporanea: lungi dal costituire una serie diffusa e sconnessa di eventi di destabilizzazione, essa si configura come un metodo strumentale a generare effetti operativi senza oltrepassare la soglia del conflitto convenzionale e della violenza intesa in termini tradizionali. In questa prospettiva, attori statali e non statali ricorrono a una combinazione integrata di strumenti politici, economici, informativi, tecnologici e, solo in ultima istanza, militari, al fine di influenzare il comportamento dell'avversario, modellandone l'ambiente decisionale e sfruttandone le vulnerabilità sistemiche. Le democrazie sono maggiormente esposte a queste dinamiche, in quanto esse esprimono il loro potenziale proprio in contesti aperti, dove interconnessione, libertà e complessità dei processi diventano facilmente bersagli da erodere dall'interno.

La nozione di minaccia ibrida ha progressivamente ampliato la portata dei discorsi sulla sicurezza oltre la dimensione strettamente militare, includendo azioni sinergiche e parallele nei domini fisici, digitali e cognitivi. In questo quadro, il conflitto si manifesta sempre più come una combinazione di ostilità convenzionale e strumenti non cinetici. Il

[*] Responsabile delle relazioni esterne e istituzionali del Centro Studi Americani e Responsabile redazionale e Senior Fellow del Centro Studi Geopolitica.info.

cyberspazio, come sancito dal NATO Summit di Varsavia del 2016 che lo elevò a V° dominio operativo, emerge come strumento privilegiato per la realizzazione di strategie ibride. La sua natura a-territoriale, l'alto grado di intrinseca interconnessione nonché l'anonimia che i suoi meccanismi consentono, contribuiscono a rendere il *cyberspace* particolarmente efficace efficace su più livelli, generando effetti persistenti che spaziano dalla manipolazione dei processi decisionali (infiltrazione nelle reti di informazione, manipolazione della stessa), all'acquisizione di vantaggio informativo (furto di dati strategici e critici), fino ad arrivare alla perturbazione o addirittura compromissione fisica di infrastrutture critiche e vitali, sancendo il carattere di una minaccia al confine tra spazialità e virtualità, tra materialità e intangibilità.

La progressiva weaponizzazione del cyberspazio rappresenta, dunque, una delle manifestazioni più rilevanti della trasformazione in atto, segnando il passaggio da un utilizzo delle tecnologie digitali in chiave prevalentemente difensiva o funzionale a una loro piena integrazione come strumenti di proiezione della forza. In tale scenario, la distinzione tra tempo di pace e tempo di guerra, così come quella tra ambito civile e militare, tende a sfumare, mentre aumenta il rischio che operazioni condotte al di sotto della soglia del conflitto armato producano effetti significativi sulla popolazione civile e sul funzionamento di infrastrutture essenziali, stravolgendo le categorie classiche alla base della determinazione cognitiva e giuridica, come vedremo, del conflitto.

Queste dinamiche pongono infatti sfide profonde al diritto internazionale e in particolare al diritto internazionale umanitario, tradizionalmente concepito per disciplinare ostilità di natura cinetica e territorialmente delimitate. La dematerializzazione degli attacchi, l'anonimato degli attori, la difficoltà di attribuzione e la natura sistemica degli effetti cibernetici rendono più complessa l'applicazione delle strutture giuridiche esistenti, soprattutto con riferimento alla qualificazione dell'uso della forza e alla protezione dei civili.

Alla luce di tali trasformazioni, il presente contributo si propone di analizzare il rapporto tra la dimensione cibernetica del conflitto e il diritto internazionale umanitario, con particolare attenzione alla tutela della popolazione civile e delle infrastrutture critiche. L'obiettivo è verificare se e in quale misura il quadro giuridico vigente sia in grado di rispondere alle sfide poste dalla weaponizzazione del cyberspazio, sostenendo che, pur in assenza di un *corpus* normativo specifico, i principi fondamentali del diritto dei conflitti armati possano essere applicati anche al dominio digitale attraverso un'interpretazione evolutiva e contestualizzata.

2. *Inquadrare il fenomeno*

I dati provenienti da recenti report e analisi sulle principali minacce nel cyberspazio delineano uno scenario in rapida evoluzione, caratterizzato da un aumento significativo degli attacchi informatici e da una crescente rilevanza geopolitica delle operazioni cyber. In particolare, la media mensile degli incidenti è incrementata da 337 nella seconda metà del 2024 a 459 nel 2025[1] segnalando una fase di intensificazione della minaccia ibrida nell'ottica di una vera e propria "guerra cibernetica diffusa". Il nostro Paese si colloca tra quelli più coinvolti: nel primo semestre dell'anno, il 10,2% degli incidenti a livello mondiale si è infatti verificato in Italia, contro il 9,9% del 2024, confermando una *escalation* dal 3,4% del 2021 e dal 7,6% del 2022[2]. Le infrastrutture critiche rappresentano oggi un bersaglio privilegiato, mentre settori come governo, ambito militare e sanitario risultano tra i più colpiti, con una quota significativa di attacchi che coinvolge soggetti statali e pubblici, in crescita rispetto agli anni precedenti. Parallelamente, le tecniche di attacco più diffuse includono *Distributed Denial of Service* (DDoS) e *ransomware*, rispettivamente con circa il 41,1% e il 25,8% degli incidenti, spesso combinati con altre modalità operative come *data breach* e *social engineering*[3]. Si evidenzia inoltre come, quanto all'origine della minaccia, le attività *state-aligned* rappresentino il segmento più sofisticato della minaccia *cyber*. Secondo ENISA, tra luglio 2024 e luglio 2025 il 7,2% degli incidenti associati a gruppi allineati a Stati ha colpito membri dell'UE, con una percentuale più elevata (32%) attribuibile alla Russia, seguita da Cina (24%), Corea del Nord (12%) e Iran (5.3%)[4].

Gli attacchi cibernetici possono essere ricondotti a macro-categorie in base al vettore di intrusione e alla finalità operativa. Gli attacchi basati sulle credenziali mirano all'acquisizione non autorizzata di accessi a sistemi e account attraverso tecniche come *brute force*, *phishing* o *keylogging*, consentendo agli aggressori di ottenere privilegi e operare all'interno di reti protette. Gli attacchi basati su *malware* utilizzano *software* malevoli

[1] Clusit – Associazione Italiana per la Sicurezza Informatica, *Rapporto Clusit sulla cybersecurity in Italia e nel mondo*, 2025, www.clusit.it

[2] *Ibidem*.

[3] ENISA – European Union Agency for Cybersecurity, *Report on the State of the Cybersecurity in the Union, 2024*, www.enisa.europa.eu.

[4] ENISA – European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025*, www.enisa.europa.eu.

(quali *ransomware*, *spyware*, *trojan* e *worm*[5]) per compromettere i sistemi, sottrarre dati, esercitare controllo remoto o causare danni operativi; in questa categoria rientrano anche casi emblematici come Stuxnet e WannaCry, che evidenziano la capacità di propagazione e impatto su larga scala. Gli attacchi basati sulla rete, come DoS e DDoS[6], agiscono invece saturando le risorse di un sistema o intercettando le comunicazioni tramite tecniche di tipo *man-in-the-middle*[7], con l'obiettivo di interrompere servizi o manipolare il traffico informativo. A questi si aggiungono gli attacchi di ingegneria sociale, che sfruttano fattori psicologici per indurre gli utenti a rivelare informazioni sensibili o concedere accessi, spesso rappresentando la fase iniziale di operazioni più complesse. Infine, gli attacchi mirati ai dati comprendono attività di esfiltrazione, manipolazione e furto di informazioni, anche mediante tecniche come *SQL injection* o campagne di doppia estorsione[8], con finalità economiche, strategiche o di intelligence[9]. Questa classificazione evidenzia come le minacce cibernetiche si articolino in modalità eterogenee ma spesso interconnesse, contribuendo a rendere il cyberspazio un ambiente operativo altamente complesso e multifattoriale.

[5] *Ransomware*: crittografia di dati sensibili e blocco del sistema la cui restituzione è sottoposta al pagamento di un riscatto.

Spyware: *malware* per raccogliere/monitorare dati su utenti e trasferirli a terzi. Operano per infiltrazione, monitoraggio e acquisizione e trasmissione.

Trojan Horse: *malware* che infetta il dispositivo fingendosi un'applicazione legittima attraverso un codice dannoso in un file che una volta aperto si integra nel sistema e ne prende il controllo e consentendo attacchi con *software* più dannosi disabilitando i controlli di sicurezza.

Worm: capaci di infiltrarsi e propagarsi infettando altri dispositivi connessi.

[6] DoS (*Denial of Service*): sovraccarico dei sistemi e reti con richieste fraudolente, impedimento di funzioni di routine. DDoS (*Distributed Denial of Service*): versione più sofisticata della precedente che coinvolge più di un dispositivo amplificando la portata e rendendo l'attacco più difficile da rilevare.

[7] MitM (*Man in the Middle*): compromissione delle comunicazioni sicure tra un utente e un sito/applicazione (*client-server*) tramite la loro intercettazione e decrittazione.

[8] Doppia estorsione: furto di dati e ostaggio condizionato al pagamento di un riscatto, minaccia di pubblicazione SQL *Injection*: sfruttamento delle vulnerabilità dei database SQL per esporre e modificare dati sensibili senza autorizzazione.

[9] O. ASLAN,S. S. ACTUĞM. OZKAN-OKAY, A. A.YILMAZ, E.AKIN, *A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions*, in *Electronics*, v. 12 n. 6, 2023, p. 1333.

3. La weaponizzazione del cyberspazio nel contesto della guerra ibrida

Il termine cyberspazio fu inizialmente coniato negli anni '80 in ambito fantascientifico dal William Gibson[10] che, anticipando in maniera romanzata l'interconnessione globale di dati e sistemi su cui oggi si imperniano numerose attività umane, lo definiva «rappresentazione grafica dei dati ricavati dai computer del sistema umano, linee di luci allineate nel non-spazio della mente, ammassi e costellazioni di dati come luci di una città che si allontanano» [11]. L'odierna e pervasiva fiducia delle collettività nei confronti proprio di queste interconnessioni e la loro integrazione nella maggior parte delle attività economiche, politiche, sociali – e militari -, hanno rafforzato il lato oscuro del potenziale catalizzatore delle ITC, le quali secondo Henry Kissinger «sfidano ogni esperienza storica e dischiudono prospettive del tutto nuove» [12]. Questa consapevolezza ha portato a ridefinire lo spazio cyber da una narrazione prevalentemente fantascientifica ad una antropica e operativa: successivamente infatti il mondo accademico ha rielaborato il concetto per indicare l'insieme delle infrastrutture informatiche globali – *hardware*, *software*, dati e utenti – e delle relazioni che le collegano[13]. Esso configura uno spazio antropico, dinamico e a-territoriale, che trascende i confini fisici e ridefinisce le dinamiche del potere, concentrandolo nelle mani di chi controlla i flussi informativi e le tecnologie di comunicazione. Il controllo è allora elemento intrinseco: il prefisso "cyber"[14] deriva dal greco κυβερνήτης (kybernetes) ed indica proprio il timoniere, il pilota di una nave e dunque, per estensione, colui che governa e guida.

Rileggendo la teoria di Nye, l'ascesa di tale dominio segna una rottura della ciclicità della *translatio imperii* e fa tremare le fondamenta del realismo tradizionale, inaugurando un paradigma di distribuzione del potere che vede la prerogativa intrinseca dello Stato sovrano del monopolio della violenza e della forza erodersi per aprirsi invece ad attori terzi. La cosiddetta *commodification*[15] delle capacità nonché la proliferazione di

[10] G. Martino, *La quinta dimensione della conflittualità: il cyberspazio*, in *Centro Studi Strategici Internazionali e Imprenditoriali*, 2021.

[11] *Ibidem*.

[12] H. Kissinger, *World Order*, Penguin Press, New York, 2014, p. 344.

[13] Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico, Roma*, 2013, www.agid.gov.it.

[14] Definizione di "*cyber*", accademiadellacrusca.it.

[15] M.A. Cherry, *Cyber Commodification*, in *Maryland Law Review*, 2013, pp. 381 e ss.

soluzioni economiche e *open source* hanno progressivamente democratizzato potenzialità che riducono la soglia di accesso all'uso della forza ad attori non statali, mettendo così in crisi il concetto di "soggettività" nel diritto internazionale e aprendo nuovi interrogativi circa la responsabilità giuridica e, a monte, il concetto stesso di "forza" ai sensi delle valutazioni legali.

Sempre reinterpretando le categorie classiche degli studi strategici, la militarizzazione del cyberspazio può essere compresa alla luce di una rilettura del tradizionale *security dilemma* in chiave *dual-use*[16] e costruttivista. Le tecnologie digitali, infatti, sono intrinsecamente ambivalenti, potenzialmente impiegabili tanto per fini civili quanto militari, con una continua e bidirezionale traslazione tra i due ambiti. In un contesto internazionale caratterizzato da incertezza circa le intenzioni degli attori, questa natura duale amplifica la dinamica a spirale tipica del dilemma della sicurezza, alimentando una competizione tecnologica[17] che si traduce nella progressiva militarizzazione di nuovi domini, come quello in esame.

Ad una lettura costruttivista del dilemma della sicurezza a duplice uso, si comprende come le incertezze degli attori che agiscono sul terreno globale così come le loro reazioni alle stesse sono costruite socialmente. Il concetto di securitizzazione cristallizza efficacemente questa dinamica e mira a comprendere come e perché le élites etichettino questioni comuni come problemi di sicurezza prioritari in agenda[18], giustificando così misure straordinarie che possono, in *extrema ratio*, esulare dalle competenze regolari degli "attori securitizzanti". Se, dunque, la conseguenza primaria del *security dilemma* in chiave classica è la corsa alle armi e un incremento della forza militare aggregata nel sistema, possiamo sostenere che l'introduzione nell'equazione dei caratteri dei sistemi *dual-use* conducano ad una dinamica di militarizzazione di nuovi domini. In questo senso, il cyberspazio si afferma come terreno privilegiato di competizione strategica, in cui il controllo delle tecnologie e dei flussi informativi diventa un elemento centrale del potere.

[16] M.R. ATLAS, M. DANDO, *Il dilemma del duplice uso per le scienze della vita: prospettive, enigmi e soluzioni globali*, in *Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science,* 2006, 4(3), pp. 276 e ss.

[17] S. SCHMID, D. LAMBACH, C. DIEHL, C. REUTER, *Arms Race or Innovation Race? Geopolitical AI Development*, in *Geopolitics* 2025, pp. 1 e ss.

[18] O.WÆVER, *Securitization and Desecuritization*, *Centre for Peace and Conflict Research*, Copenhagen, 1993, p. 57.

Questo processo ha trovato una formalizzazione istituzionale a partire dalla seconda metà degli anni 2000, quando il cyberspazio è stato progressivamente riconosciuto come dominio operativo militare. In particolare, l'esperienza statunitense[19] evidenzia il passaggio da una concezione della cybersicurezza in chiave prevalentemente difensiva e criminale a una piena integrazione del dominio cyber nelle strategie di sicurezza nazionale, includendo capacità offensive, logiche di deterrenza e strutture dedicate come lo USCYBERCOM. Tale evoluzione riflette l'emergere di un paradigma in cui la difesa delle reti si accompagna alla possibilità di proiezione della forza nel dominio digitale.

Analoghi sviluppi, seppur più graduali, si riscontrano anche in altri contesti, come quello italiano, dove il riconoscimento del cyberspazio come quinto dominio dell'azione militare e l'istituzione di organismi dedicati segnano un progressivo allineamento alle dinamiche internazionali. Sebbene già nel 2020 fosse stato istituito il COR (Comando per le Operazioni in Rete), incaricato di coordinare le attività di sicurezza e difesa *cyber* della Difesa e posto sotto diretto comando dello Stato Maggiore della Difesa, si può affermare che l'Italia abbia formalmente preso parte al processo di militarizzazione del cyberspazio con la decisione, risalente al 2022, di modificare l'art. 88 del Codice dell'Ordinamento Militare (COM) che riconosce, in linea con la postura atlantica sebbene in ritardo, il *cyberspace* come quinto dominio dell'uso della forza militare. Nello specifico, l'articolo in questione sanciva che «*lo strumento militare è volto a consentire la permanente disponibilità di strutture di comando e controllo di Forza armata e interforze, facilmente integrabili in complessi multinazionali, e di unità terrestri, navali e aeree di intervento rapido, preposte alla difesa del territorio nazionale e delle vie di comunicazione marittime e aeree; è finalizzato, altresì, alla partecipazione a missioni anche multinazionali per interventi a supporto della pace*», formula alla quale viene aggiunto il riferimento alle «*unità cibernetiche e aerospaziali*» per la difesa dei nuovi domini spaziale e digitale. Questa modifica formale consentirebbe dunque all'apparato della Difesa di prepararsi ad azioni "offensive" sebbene nell'accezione edulcorata di "*active cyber defence*", in uno scenario di attacchi informatici contro le infrastrutture critiche in aumento. In tale direzione si collocano le posizioni espresse dal Ministro della Difesa Guido Crosetto, il quale ha sottolineato la necessità

[19] The White House, *National Security Strategy of the White House*, Washington, 2010, history.defense.gov.

di rafforzare le capacità nazionali nel dominio cibernetico[20], includendo strumenti di risposta attiva agli attacchi informatici in un'ottica di deterrenza. Il dibattito italiano evidenzia infatti una crescente apertura verso forme di "difesa attiva", pur nel rispetto dei vincoli costituzionali e del diritto internazionale.

Parallelamente, a livello europeo, emergono sviluppi più avanzati. In Germania[21], nel corso dell'ultimo anno, sono state elaborate proposte legislative volte ad ampliare i poteri delle agenzie di sicurezza e intelligence, consentendo interventi anche su infrastrutture digitali situate all'estero e introducendo forme di risposta attiva agli attacchi informatici. In particolare, i progetti normativi prevedono la possibilità di interrompere sistemi informatici, reindirizzare il traffico dati e persino modificare o cancellare informazioni su server stranieri, segnando un significativo ampliamento delle capacità operative statali nel cyberspazio. In parallelo, il dibattito politico tedesco ha registrato un ulteriore irrigidimento, con l'esplicita apertura all'adozione di misure di "*hack-back*", ossia operazioni di controffensiva[22] digitale volte a colpire infrastrutture ostili anche al di fuori del territorio nazionale. Tale evoluzione rappresenta un mutamento rilevante rispetto alla tradizionale cautela tedesca e contribuisce a consolidare, anche nel contesto europeo, una progressiva normalizzazione dell'impiego della forza nel cyberspazio.

4. L'applicazione del diritto internazionale al dominio cibernetico

La gestione delle nuove tecnologie digitali e del loro impatto sulla sicurezza internazionale è stata oggetto di un intenso dibattito in seno alle Nazioni Unite, che rappresentano il principale foro di confronto tra Stati su tali tematiche. In questo contesto, numerose iniziative, tra cui i lavori del *Group of Governmental Experts* (GGE)[23] e del *Open-Ended Working Group* (OEWG), hanno cercato di promuovere un quadro condiviso di

[20] A. CALABRESE, *Verso un'arma cyber nazionale: la strategia del Min. Crosetto nel contesto europeo*, in Geopolitica.info, 14 novembre 2025.

[21] M. WACKET, *German authorities to get more powers against foreign hackers, draft law shows*, in Reuters, 27 febbraio 2026, www.reuters.com.

[22] O. LUNGESCU, *Germany will 'strike back' against Russian cyber attacks, minister vows*, in *Financial Times*, 26 gennaio 2026, www.ft.com.

[23] Assemblea Generale delle Nazioni Unite, Risoluzione A/RES/73/266 – *Developments in the field of information and telecommunications in the context of international security*, 22 gennaio 2019.

comportamento responsabile nel cyberspazio e di chiarire l'applicabilità del diritto internazionale.

Nonostante il riconoscimento generale della rilevanza della Carta ONU e delle norme internazionali, persistono profonde divergenze tra gli Stati, in particolare circa l'applicazione del diritto internazionale umanitario e la qualificazione delle operazioni *cyber*. Tali fratture riflettono visioni strategiche e politiche contrapposte: da un lato, alcuni Stati sostengono un'estensione delle norme esistenti anche al dominio digitale; dall'altro, altri temono che ciò possa legittimare la militarizzazione del cyberspazio. La divergenza di visioni e posizioni è stata infatti tale da portare ad uno stallo nel processo di approvazione del rapporto finale GGE del 2017, che ricordiamo necessita del consenso di tutti i membri, in particolare a causa del rifiuto di Russia[24], Cina e Cuba[25] di includere il riferimento all'applicazione delle norme di diritto internazionale umanitario, delle contromisure e della legittima difesa nel *cyberspace*.

Il fatto che schieramenti opposti di Paesi sembrino talvolta ricercare, anche strategicamente, ambiguità e vaghezza nella definizione di un framework vincolante – così da preservare margini di manovra coerenti con le proprie interpretazioni di ciò che è consentito – unito alla persistente mancanza di fiducia reciproca, rafforza il pessimismo circa l'efficacia di tali strumenti nel produrre regole chiare e universalmente condivise. L'impraticabilità di un consenso globale pieno induce pertanto a considerare soluzioni alternative, quali lo sviluppo di quadri normativi limitati tra gruppi ristretti di Stati accomunati da visioni affini, all'interno dei quali le divergenze giuridiche possano essere più agevolmente affrontate e progressivamente armonizzate.

In questa prospettiva, un modello di riferimento è rappresentato da iniziative come il *Manuale di Tallinn sul diritto internazionale applicabile alla guerra informatica*, frutto del lavoro di esperti sull'applicabilità del diritto internazionale alla *cyber warfare*, i cui risultati potrebbero essere progressivamente estesi ad un numero più ampio di Stati secondo una logica di diffusione incrementale (*spillover*). Pubblicato nel 2013 e poi aggiornato nel 2017, questo prodotto giuridicamente non vincolante mira ad analizzare l'applicazione dello *jus ad bellum* e dello *jus in bello*

[24] Ministero degli Affari Esteri della Federazione Russa, *Statement on International Information Security*, 6 aprile 2017, www.mid.ru.

[25] *Declaration on International Law Related to the Use of ICTs in the Context of International Security*, 2017, www.justsecurity.org.

al contesto informatico attraverso 154 "*Rules*" redatte da un gruppo internazionale e multidisciplinare di esperti, su mandato del Cooperative Cyber Defence Centre of Excellence di Tallinn. Lungi dall'avere valore di legge[26], tuttavia queste "*Rules*" possono essere considerate un esercizio di "s*oft codification*", collocandosi dunque a metà tra *lex lata* e *lex ferenda*, in quanto consente, pur non avendo valore giuridico obbligatorio, di influenzare significativamente la prassi e l'evoluzione normativa[27].

Diviso in quattro sezioni, ognuna dedicata ad indagare uno specifico settore del diritto internazionale generale, il Manuale tenta di colmare una delle lacune più dibattute sul tema: la qualificazione giuridica della *cyberforce* alla luce dei suoi caratteri ambigui e che sfuggono alle categorie classiche (territorio, danno, responsabilità) e il fatto che, ad oggi, non si siano ancora manifestati casi di cyber attacchi che abbiano scatenato un conflitto armato tra Stati e la maggior parte delle attività malevole non incontrino oggi la soglia di scala ed effetti necessari alla definizione di un attacco armato. Quanto alla proibizione dell'uso della forza sancita dall'art. 2, par. 4 della Carta ONU, nel parere circa la legittimità delle armi nucleari del 1998 la Corte Internazionale di Giustizia (CIG) chiarisce che gli articoli riguardanti l'uso della forza «non si riferiscono ad armi specifiche […] La Carta non proibisce né permette esplicitamente l'uso di specifiche armi»[28]. Degno di nota è poi l'art. 36 del Primo Protocollo Addizionale alle Convenzioni di Ginevra, il quale sancisce che «*nello studio, sviluppo, acquisizione o adozione della nuova arma, mezzo o metodo di guerra, la Parte Contraente ha l'obbligo di determinare se l'uso degli stessi sia, in alcune o in ogni circostanza, proibita dal presente Protocollo o da qualsiasi altra regola di diritto internazionale applicabile alla Parte*». Coerentemente, la regola n. 11 del Manuale decreta che un'operazione *cyber* costituisce un uso della forza quando la sua portata ed effetti sono comparabili ad operazioni cinetiche che raggiungono la soglia dell'uso della forza, riprendendo così la prassi della CIG nel caso delle Attività militari e paramilitari in e contro il Nica-

[26] M. SCHMITT, *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, in *Georgetown Journal of International Law*, 2017, pp. 403 e ss.

[27] A. CALABRESE, *Cyberwar e diritto internazionale: la frontiera digitale del conflitto armato tra principi umanitari, responsabilità e protezione dei civili*, Università degli Studi di Torino, 2025.

[28] Corte Internazionale di Giustizia, Parere consultivo sulla legittimità della minaccia o dell'uso delle armi nucleari, 8 luglio 1996, www.icj-cij.org.

ragua (1986)[29]. Tuttavia, si segnala come tale definizione e approccio comparativo rischi di essere dirimente rispetto alla categorizzazione di una serie di operazioni psicologiche non distruttive o PSYOPS virtuali che, sebbene non raggiungano la soglia dell'uso della forza, sono potenzialmente lesive dell'integrità sovrana. Paragonabili a forme di pressione politica, economica e psicologica[30] non considerate uso della forza per il diritto internazionale classico, tali operazioni nello spazio *cyber* possono assumere "forme gravi di propaganda da parte di Stati Nazionali di tipo guerrafondaio, sovversivo, e diffamatorio costituiscono una minaccia alla pace"[31], con effetti ancor più diffusi e incontrollati. Il Manuale, inoltre, propone 8 criteri indicativi per la valutazione di un'operazione *cyber* sotto il profilo dell'uso della forza:

1. *Severità*: azioni che causano danni gravi (distruzione, feriti, morte o impatto su interessi nazionali critici) sono più facilmente considerate uso della forza. Atti di minima gravità (principio *de minimis*) o alcune attività come misure di polizia e operazioni di *active cyber defence* non superano questa soglia.
2. *Immediatezza*: effetti immediati rendono più probabile la qualificazione come uso della forza, perché limitano la possibilità di risposta pacifica. Operazioni *cyber* possono invece avere effetti ritardati e difficilmente attribuibili.
3. *Directness (nesso causale)*: più il legame tra azione e conseguenze è diretto, più è probabile parlare di uso della forza. Nel *cyber* questo legame è spesso difficile da dimostrare.
4. *Invasività*: riguarda il livello di intrusione nei sistemi di uno Stato. Maggiore è la penetrazione (soprattutto in sistemi critici o governativi), maggiore è la rilevanza dell'atto.
5. *Misurabilità degli effetti*: nel *cyberspace* è complesso valutare i danni. Si considerano sia parametri tecnici (dati compromessi, sistemi colpiti) sia effetti operativi, economici e reputazionali, oltre a possibili conseguenze indirette nel mondo fisico.

[29] Corte internazionale di giustizia, sent. 27 giugno 1986, *Attività militari e paramilitari in e contro il Nicaragua* (*Nicaragua c. Stati Uniti d'America*).

[30] Simma, B. Khan, D.-E. Nolte, G. Paulus, *The Charter of the United Nations – A Commentary, vol. I*, Oxford University Press, Oxford, 2012.

[31] G.P. Pierini, *The Legal Framework for Psychological Operations and Influence Operations Under International Law, the Law Applicable to Armed Conflict and International Criminal Law*, in *Rassegna della giustizia militare* 2020, www.giustiziamilitare.difesa.it.

6. *Carattere militare*: un collegamento con attività o obiettivi militari facilita la qualificazione come uso della forza. È tuttavia interessante riflettere attorno alla natura ambigua e cangiante che le nuove tecnologie hanno conferito alla guerra contemporanea: oggi il perseguimento dell'interesse statale nell'ambiente cibernetico passa attraverso la *covert action* di enti parastatali affiliati e dotati di capacità *cyber* raffinate, non direttamente inserite nel tessuto "armato" e "militare" dello Stato.
7. *Coinvolgimento dello Stato*: più è chiaro il legame tra operazione e Stato, più è probabile parlare di uso della forza. Tuttavia, la presenza di attori "proxy" rende spesso difficile l'attribuzione.
8. *Presunta legalità*: attività non espressamente vietate (es. spionaggio, propaganda) sono generalmente considerate lecite. Inoltre, l'uso della forza può essere giustificato in alcuni casi (legittima difesa, autorizzazione ONU, consenso dello Stato colpito, e secondo alcuni anche intervento umanitario o difesa preventiva).

La definizione del concetto di uso della forza è alla base della categorizzazione di attacco armato che, ai sensi dell'art. 51 della Carta Onu, innescherebbe il legittimo uso della forza per legittima difesa. L'International Group of Expert condusse un complesso dibattito attorno alla nozione di "attacco armato" e arrivò a sostenere unanimemente che, dal momento che oggi le armi *cyber* producono effetti distruttivi e irreparabili quanto quelle convenzionali, la scelta del mezzo per compiere l'aggressione non influenza la classificazione di un'operazione come attacco armato, richiamando la conclusione della CIG nel parere circa la legittimità delle armi nucleari. Nella sentenza Nicaragua, infatti, la Corte si concentra sulla "portata e gli effetti" delle operazioni e non sui mezzi[32]. Tuttavia, i parametri di "*scale and effect*" rimangono sfumati e indefiniti: se, in casi in cui l'uso della forza ferisce o causa la morte di persone o implica la distruzione o il danneggiamento fisico di proprietà determinati criteri sarebbero soddisfatti, usi della forza che non risultano in ferimento, morte, distruzione e danneggiamento ma che inducono comunque a conseguenze nefaste estese rimangono dunque incerti. Questa riflessione assume particolare rilevanza alla luce dei crescenti

[32] Corte internazionale di giustizia, sent. 27 giugno 1986, *Attività militari e paramilitari in e contro il Nicaragua* (*Nicaragua c. Stati Uniti d'America*).

attacchi alle vulnerabili infrastrutture critiche, che per altro ricoprono ormai una duplice funzione civile e strategico-militare: Si immagini, ad esempio, il caso di un'operazione diretta contro le componenti di un impianto di purificazione idrica: gli effetti nefasti attesi sulla salute e l'incolumità della popolazione rientrerebbero tra gli elementi da considerare, al di là dell'effettivo ferimento, morte o distruzione[33].

Al fine di fornire un quadro operativo e maggiormente applicabile nella pratica per la qualificazione di un'operazione cyber come attacco armato, è possibile combinare un approccio quantitativo, basato sulla misurazione degli effetti (fisici, economici e sociali), con un approccio qualitativo, fondato sulla natura e sulle modalità dell'attacco. Tale impostazione prende ispirazione dai modelli di categorizzazione sviluppati da alcuni Stati, in particolare Francia[34], Regno Unito[35] e Paesi Bassi[36-37], che hanno proposto criteri basati rispettivamente sulla severità degli effetti, sull'impatto sugli *asset* nazionali e sull'identificazione dei processi vitali dello Stato. L'integrazione di questi approcci consente di individuare soglie più concrete e di strutturare una classificazione tripartita delle operazioni cyber, distinguendo tra attacchi direttamente comparabili a quelli cinetici, attacchi indirettamente dannosi e operazioni che producono prevalentemente effetti di disgregazione sociale. Il risultato di tale approccio integrativo è proposto e sintetizzato nella seguente tabella:

[33] A. Calabrese, *Cyberwar e diritto internazionale: la frontiera digitale del conflitto armato tra principi umanitari, responsabilità e protezione dei civili*, op.cit.

[34] Ministero delle Forze Armate francese, *Droit international appliqué aux opérations dans le cyberespace*, Parigi, 2021, www.defense.gouv.fr.

[35] Discorso del procuratore Generale del Regno Unito J. Wright QC, *Cyber and International Law in the 21st Century*, in Chatham House, 23 maggio 2018, www.gov.uk.

[36] Coordinamento Nazionale per l'antiterrorismo e la sicurezza olandese (NCTV), *Overzicht vitale processen*, www.nctv.nl.

[37] F.M.E. Oosprong, P.A.L. Ducheine, B.M.J. Pijpers, *Armed Attack in Cyberspace: Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands' Right of Self-Defence*, cit., pp. 13 e ss.

Categoria	**Esempi pratici** *(di beni di sicurezza 'core' interrotti, degradati o distrutti)*	**Caratteristiche**	**Criteri contributivi** *(dal più importante al meno importante)*
I	- Produzione, stoccaggio e lavorazione di **materiale nucleare** (portando a un disastro nucleare) - **Barriere idriche** (portando a inondazioni catastrofiche) - Produzione/lavorazione/stoccaggio su larga scala di **sostanze (petro) chimiche** (portando a un disastro ecologico) - **Controllo del traffico aereo** (portando a disastri aerei) - **Capi di stato** (portando al loro assassinio)- **Servizi medici essenziali** (portando alla morte di pazienti)	- comparabili ad attacchi cinetici- direttamente collegati a danni fisici- intrinsecamente pericolosi	(a) un **danno fisico diretto** di 1 o più persone morte (b) un **danno sociale** a **100.000** persone con gravi problemi di sopravvivenza sociale (c) un **danno economico** di almeno **5 miliardi di euro**
II	- Produzione, distribuzione e trasporto di **elettricità, gas e petrolio** (causando la loro indisponibilità) - **Fornitura di acqua pulita** (portando alla scarsità di acqua potabile) - **Reti di comunicazione** (necessarie per il mantenimento dell'ordine pubblico)	- comparabili ad attacchi cineticiindirettamente portano a danni fisici	(a) un **danno fisico indiretto** di oltre **1.000** persone morte, gravemente ferite o malate croniche (b) un **danno sociale** da **100.000 – 1.000.000** di persone con gravi problemi di sopravvivenza sociale (c) un **danno economico** tra **5 miliardi – 50 miliardi di euro**
III	- **Sistemi finanziari** (inclusi i processi di pagamento governativi per la tassazione) - **Internet stesso** (disattivazione delle infrastrutture digitali o servizi necessari al funzionamento della società)	- non comparabili ad attacchi cinetici- collegati a "disgregazione sociale"	**"Disgregazione sociale"**, il criterio più difficile per questa categoria, potrebbe essere raggiunto con: (a) un **danno sociale** ad almeno **1.000.000** di persone (come minimo assoluto) (b) un **danno economico** di almeno **50 miliardi di euro** (come minimo assoluto)

La Categoria I rientra più chiaramente nell'attacco armato, in quanto

include operazioni con effetti diretti e immediati comparabili a quelli cinetici, soprattutto in presenza di danni fisici. La Categoria II rappresenta una zona intermedia: può configurare un attacco armato solo se gli effetti indiretti raggiungono una soglia elevata in termini di vittime, impatto sociale o danno economico. La Categoria III, infine, difficilmente integra un attacco armato, salvo casi eccezionali di impatto sistemico estremamente grave.

5. *Diritto internazionale umanitario e operazioni* cyber*: distinzione, indiscriminazione e proporzionalità*

Se il contributo sino ad ora ha indagato l'applicabilità dello *jus ad bellum* ovvero delle norme consuetudinarie di diritto internazionale e Carta ONU o "il diritto di fare la guerra", l'analisi prosegue con una necessaria riflessione circa l'applicazione e l'adattamento dello *jus in bello* e dei principi di diritto umanitario internazionale, applicabili durante un conflitto armato e che mira a limitare gli effetti delle ostilità.

Vi è generale consenso, almeno tra gli Stati occidentali, attorno al fatto che il diritto umanitario si applica a tutte le operazioni cyber condotte in contesto di conflitto. Come osservato, le capacità *cyber* offrono ormai possibilità tali da rendere operazioni offensive veri e propri attacchi ai sensi del DIU e richiedono dunque una riflessione circa l'adeguatezza e l'applicazione di determinati principi, primo fra tutti il principio di distinzione cristallizzato nell'art. 48 del Protocollo Addizionale I alle Convenzioni di Ginevra: «*in modo da assicurare il rispetto e la protezione della popolazione civile e degli oggetti civili, le Parti del conflitto dovranno sempre distinguere tra la popolazione civile e i combattenti e tra gli oggetti civili e gli obiettivi militari e, di conseguenza, dovranno dirigere le loro operazioni solo contro obiettivi militari*»[38]. Due criticità emergono guardando all'estensione di tali principi all'uso degli strumenti cibernetici in guerra. Da un lato, eventi recenti come l'attacco alla rete terrestre del satellite KA-SAT di Viasat nel febbraio 2022 poche ore prima dell'inva-

[38] L'art. 52, par. 1 riprende e amplia questa protezione anche agli oggetti civili, dei quali viene data una definizione "negativa": gli oggetti civili sono oggetti non militari, e questi ultimi sono definiti come quegli oggetti, beni, infrastrutture che «per la loro natura, localizzazione, scopo o uso contribuiscono in maniera effettiva all'azione militare e la cui totale o parziale distruzione offre un effettivo vantaggio militare». Nel contesto cyber, oggetti militari possono includere computer, reti, e infrastrutture cibernetiche ossia i sistemi C4ISR (*military command, control, communications, computer, intelligence, surveillance and reconnaissance*).

sione ucraina da parte di gruppi filorussi[39] hanno dimostrato la centralità e la vulnerabilità delle infrastrutture critiche dual-use: il target in oggetto forniva comunicazioni satellitari e servizi internet ad infrastrutture civili in Ucraina oltre che supportare i servizi di sicurezza e le forze armate ucraine[40]. L'attacco ha inibito le sue funzioni e reso inutilizzabili migliaia di modem di privati ma anche di agenzie governative, causando impatto anche su clienti in Polonia, Germania, Regno Unito, Francia e Repubblica Ceca. L'effettivo uso per scopi militari rende queste infrastrutture un obiettivo strategico e legittimo, ma interferenze su larga scala possono causare danni sproporzionati ai civili anche indiretti, violando il principio di proporzionalità e configurandosi come un attacco indiscriminato, in violazione dei principi di DIU. Qui si insinua, dunque, il secondo dilemma: le Convenzioni di Ginevra proibiscono l'uso di qualsiasi mezzo o metodo di guerra che non può essere diretto contro un obiettivo specifico ed è intrinsecamente indiscriminato nel suo funzionamento, e i cui effetti non possono essere limitati come necessario nel rispetto delle Convenzioni. Alcuni strumenti utilizzati per compiere operazioni cibernetiche offensive presentano caratteristiche potenzialmente in contrasto con il rispetto di alcuni principi e intrinsecamente indiscriminati: basti pensare a Wannacry e NotPetya[41], *worms* capaci di auto-diffusione all'interno dei sistemi operativi e reti in maniera non controllata e indiscriminata. Allo stesso modo gli attacchi DDos sfruttano dispositivi compromessi per propagarsi, come dimostrano le recenti botnet IoT derivate da Mirai[42], che infettano automaticamente migliaia di dispositivi (router, telecamere, ecc.) trasformandoli in nodi di attacco distribuito, con effetti spesso indiscriminati e difficilmente controllabili. Casi studio come quello di Stuxnet[43], il famoso *malware* che si presume USA e Israele abbiano

[39] CONSIGLIO DELL'UNIONE EUROPEA, *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union*, 10 maggio 2022.

[40] E. NAKASHIMA, *Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say*, The Washington Post, 24 marzo 2022, www.washingtonpost.com.

[41] L. GISEL, T. RODENHAUSER, K. DÖRMANN, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, cit., p. 294.

[42] V. MIRAI, *IoT Botnet: Behind Record-Breaking DDoS Attack*, www.vulnu.com.

[43] Stuxnet è un *malware* altamente sofisticato scoperto nel 2010 e considerato uno dei primi esempi di arma informatica capace di produrre effetti nel mondo reale. Progettato per colpire specifici sistemi industriali (SCADA *systems*) in Iran alla base del controllo delle centrifughe nucleari per l'arricchimento di uranio, il virus si diffondeva attraverso reti informatiche e dispositivi come chiavette USB, individuando sistemi che

impiegato contro l'impianto nucleare iraniano di Natanz, dimostrano che a livello tecnico è possibile sopperire alla lacuna dell'indiscriminazione dell'attacco attraverso alcune soluzioni, sebbene molto sofisticate e dunque non di portata universale[44]. In particolare, è possibile ridurre i rischi di propagazione incontrollata attraverso pratiche di weaponizzazione mirata[45], con *exploit* e *payload*[46] che funzionano solo su determinate versioni o configurazioni di sistemi. Analogamente, l'utilizzo di *kill switch* e sistemi di disattivazione automatica permette di contenere temporalmente gli effetti dell'operazione, migliorandone la prevedibilità e la controllabilità. Ulteriori strumenti, quali la validazione preventiva del *target* e il *testing* in ambienti simulati (*sandbox*)[47], contribuiscono a garantire che l'azione sia effettivamente diretta verso obiettivi militari specifici, minimizzando i danni collaterali. Infine, lo sviluppo di *payload* modulari e altamente specializzati consente di calibrare l'impatto dell'attacco in funzione dell'obiettivo, rafforzando il rispetto dei principi di distinzione e proporzionalità. Il caso Stuxnet è interessante da analizzare: sebbene la controllabilità fosse garantita da alcuni aspetti come un'alta conoscenza[48] della tipologia di PLC[49] utilizzati nei sistemi da attaccare grazie ad attività di intelligence e il conseguente sviluppo di un malware specializzato che si attivava solo su quegli specifici sistemi, il virus si propagò installandosi nelle reti Windows di diversi paesi infettando più di 60 mila computer (anche civili), situati per la metà in Iran ma coinvolgendo anche India, Indonesia, Cina, Azerbaigian, Corea del Sud, Malesia, Stati Uniti, Regno Unito, Australia,

utilizzavano il software Siemens Step7. Una volta infiltrato, alterava il funzionamento delle macchine senza essere rilevato, causando danni fisici all'impianto e rallentando il programma nucleare di Teheran.

[44] L. Gisel, T. Rodenhauser, E K. Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, cit., p. 295.

[45] Darktrace Glossary, *What is the Cyber Kill Chain*?, www.darktrace.com.

[46] *Exploit*: sequenza di comandi o codice che sfrutta una vulnerabilità di un sistema o di applicazione per ottenere un comportamento non previsto (es. accesso non autorizzato); Payload: porzione dell'exploit che, una volta eseguita, compie l'azione desiderata dall'attaccante (es. apertura di una backdoor per l'accesso, esfiltrazione di dati).

[47] A. Boström, A. Hylander, *Selecting Better Attacks for Cyber Defense Exercises – Criteria to Enhance Cyber Range Content*, Linköping University, Department of Computer and Information Science, 2024, p. 25.

[48] A. Basu, K. Saini, *Setting International Norms of Cyber Conflict Is Hard, but That Doesn't Mean We Should Stop Trying,* in *Modern War Institute at West Point*, 2019.

[49] Un PLC (*Programmable Logic Controller*) è un computer industriale utilizzato per controllare automaticamente macchinari e processi in ambito produttivo.

Finlandia e Germania[50]. Benché inoltre, vi fosse un termine di scadenza delle attività di intrusione, il malware viola il concetto di controllabilità e di limitazione e predicibilità degli effetti nonché di non propagazione, esponendo target civili a danni collaterali e aumentando la possibilità di alterare e replicare il codice in maniera malevola e incontrollata attraverso tecniche di *reverse engineering*[51], presentando quindi riflessioni circa il rispetto del principio di proporzionalità e precauzione.

6. *Verso una metodologia di* Collateral Damage Estimation *nel cyberspazio*

Proprio il principio di proporzionalità è il secondo pilastro del Diritto umanitario dei conflitti armati, cristallizzato negli articoli 51, par. 1 e 57, par. 2 del Protocollo Addizionale I. Riprendendo le succitate norme, la regola n. 51 del Manuale di Tallinn esplicita che un cyber attacco che ci si aspetta possa causare perdita di vite umane, ferimento di civili, danni a oggetti e beni civili o una combinazione degli stessi, che sarebbe eccessiva in relazione al concreto e diretto vantaggio militare previsto, è proibito. È evidente che il concetto di eccessività è vago, tuttavia relativo ad una valutazione del vantaggio militare[52] atteso date le circostanze, manifestando il principio di bilanciamento tra le necessità di guerra e i principi umanitari proprio del DIU[53]. Il termine "previsto" rispetto al vantaggio militare indicano che sia necessaria una valutazione delle circostanze al momento della pianificazione e dell'attacco al fine di determinare se questo sia proporzionato o no. Si situano in questo solco le metodologie di *Collateral Damage Estimation*, ovvero approcci volti a misurare e va-

[50] P. FARWELL, R. ROHOZINSKI, *Stuxnet and the future of Cyber War*, in *Survival*, 53 (1), 2011, p. 23.

[51] Il *reverse engineering* è un processo con cui un attaccante può utilizzare un malware già esistente retro-analizzando e decostruendo il codice alla fonte al fine di condurre un'operazione diversa cambiandone le funzionalità e gli obiettivi. Anche in case, dunque, di casi di attacco cyber leciti e tecnicamente limitati nella loro portata e targeting, il *reverse engineering* va considerato come potenziale fattore di impatto indiretto. E' stato inoltre riportato nel 2018 che oltre 22 milioni di sezioni di malware hanno utilizzato la logica operativa di Stuxnet per colpire Stati e organizzazioni.

[52] C. BRUDERLEIN, *Manual on International Law Applicable to Air and Missile Warfare, Program on Humanitarian Policy and Conflict Research at Harvard University*, 2009, p. 17 ss.

[53] J.K., KLEFFNER, *Section IX of the ICRC Interpretive Guidance on Direct Participation in Hostilities: The End of Jus in Bello Proportionality as We Know It?*, in I*srael Law Review*, 45, n. 1, 2012, p. 41.

lutare il numero di civili coinvolti come effetto collaterale di un attacco o altri danneggiamenti/danni a oggetti ed ambiente.

Per ciò che concerne il contesto *cyber*, la valutazione degli effetti sui civili si fa più complessa: sebbene alcuni danni prevalentemente fisici possano essere comparabili in termini qualitativi a quelli inflitti da operazioni cinetiche, vi sono comunque alcune differenze in quanto la compromissione di dati sensibili e personali potrebbe anch'essa essere considerata un danno ai sensi del DIU. Inoltre, particolare rilevanza assumono gli effetti indiretti: l'immediatezza sostanziale e diretta delle conseguenze può non essere esplicita in quanto spesso operazioni cibernetiche, soprattutto se dirette a infrastrutture critiche e *dual-use*, hanno *knock-on effects*[54] o effetti cascata potenzialmente più estesi in virtù della sempre più consolidata interconnessione e dipendenza tecnologica servizi essenziali da reti e infrastrutture digitali. A titolo di esempio, nel 2015 un gruppo filorusso colpì con il *malware* BlackEnergy3 una rete energetica disattivando più di trenta stazioni e lasciando senza energia oltre 230.000 persone per diverse ore[55]. È discutibile dunque se tale manovra sia proporzionata, avendo colpito utenze domestiche civili ma anche imprese e servizi essenziali come sistemi idrici, riscaldamento (rilevante per le peculiarità climatiche del territorio e la stagione invernale), comunicazioni e sistema sanitario.

Occorre dunque reinterpretare i paradigmi tradizionali di *Collateral Damage Estimation* (CDE) alla luce delle sfide che impone il nuovo contesto digitale e la sua militarizzazione. La metodologia CDE si configura come un processo strutturato volto a valutare e minimizzare i danni collaterali nel rispetto dei principi di distinzione e proporzionalità, e può essere adattata al dominio cibernetico attraverso un'estensione dei suoi criteri tradizionali. È un corpo di standard congiunti, metodi e tecniche per condurre l'analisi e produrre stime sui *collateral damage* nel processo di targeting. Ad oggi la metodologia statunitense contenuta nel US CJCSI 3160.01, "*No-Strike and the Collateral Damage Estimation Methodology*" serve come framework di riferimento per la metodologia emergente in ambito NATO[56]. Essa consta di 5 fasi. In una prima fase, si procede con

[54] V. Palleti, S. Adepu, V. Mishra, et al., *Cascading effects of cyber-attacks on interconnected critical infrastructure*, in *Cybersecurity*, n. 4, 2021.

[55] J. Styczynski, N.E Beach-Westmoreland, *When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure*, Booz Allen Hamilton, 2016.

[56] CJCSI, *Joint Targeting Cycle and Collateral Damage Estimation Methodology* (CDM), 2009, www.aclu.com.

l'*identificazione e validazione del target,* verificando la possibilità di una *positive identification* (PID) e la sua natura militare; nel contesto cyber, tale operazione risulta più complessa, in quanto il bersaglio può articolarsi su più livelli (fisico, logico e umano) e presentare ambiguità geospaziali o caratteristiche dual-use. La seconda fase interessa invece un'analisi più approfondita del target, che nel cyberspazio richiede la *comprensione dell'architettura dei sistemi* (*client-server*, *cloud*, distribuiti), delle interdipendenze con reti civili e delle vulnerabilità tecniche, al fine di individuare potenziali effetti a catena derivanti dall'interconnessione delle infrastrutture digitali[57]. La terza fase riguarda la *valutazione degli effetti e delle alternative operative*, nella quale l'impatto dell'operazione viene stimato non solo in termini fisici, ma anche secondo parametri di diffusione (scala spaziale), durata (scala temporale) e probabilità, elementi particolarmente rilevanti nel dominio *cyber* dove gli effetti possono propagarsi oltre il target iniziale. In questa fase, è essenziale bilanciare tali effetti con il vantaggio militare atteso e considerare soluzioni alternative o configurazioni tecniche dell'attacco che consentano di ridurre i rischi. Successivamente, una *refined analysis* permette di affinare la stima dei danni collaterali attraverso modelli più complessi e probabilistici, superando l'approccio tradizionale basato sulla distanza e integrando variabili tipiche del cyberspazio, quali la propagazione del codice, le dipendenze sistemiche e l'impatto su servizi essenziali. Infine, la fase conclusiva prevede la *minimizzazione degli effetti indesiderati e la decisione operativa*, attraverso l'adozione di misure tecniche di contenimento (ad esempio limitazione della diffusione, *kill switch*, segmentazione del *targeting*) e sistemi di monitoraggio continuo che consentano una rivalutazione dinamica dell'operazione. Se queste misure di controllo sono considerate inefficaci, dovrebbe essere selezionato un altro bersaglio o, in caso di ambiguità circa la valutazione di effetti collaterali fino all'ultimo e quinto stadio, l'operazione andrebbe annullata o sospesa[58]. In tale prospettiva, l'adattamento della CDE al dominio cibernetico richiede un approccio più flessibile, sistemico e probabilistico, capace di tenere conto della natura interconnessa, non lineare e spesso imprevedibile degli effetti delle operazioni cyber.

La seguente tabella riepiloga il modello integrato per un possibile *framework* di valutazione CDEM (*Collateral Damage Estimation Metho-*

[57] S. ROMANOSKY, Z. GOLDMAN, *Understanding Cyber Collateral Damage, in Procedia Computer Science*, vol. 95, 2016, pp. 10-17.

[58] C. MAATHUIS, W. PIETERS, J. VAN DEN BERG, *Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations*, cit., p. 440.

dology) specifico per le operazioni cibernetiche, sulla base di quanto esposto e analizzato in precedenza e in riferimento agli attuali quadri metodologici esistenti per l'assessment di mezzi cinetici.

Fase	Parametro di valutazione	Descrizione	Valori
Fase 1: Identificazione e Validazione del *Target*	1. *Layer* coinvolto 2. legittimità militare del bersaglio 3. ambiguità geospaziale	1. identificare il livello 2. verifica au senso del DIU: natura, scopo e uso del *target* 3. valutazione della possibile precisa geolocalizzazione e distinzione	1. *physical/logical/*persona layer 2. si/no/ambiguo (possibile dual-use?) 3. preciso/parziale/non determinabile
Fase 2: Analisi del *target*	4. architettura del sistema 5. interdipendenze civili 6. funzioni e traffico 7. misure di difesa	4. tipologia tecnica del sistema 5. coinvolgimento diretto o indiretto con sistemi civili 6. natura del traffico di rete, protocollo, funzioni operative 7. valutare protezioni e vulnerabilità	4. *Client-Server* / Distribuito / *Cloud* / *Legacy* / SCADA / *Dual-Use* / *Mesh* / Segmentato 5. Nessuna / Moderate / Estese / Incerte 6.Input/output critici, traffico condiviso, protocollo obsoleto.. 7. *Firewall*, VPN, IDS, cifratura, segmentazione
Fase 3 : Valutazione degli effetti	8. Impatto spaziale stimato 9. Impatto temporale stimato 10. Probabilità del danno collaterale 11. Severità dell'impatto civile 12. Vantaggio Militare Atteso 13. Esistenza di alternative operative	8. Scala geografica dell'effetto collaterale 9. Durata attesa dell'effetto 10. Stima probabilistica basata su analisi tecnica e di scenario 11. Tipo di danno atteso su persone o oggetti civili 12. Effetto previsto su decisioni nemiche, persistenza, reversibilità 13. Esistono opzioni con minore rischio collaterale?	8. *Target* / *Network of Target* / *National* / *Regional* / *Global* 9. 0–1h / 1h–1d / 1d–1w / 1w–1m / 1m–6m / 6m–1y / 1y–3y 10.Nullo (0%) / Basso (0–25%) / Moderato (25–50%) / Alto (50–75%) / Molto alto (75–100%) 11. Lieve / Moderato / Grave / Letale (secondo scala NATO/DoD) 12. Basso / Moderato / Alto / Strategico 13. si/no/parzialmente
Fase 4: Valutazione Effetti Collaterali (Refined Analysis)	14. Matrice di rischio Proporzionalità vs Vantaggio 15. Tollerabilità giuridica del danno collaterale	14. Valutazione incrociata tra scala dei danni con vantaggio militare per valutare proporzionalità 15. Il danno stimato è tollerabile secondo DIU?	14. Proporzionato / Discutibile – rivalutare / Disproporzionato – sconsigliato 15. Accettabile / Tollerabile con modifiche / Non accettabile
Fase 5 Minimizzazione e Decisione Finale	16. Misure di mitigazione previste 17. Decisione finale sull'operazione 18. Sistemi di monitoraggio e revisione	16. Malware auto-contenuto, kill-switch, *targeting* segmentato, esclusione *target* civili, simulazioni 17. Sulla base di tutto quanto emerso, l'operazione è lecita e proporzionata? 18. Sono attivi sistemi per rivalutare l'operazione in tempo reale?	16. Indicare misure adottate 17. Autorizzata / Autorizzata con modifiche / Non autorizzata 18. Si/no/parziali

7. *Conclusioni*

In un'epoca in cui la tecnologia digitale permea ogni aspetto delle relazioni internazionali e dei conflitti armati, la necessità di reinterpretare e rafforzare il diritto internazionale alla luce dei nuovi ambiti di guerra diventa ineludibile. Le operazioni nel dominio cibernetico, caratterizzate da interconnessione globale, dipendenze sistemiche e possibilità di effetti non lineari e diffusi, mettono in crisi concetti tradizionali del diritto come "danno", "violenza", "attacco" e "distinzione", che sono stati storicamente formulati per scenari di conflitto cinetico. Nel cyberspazio, un'azione tecnica apparentemente circoscritta può riverberarsi su infrastrutture civili essenziali – reti elettriche, sistemi sanitari, servizi pubblici – producendo conseguenze che sfuggono alle categorie giuridiche consolidate e rischiando di esporre la popolazione civile a rischi gravi e diffusi. È proprio in questo contesto che il diritto internazionale umanitario (DIU), con la sua attenzione alla protezione delle persone non coinvolte nelle ostilità, si trova a confrontarsi con sfide senza precedenti: la protezione dei civili non è più un principio astratto ma un imperativo operativo che richiede strumenti di regolazione e valutazione adeguati alla complessità tecnologica contemporanea.

Le operazioni *cyber offensive*, se non progettate con criteri di discriminazione, controllabilità e limitazione degli effetti, rischiano di violare i principi fondamentali del DIU, in particolare quelli di distinzione, proporzionalità e precauzione. L'esempio di casi come Stuxnet dimostra che anche strumenti tecnicamente sofisticati, pur essendo mirati a obiettivi ritenuti legittimi, possono produrre effetti collaterali estesi e non previsti, sollevando dubbi sulla loro conformità ai vincoli giuridici internazionali. Allo stesso modo, attacchi basati su malware auto-propaganti o su botnet illustrate nelle operazioni DDoS evidenziano come la mancanza di controllabilità nella diffusione possa tradursi in danni a infrastrutture civili critiche, erodendo la distinzione tra obiettivi militari e non militari.

In questo scenario, l'articolo ha inteso mostrare che non è sufficiente affermare l'incompatibilità intrinseca del cyberspazio con i principi del DIU, ma è necessario sviluppare quadri interpretativi e metodologie operative che permettano di integrare tali principi nel contesto digitale. Attraverso l'analisi di tecniche di contenimento, di targeting mirato e di stime del danno collaterale adattate al dominio cyber, si è voluto evidenziare come sia possibile – almeno in linea teorica e con adeguato livello di sofisticazione tecnica – progettare operazioni che rispettino gli obblighi di protezione dei civili. La proposta di un approccio di *Colla-*

teral Damage Estimation esteso al cyberspazio rappresenta un contributo in questa direzione, offrendo una lente sistemica e probabilistica per valutare e mitigare gli effetti indesiderati delle azioni offensive digitali.

In conclusione, la protezione dei civili deve rimanere al centro dell'applicazione del diritto internazionale, anche – e soprattutto – quando la tecnologia rende più labili i confini tra spazio di battaglia e vita quotidiana. La sfida contemporanea non è solo tecnica o strategica, ma profondamente giuridica e umanitaria: richiede che gli ordinamenti internazionali e gli interpreti del diritto siano in grado di tradurre i principi fondanti del DIU in regole operative applicabili al dominio cibernetico, preservando l'essenza della protezione umana in un mondo in cui le minacce ibride si manifestano con modalità sempre più sofisticate e pervasive.

DAL CODICE NASCOSTO AL CODICE MIGRANTE: EVOLUZIONE DELLA CRITTOGRAFIA NON CONVENZIONALE

Michele Empler[*]

1. *Prolegomeni teorici: crittografia, semiotica e controllo dell'informazione*

La storia della crittografia è, prima di tutto, la storia di un conflitto asimmetrico: da una parte, chi detiene il potere di sorvegliare; dall'altra, chi intende sottrarsi a tale sorveglianza. Questa dinamica, che attraversa trasversalmente la storia militare, diplomatica e criminale dell'umanità, ha conosciuto nell'era digitale una radicalizzazione senza precedenti. La diffusione capillare dei sistemi automatizzati di monitoraggio del linguaggio – fondati su tecniche di *Natural Language Processing* (NLP), analisi delle reti e classificazione semantica automatica – ha reso il testo scritto, nella sua forma convenzionale, il terreno più esposto e vulnerabile della comunicazione clandestina.

La premessa da cui muove il presente contributo è di natura paradossale. Ci si attenderebbe, in linea con la traiettoria evolutiva della crittografia tradizionale, che la risposta a una sorveglianza sempre più sofisticata consistesse in un ulteriore innalzamento della complessità algoritmica: codici più potenti, chiavi crittografiche più lunghe, protocolli più imperscrutabili. Eppure, l'evidenza empirica emersa dall'osservazione sistematica dei canali digitali attraverso cui operano le reti migratorie irregolari

[*] Dottorando di ricerca in "Società in mutamento: politiche, diritti e sicurezza" nell'Università degli Studi della Tuscia.

lungo le rotte dal Sahel verso l'Europa contraddice questa aspettativa in modo netto[1]. L'evoluzione del codice clandestino non ha seguito la traiettoria algoritmica, bensì una direzione radicalmente diversa e, per molti versi, controintuitiva: quella della semplicità visiva, dell'immediatezza iconografica e della pluralità semantica.

Il «codice nascosto», concepito tradizionalmente come un sistema di cifratura matematicamente sofisticato, ha progressivamente ceduto il passo a quello che proponiamo di denominare «codice migrante»: un sistema di comunicazione ibrido, multimodale e transculturale, fondato sull'integrazione strategica di *emoji*, *slang* regionali, idiomi misti e simboli iconografici. Questo sistema assolve una duplice funzione che nessun sistema crittografico convenzionale sarebbe in grado di svolgere simultaneamente: da un lato, elude i meccanismi di rilevamento automatico dei sistemi NLP, rendendosi semanticamente opaco agli algoritmi di *content moderation*; dall'altro, abbatte le barriere linguistiche e di alfabetizzazione che frammentano le popolazioni del Sahel, garantendo una comunicazione immediata e universalmente accessibile a soggetti linguisticamente eterogenei e con scarse risorse digitali[2].

L'analisi di questo fenomeno impone un approccio necessariamente interdisciplinare, capace di integrare la teoria crittografica con la semiotica peirciana, la sociolinguistica e le scienze dell'*intelligence*. Sul piano crittografico, ci interessa ricostruire la genealogia del passaggio dal «codice nascosto» al «codice migrante» e collocarlo nel solco della più lunga storia dei sistemi di comunicazione clandestina. Sul piano semiotico, ci proponiamo di descrivere i meccanismi attraverso cui l'*emoji* – nato come strumento paraverbale di comunicazione informale – si trasforma in un vero e proprio sistema semiologico autonomo con una propria grammatica implicita e convenzioni d'uso che variano significativamente tra culture diverse. Sul piano sociolinguistico, intendiamo dar conto della specificità del contesto saheliano, in cui la frammentazione linguistica estrema e i bassi tassi di alfabetizzazione rendono il codice visivo non già un'opzione comunicativa, ma la soluzione più efficiente e inclusiva

[1] Le evidenze empiriche qui richiamate derivano dalla ricerca condotta in M. EMPLER, C. CAPASSO, *Metodi e tecniche di monitoraggio web*, cit., §§ 4-5, basata sull'analisi di un campione rappresentativo di cento gruppi per ciascuna delle principali piattaforme *social* (Facebook, Instagram, TikTok, YouTube, Telegram), mediante tecniche di *web crawling* e analisi OSINT.

[2] Sul concetto di inclusione comunicativa nei contesti digitali multilingui, cfr. anche C. MUNGAI, *«We are just focused on being where readers are»: Pan-African weekly The Continent publishes directly on WhatsApp and Signal*, in niemanlab.org, 2021.

disponibile. Sul piano dell'*intelligence,* infine, ci preme valutare le implicazioni operative di questo fenomeno per i sistemi di monitoraggio digitale e proporre alcune indicazioni metodologiche per un approccio analitico adeguato alla sfida.

Il percorso argomentativo si articola in cinque paragrafi. Nel paragrafo 2 si ricostruisce in forma sintetica ma rigorosa la genealogia della crittografia convenzionale, identificandone il limite strutturale fondamentale. Nel paragrafo 3 si descrive il paradosso della trasparenza che caratterizza l'evoluzione attuale dei codici clandestini. Nel paragrafo 4 si presenta la «Teoria del Codice Migrante» nei suoi elementi costitutivi: gli assiomi fondamentali, la formula esplicativa, la funzione translinguistica e i meccanismi adattativi, avvalendosi delle evidenze empiriche raccolte nell'ambito di una più ampia ricerca sulla disinformazione migratoria digitale[3]. Nel paragrafo 5 si discutono le implicazioni per l'*intelligence* e il monitoraggio digitale, proponendo una ridefinizione funzionale del concetto stesso di crittografia.

2. *Genealogia della crittografia convenzionale: dal cifrario di Cesare alla crittografia a chiave pubblica*

Per comprendere la portata della trasformazione qui descritta, è necessario ricostruire la traiettoria evolutiva della crittografia convenzionale, identificandone non soltanto le conquiste tecniche, ma – e soprattutto – il limite strutturale che ne ha paradossalmente determinato il superamento.

La storia del segreto codificato si articola in tre grandi epoche,ciascuna contraddistinta da un salto qualitativo nel rapporto tra complessità del meccanismo di cifratura e capacità degli avversari di decrittarne il contenuto.

La *prima epoca* è quella della crittografia per sostituzione e trasposizione, il cui archetipo è il *cifrario di Cesare*,attestato già nel I secolo a.C. e documentato da Svetonio nelle sue biografie degli imperatori romani: ogni lettera del messaggio originale viene sostituita con la lettera posta a distanza fissa nell'alfabeto, abitualmente tre posizioni in avanti[4]. Pur

[3] M. Empler, C. Capasso, *Metodi e tecniche di monitoraggio web*, cit. Il presente contributo si configura come sviluppo autonomo degli spunti teorici ivi elaborati, con particolare riferimento al § 5.1 (*Teoria del codice migrante: sistemi semiotici ibridi nella disinformazione digitale*).

[4] C. Svetonio Tranquillo, *De vita Caesarum*, I-II sec.d.C., lib. I (*Divus Iulius*),§ 56.

nella sua elementarità, il cifrario di Cesare incarna già il principio fondamentale che dominerà la crittografia per due millenni: l'occultamento del significato attraverso la trasformazione sistematica del segno linguistico secondo una regola nota soltanto ai comunicanti. Il *cifrario di Vigenère*, elaborato nel XVI secolo, rafforza questa logica attraverso l'introduzione di un sistema polialfabetico che utilizza una parola chiave per variare lo scostamento lettera per lettera, rendendo inefficace la semplice analisi delle frequenze che poteva violare il cifrario cesariano[5].

La *seconda epoca* coincide con lo sviluppo della crittografia meccanica ed elettromeccanica nel corso del XX secolo. La macchina *Enigma,* adottata dalla *Wehrmacht* tedesca durante la Seconda guerra mondiale, eleva il principio polialfabetico a una complessità ingegneristica di ordine superiore, generando miliardi di possibili configurazioni di cifratura attraverso un sistema di rotori intercambiabili e un pannello di collegamento (*Steckerbrett*)[6]. La sua decrittazione da parte degli analisti di Bletchley Park – tra cui Alan Turing, con la macchina *Bombe* – rappresenta uno dei momenti fondativi della moderna informatica e della crittoanalisi scientifica, ma documenta anche un principio destinato a rimanere valido: sistemi crittografici apparentemente inviolabili possono essere sconfitti dalla combinazione di analisi statistica del traffico, potenza computazionale e intelligenza umana.

La *terza epoca* è quella della crittografia computazionale a chiave pubblica, la cui nascita coincide con la pubblicazione del saggio fondativo di Claude Shannon, *A Mathematical Theory of Communication*, nel 1948[7]. Shannon formalizza matematicamente il concetto di informazione e introduce la nozione di *entropia informativa* come misura dell'imprevedibilità di un messaggio, ponendo le basi per lo sviluppo di sistemi crittografici fondati su dimostrazioni probabilistiche di sicurezza. L'elaborazione teorica shannoniana genera, nei decenni successivi, un programma di ricerca straordinariamente fecondo: Whitfield Diffie e Martin Hellman pubblicano nel 1976 «New Directions in Cryptography», introducendo

Per la ricostruzione del cifrario cesariano nella storia della crittografia, cfr. D. KAHN, *The Codebreakers. The Story of Secret Writing*, Scribner, New York, 1996, pp. 75-83.

[5] B. DE VIGENÈRE,*Traicté des Chiffres, ou Secrètes Manières d'Escrire*,Abel l'Angelier,Paris,1586. Cfr. D. KAHN, *The Codebreakers*, cit., pp. 144-154.

[6] Per la storia tecnica e operativa della macchina *Enigma* e della sua decrittazione, cfr. F.H. HINSLEY, A. STRIPP, a cura di, *Codebreakers: The Inside Story of Bletchley Park*, Oxford University Press, Oxford, 1993.

[7] C. SHANNON, *A Mathematical Theory of Communication*, in *Bell System Technical Journal*, v. 27, n. 3, 1948, pp. 379-423; v. 27, n. 4, 1948, pp. 623-656.

il concetto rivoluzionario di crittografia a chiave pubblica – un sistema in cui la chiave di cifratura è pubblica e accessibile a chiunque, mentre la chiave di decifratura rimane privata e segreta[8]. Questo principio viene implementato nel 1978 da Ronald Rivest, Adi Shamir e Leonard Adleman nel protocollo RSA, che costituisce ancora oggi la base della sicurezza delle comunicazioni digitali in rete[9]. La sua incarnazione più nota nell'ambito della comunicazione individuale è il sistema *Pretty Good Privacy* (PGP), sviluppato da Phil Zimmermann nel 1991 e distribuito gratuitamente come strumento per la protezione della *privacy* digitale[10].

Questa traiettoria evolutiva segue una logica coerente che potremmo denominare *sicurezza per oscurità algoritmica*: il messaggio viene protetto rendendo il processo di trasformazione matematicamente complesso al punto da risultare computazionalmente intrattabile per chiunque non disponga della chiave privata. L'elevazione progressiva della complessità algoritmica – da poche posizioni nell'alfabeto a chiavi RSA di 4.096 bit – rappresenta la risposta sistematica alla crescente capacità computazionale degli avversari.

Eppure, questo paradigma, nella sua perfezione teorica, nasconde un limite strutturale divenuto sempre più rilevante nell'era della sorveglianza digitale di massa: la crittografia convenzionale protegge il *contenuto* del messaggio, ma non la sua *esistenza*. Un messaggio cifrato con PGP è matematicamente inviolabile; ma la sola presenza di una comunicazione cifrata in una rete di soggetti sorvegliati costituisce, per qualunque sistema di *traffic analysis*, un segnale di allarme inequivocabile[11]. L'alfabeto di *Enigma* restava segreto, ma il fatto che i sottomarini tedeschi trasmettessero messaggi radio era visibile a chiunque disponesse di un ricevitore. Allo stesso modo, un messaggio cifrato con RSA rivela a chi monitora il traffico di rete che qualcuno ha qualcosa da nascondere. La crittografia convenzionale risolve il problema del «*cosa*»,lasciando irrisolto il proble-

[8] W. Diffie, M. Hellman, *New Directions in Cryptography*, in *IEEE Transactions on Information Theory*, v. 22, n. 6, 1976, pp. 644-654.

[9] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, in *Communications of the ACM*, v. 21, n. 2, 1978, pp. 120-126.

[10] S. Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly Media, Sebastopol, 1994. Sul contesto politico e culturale in cui PGP fu sviluppato e distribuito, cfr. anche B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, Wiley, New York, 2000, pp. 69-82.

[11] Sul concetto di *traffic analysis* e sui suoi limiti nel neutralizzare la crittografia convenzionale, cfr. B. Schneier, *Secrets and Lies*, cit., pp. 91-105; R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3a ed., Wiley, New York, 2020, pp. 201-218.

ma del «*che*». È questa la contraddizione strutturale che il codice migrante – attraverso la strategia opposta della semplicità visiva – si propone, talvolta inconsapevolmente ma sempre efficacemente, di superare.

3. Il paradosso della trasparenza: quando l'ovvio diventa invisibile

La presa di coscienza del limite strutturale della crittografia convenzionale – il suo fallimento nel nascondere non il contenuto bensì l'*esistenza* del messaggio – ha orientato la ricerca di strategie comunicative alternative lungo due direttrici distinte. La prima, che rientra nella categoria della *steganografia*, si propone di occultare l'esistenza stessa della comunicazione celando il messaggio all'interno di un vettore apparentemente innocuo: un'immagine digitale, un file audio, un testo di superficie privo di apparente contenuto sensibile[12]. La seconda – quella che qui ci interessa direttamente – non occulta né il contenuto né l'esistenza del messaggio in senso stretto, ma ne rende la decodifica semanticamente opaca ai sistemi automatizzati di analisi, sfruttando il dominio visivo-iconico come spazio comunicativo intrinsecamente extra-linguistico rispetto agli strumenti NLP.

I sistemi automatizzati di moderazione dei contenuti e le piattaforme di *Natural Language Processing* utilizzate dalle grandi piattaforme digitali si sono sviluppati seguendo una logica progressivamente più sofisticata. Nei loro stadi iniziali, essi si limitavano all'identificazione di parole chiave (*keyword filtering*): elenchi di termini proibiti la cui sola presenza nel testo innescava l'intervento moderativo[13]. Questa tecnica elementare si rivelò rapidamente inadeguata, poiché facilmente aggirata attraverso sostituzioni fonetiche, ortografiche o sinonimiche. La risposta fu l'introduzione di tecniche di analisi semantica contestuale, capaci di valutare il significato di un termine in relazione agli altri termini del cotesto. L'ulteriore passo evolutivo è rappresentato dai grandi modelli di linguaggio (*Large Language Models*, LLM) basati sull'architettura *transformer* – a

[12] Per una trattazione sistematica della distinzione tra crittografia e steganografia e delle loro implicazioni operative, cfr. N. JOHNSON, S. JAJODIA, *Exploring Steganography: Seeing the Unseen*, in *IEEE Computer*, v. 31, n. 2, 1998, pp. 26-34.

[13] Per un'analisi delle evoluzioni storiche e dei limiti strutturali dei sistemi di *content moderation*, cfr. T. GILLESPIE, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, New Haven, 2018.

partire da BERT (*Bidirectional Encoder Representations from Transformers*), introdotto da Devlin e colleghi nel 2018 – capaci di rilevare relazioni semantiche di ordine superiore e di classificare i contenuti con una precisione che supera di molto quella degli approcci precedenti[14].

Di fronte a questa progressiva sofisticazione dei sistemi di sorveglianza testuale, si è prodotta una risposta adattiva da parte degli attori che intendono eludere il controllo. Questa risposta non è consistita, come ci si potrebbe attendere, in un ulteriore innalzamento della complessità crittografica. Al contrario, essa ha preso la forma di una radicale semplificazione: l'abbandono del testo scritto – vulnerabile per definizione ai sistemi di analisi linguistica – in favore di sistemi comunicativi di natura visivo-iconica che, pur essendo «ovvi» nella loro struttura superficiale, risultano semanticamente opachi alle analisi automatizzate proprio per la loro extra-linguisticità.

Questo è ciò che denominiamo il *paradosso della trasparenza*: ciò che appare evidente – una sequenza di *emoji*, un'icona, una bandierina – è, dal punto di vista dei sistemi automatizzati di rilevamento, radicalmente invisibile, perché non appartiene al dominio semantico che tali sistemi sono stati progettati per analizzare. I modelli NLP sono stati addestrati prevalentemente su corpus testuali scritti in lingue naturali; la loro capacità di interpretare sequenze pittografiche – e soprattutto di cogliere le relazioni contestuali che determinano il significato specifico di una data sequenza *emoji* all'interno di una comunità di pratica – è ancora largamente insufficiente[15]. L'ovvio diventa così il perfetto schermo per l'occulto; la trivialità iconica si trasforma in uno strumento di elusione altrettanto efficace – e assai più accessibile – della sofisticazione algoritmica.

Un esempio tratto dalla ricerca empirica sui canali digitali delle reti migratorie illustra il meccanismo con immediata evidenza. Invece di scrivere esplicitamente «viaggio in barca dalla Tunisia all'Italia» – una frase che qualunque sistema di *keyword filtering* intercetterebbe istantaneamente – un *post* su Facebook o Instagram contiene una sequenza di icone 🇹🇳🚤🇮🇹. Tale sequenza è tecnicamente accessibile a

[14] J. Devlin, M. Chang, K. Lee, K. Toutanova, *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*, in *arXiv preprint*, 2018

[15] Cfr. F. Kralj Novak, T. Smailović, B. Sluban, I. Mozetič, *Sentiment of Emojis*, in *PLOS ONE*, v. 10, n. 12, 2015, e0144296. La ricerca documenta come il significato attribuito alle *emoji* vari significativamente in funzione del contesto d'uso e della piattaforma, rendendo estremamente difficile la costruzione di modelli automatici di classificazione semantica affidabili.

chiunque possa vederla sullo schermo; eppure nessun algoritmo di *content moderation* attualmente in uso la classificherebbe come contenuto sospetto, perché la relazione tra questi simboli e il fenomeno della migrazione clandestina non è una relazione linguistica – non è codificata in nessun dizionario semantico, in nessun corpus di addestramento – bensì una relazione contestuale-pragmatica che esiste soltanto all'interno della comunità di pratica che ne condivide le convenzioni[16]. Il codice migrante si colloca dunque in uno spazio semiologico ibrido che non appartiene né alla crittografia convenzionale – la quale nasconde il contenuto attraverso la complessità algoritmica – né alla steganografia – la quale nasconde l'esistenza del messaggio occultandolo in un vettore. Esso realizza qualcosa di diverso e, per certi versi, più radicale: rende il messaggio *visibile* ma *illeggibile* per i sistemi di sorveglianza, fondando la sua efficacia non sulla segretezza del codice ma sull'inadeguatezza degli strumenti analitici disponibili. È, in senso proprio, una crittografia dell'ovvio.

4. Il codice migrante come sistema crittografico non convenzionale

Il fenomeno che qui denominiamo «codice migrante» costituisce un'istanza paradigmatica della logica di trasparenza paradossale descritta nel paragrafo precedente. Nell'ambito delle ricerche condotte sui canali digitali che operano lungo le rotte migratorie dal Sahel verso l'Europa – attraverso tecniche di *web crawling*, analisi OSINT (*Open Source Intelligence*) e mappatura delle reti comunicative su Facebook, Telegram, Instagram e TikTok – è emerso con chiarezza come la comunicazione tra migranti, trafficanti e intermediari non ricorra principalmente agli strumenti di crittografia informatica convenzionale[17]. Questi ultimi sono, del resto, troppo complessi da maneggiare per popolazioni con bassa alfabetizzazione digitale e accesso limitato a dispositivi tecnologici avanzati. Al loro posto, il sistema comunicativo osservato è fondato sull'integrazione strategica di *emoji*, *slang* regionali, idiomi misti e simboli iconografici:

[16] Cfr. M. EMPLER, C. CAPASSO, *Metodi e tecniche di monitoraggio web*, cit., § 5, e in particolare la Tabella 5.1 (*Il nuovo sistema di keyword utilizzato nei diversi social*), in cui vengono documentate le sequenze *emoji* ricorrenti nei canali analizzati e la loro traduzione contestuale.

[17] M. EMPLER, C. CAPASSO, *Metodi e tecniche di monitoraggio web*, cit., §§ 4 e 4.2, in cui viene descritto il metodo di *web crawling* fondato su un dizionario dinamico di *keyword* aggiornate iterativamente dall'algoritmo di scansione.

un sistema che, come dimostreremo *infra,* assolve simultaneamente alle funzioni di elusione dei sistemi di controllo e di inclusione comunicativa transculturale.

La denominazione «codice migrante» non rimanda esclusivamente alla natura migratoria dei soggetti che lo utilizzano. Essa evoca, più profondamente, il concetto linguistico di «codice in transizione»: un sistema comunicativo che non appartiene a nessuna delle tradizioni linguistiche convenzionali, ma si muove tra esse, traendo da ciascuna elementi selezionati e ricombinandoli in una sintassi inedita. Esso è, per usare la terminologia saussuriana, un sistema di segni in cui il rapporto tra *signifiant* e *signifié* è parzialmente rinegoziato rispetto alle convenzioni linguistiche d'origine, e in cui la dimensione iconica del segno – nel senso peirciano del termine – svolge un ruolo che la linguistica strutturale tradizionale non aveva contemplato[18].

4.1. La teoria del codice migrante: assiomi e formula esplicativa

La formalizzazione teorica di questo sistema comunicativo è stata elaborata nell'ambito di ricerche precedenti, che proponiamo qui di sviluppare e sistematizzare ulteriormente[19]. La «Teoria del Codice Migrante» si configura come un modello interpretativo di natura linguistico-comunicativa, volto a descrivere l'emergere di un sistema semantico transnazionale e multimodale all'interno delle comunità digitali coinvolte nei fenomeni migratori irregolari. Il sistema si fonda sull'integrazione strategica di elementi testuali, visivi ed emotivi – tra cui *slang* regionali, idiomi misti, *emoji* e simboli iconografici – con il triplice obiettivo di trasmettere contenuti complessi, eludere i meccanismi di rilevamento automatico e generare un vocabolario condiviso tra soggetti appartenenti a contesti culturali e linguistici eterogenei. Sebbene tale teoria si trovi ancora in una fase esplicitamente esplorativa, essa si configura come un primo tentativo sistematico di fornire una chiave di lettura empirica ai codici comunicativi ricorrenti nei contesti digitali osservati.

[18] Per il concetto saussuriano di *signifiant* e *signifié* e per la tricotomia peirciana icona/indice/simbolo, cfr. rispettivamente F. De Saussure, *Cours de linguistique générale* (1916), Payot, Paris, 1972; C.S. Peirce, *Collected Papers*, Harvard University Press, Cambridge, 1931-1958, v. II, §§ 247-249.

[19] La formulazione originale della Teoria del Codice Migrante è in M. Empler, C. Capasso, *Metodi e tecniche di monitoraggio web*, cit., § 5.1.

Gli assiomi fondamentali della teoria si articolano come segue.

Il *primo assioma*, che denominiamo della *sincretizzazione semiotica*, afferma che le lingue scritte tradizionali vengono integrate con elementi visivi (*emoji*, bandiere, simboli) e dialettali per formare una sintassi ibrida, capace di trasmettere significati complessi anche in assenza di un codice linguistico comune. Non si tratta, in questo caso, di una semplice aggiunta decorativa di elementi iconici al testo scritto, ma di una vera e propria sostituzione funzionale: l'*emoji* non accompagna il messaggio, lo *è*. Il simbolo della barca non illustra ciò che il testo dice: *è* la comunicazione stessa, nella sua interezza semantica.

Il *secondo assioma*, della *opacità strategica*, descrive il meccanismo attraverso cui l'uso di codici visivi e metaforici costituisce uno strumento – spesso inconsapevole nella sua formalizzazione teorica, ma sistematico negli effetti – per eludere i sistemi di rilevamento automatico, rendendo al contempo il messaggio immediatamente decifrabile per i destinatari condivisi. L'opacità non è assoluta: il messaggio non è crittograficamente inaccessibile, né è celato in un vettore steganografico. È piuttosto *selettiva*: opaca per i sistemi di sorveglianza, trasparente per i membri della rete che condividono il repertorio simbolico.

Il *terzo assioma,* della *ridondanza multilingue,* afferma che la ripetizione intenzionale dello stesso concetto in più lingue – arabo, francese, inglese, *emoji* – non costituisce una semplice ridondanza comunicativa, bensì un'espansione deliberata dell'accessibilità del messaggio, volta a coinvolgere pubblici frammentati geograficamente e culturalmente. La ridondanza è, in questo senso, una strategia di inclusione semiotica: il medesimo contenuto raggiunge contemporaneamente il giovane hausa del Niger, il tuareg maliano e il nordafricano arabofono, ciascuno attraverso il registro linguistico che gli è più familiare.

Il *quarto assioma,* della *narrazione emotiva translinguistica,* riconosce che le sequenze *emoji* e le micronarrazioni simboliche svolgono una funzione retorica ed emotiva capace di evocare aspirazioni, pericoli e successi in forma sintetica ma potente, fungendo da catalizzatori empatici che superano le barriere culturali e linguistiche. Una sequenza come 🚤💨🇮🇹❤️ non trasmette semplicemente un'informazione in senso tecnico: genera un'emozione, un'aspettativa, un desiderio. È la retorica dell'immagine applicata alla comunicazione clandestina.

Il *quinto assioma,* del *vocabolario mimetico,* descrive il processo attraverso cui i termini chiave del lessico migratorio – *boza*, *ghorba*,*haraga* e altri lessici regionali – vengono mimetizzati tra simboli e *hashtag,* creando un linguaggio che simula spontaneità ma obbedisce a schemi ripetuti e

riconoscibili all'interno delle reti sociali. La mimetizzazione non è casuale: è il risultato di un'evoluzione adattativa che seleziona le soluzioni comunicative capaci di resistere ai meccanismi di moderazione.

La formalizzazione semiotico-linguistica di questi assiomi produce la seguente formula esplicativa:

$CM = (E + Lm + Sg) \times Cc$

dove *CM* denota il Codice Migrante nella sua configurazione effettiva; *E* rappresenta l'insieme degli *Emoji* e simboli iconici; *Lm* indica i Linguaggi misti, ovvero le combinazioni di arabo, francese, inglese e dialetti locali; *Sg* denota lo *Slang* gergale o codificato; *Cc* rappresenta infine il Contesto comunicativo, inteso come variabile moltiplicativa che comprende la piattaforma utilizzata, il tono del messaggio e il profilo dei destinatari[20].

Il carattere moltiplicativo – e non meramente additivo – del contesto comunicativo è teoricamente significativo: esso indica che il valore semantico del codice non è la semplice somma dei suoi elementi costitutivi, ma è determinato in modo decisivo dalle condizioni contestuali di enunciazione e ricezione. Un medesimo *set* di *emoji* assume significati radicalmente diversi a seconda della piattaforma, del gruppo di appartenenza e del momento storico in cui viene prodotto. La stessa bandiera 🇮🇹, combinata con 🚤, significa «destinazione» in un canale migratorio saheliano e «vacanza» nel profilo di un turista. Il contesto è, pertanto, la chiave di decodifica del codice – e la chiave non è un algoritmo, ma un'appartenenza sociale.

*4.2. La funzione translinguistica dell'*emoji *nel contesto saheliano*

Per comprendere appieno la portata del codice migrante come sistema di comunicazione, è necessario considerare il contesto sociolinguistico in cui esso si sviluppa: quello della regione saheliana, caratterizzata da una frammentazione linguistica e da una diversità dialettale che non trovano paralleli in nessun'altra area del mondo di dimensioni comparabili.

Il Sahel – la fascia sub-desertica che si estende dall'Atlantico al Mar Rosso, comprendendo Mauritania, Mali, Burkina Faso, Niger, Ciad, Sudan e le aree limitrofe – ospita, secondo le stime disponibili, oltre ottocento lingue e dialetti, raggruppabili in quattro grandi famiglie linguistiche (afroasiatica, nilo-sahariana, niger-congo e khoisan), con ampie sovrap-

[20] *Ibidem*.

posizioni e transizioni graduali tra varianti contigue[21]. In questo contesto, le lingue coloniali – il francese nell'Africa occidentale e il Maghreb, l'arabo *standard* nelle aree del Maghreb e del Sahel orientale – svolgono funzioni di *lingua franca* nei contesti formali e istituzionali. Ma tale funzione è limitata: la competenza nelle lingue coloniali varia enormemente in funzione del livello di istruzione, del genere e della distanza dai centri urbani, e non garantisce una comprensione uniforme nelle comunicazioni informali tra individui provenienti da aree geografiche diverse.

A questa frammentazione linguistica si sovrappone un quadro socioeconomico che rende di fatto inaccessibili i sistemi di crittografia convenzionale. Secondo i dati UNESCO, il tasso di alfabetizzazione in alcune aree del Sahel non supera il 30-40% della popolazione adulta, con significative differenze di genere a svantaggio delle donne[22]. In tale contesto, strumenti come PGP – che richiedono la comprensione di concetti crittografici avanzati, l'uso di *software* specializzato e un livello di competenza digitale non elementare – sono praticamente inutilizzabili dalla maggioranza della popolazione potenzialmente coinvolta nei fenomeni migratori.

L'*emoji* rappresenta, in questo quadro, non soltanto uno strumento di elusione dei sistemi di controllo, ma anche – e forse soprattutto – un meccanismo di *inclusione comunicativa*. Un messaggio che combina una bandiera tunisina, un'icona di barca, un'icona di onda e una bandiera italiana è immediatamente comprensibile a un giovane hausa del Niger, a un tuareg maliano, a un berbero algerino e a un *wolof* senegalese, pur nella loro radicale diversità linguistica. Il segno iconico – nella sua natura di *icona* nel senso peirciano del termine, ovvero di segno che mantiene una relazione di somiglianza con il proprio referente – supera la barriera del codice linguistico e si rivolge direttamente alla competenza percettiva universale[23]. Chiunque riconosca le bandiere degli Stati e le forme degli oggetti rappresentati può decodificare il messaggio elementare, a pre-

[21] F. MC LAUGHLIN, *The Linguistic Ecology of the Sahel*, in S. DECALO (a cura di), *The Oxford Handbook of the African Sahel*, Oxford University Press, Oxford, 2021, pp. 780-800.

[22] Dati UNESCO sull'alfabetizzazione nell'Africa subsahariana e nel Sahel, aggiornati al 2022, consultabili in uis.unesco.org.

[23] Cfr. C.S. PEIRCE, *Collected Papers*, cit., v. II, § 247: «An Icon is a sign which refers to the Object that it denotes merely by virtue of characters of its own, and which it possesses, just the same, whether any such Object actually exists or not». Per l'applicazione della semiotica peirciana all'analisi dei sistemi comunicativi digitali, cfr. U. ECO, *A Theory of Semiotics*, Indiana University Press, Bloomington, 1976, pp. 191-217.

scindere dalla lingua madre, dal livello di alfabetizzazione e dall'accesso a strumenti tecnologici avanzati.

Questa funzione translinguistica ha implicazioni di primo piano per la comprensione dei flussi informativi nelle reti migratorie. I trafficanti e gli intermediari che operano su questi canali hanno compreso – anche senza una formalizzazione teorica esplicita – che l'*emoji* costituisce il vettore comunicativo più efficiente per raggiungere simultaneamente soggetti appartenenti a comunità linguisticamente eterogenee. La stessa sequenza iconica può essere distribuita indiscriminatamente su canali frequentati da utenti di decine di nazionalità diverse, con la certezza che il contenuto essenziale del messaggio verrà percepito e compreso da tutti. Si realizza così una «democratizzazione della crittografia»: se la crittografia convenzionale è storicamente appannaggio di attori con risorse tecniche e culturali elevate, il codice *emoji* è accessibile a chiunque possieda uno *smartphone* e la capacità di riconoscere simboli visuali elementari. Il costo di ingresso nel sistema è, per definizione, pressoché nullo. La barriera tecnologica si dissolve; rimane soltanto quella semantica – che, tuttavia, è facilmente superabile proprio grazie alla natura iconica dei segni impiegati.

4.3. Meccanismi adattativi e bypass dei sistemi di controllo automatizzato

L'efficacia del codice migrante come strumento di elusione dei sistemi di moderazione automatica dipende da un insieme di fattori strutturali che meritano di essere analizzati in forma sistematica.

Il *primo fattore* è la già menzionata *extra*-linguisticità dell'*emoji* rispetto ai sistemi di NLP. I modelli di linguaggio naturale – inclusi i più sofisticati LLM basati su architettura *transformer* attualmente disponibili – sono stati sviluppati e addestrati prevalentemente su corpus testuali scritti, e presentano capacità analitiche significativamente inferiori nel dominio dei segni pittografici rispetto a quello del testo alfanumerico. La ricerca sull'interpretazione automatica delle *emoji* ha documentato discrepanze sistematiche tra il significato inteso dal mittente e quello attribuito dai modelli automatici, anche quando questi ultimi vengono addestrati specificamente sul dominio pittografico[24]. Nel contesto delle

[24] H. Miller, D. Thebault-Spieker, S. Chang, I. Johnson, L. Terveen, B. Hecht, *«Blissfully happy» or «ready to fight»: Varying interpretations of Emoji*, in *Proceedings of*

comunicazioni clandestine, questa lacuna analitica costituisce, di fatto, una zona franca strutturale.

Il *secondo fattore* è il carattere intrinsecamente polisemico dell'*emoji*, che rende impossibile la costruzione di dizionari semantici univoci. La medesima *emoji* – poniamo 🔥 (fiamma) – può significare, a seconda del contesto, «è bellissimo/a», «questo contenuto è virale», «pericolo imminente», «partenza urgente» o «questo canale è sorvegliato». La polisemia non è una casualità: è una proprietà strutturale del segno iconico nel suo uso digitale, determinata dalle convenzioni pragmatiche che variano tra comunità, piattaforme e momenti storici[25]. L'assenza di un significato fisso e universale rende impossibile costruire regole di rilevamento basate sull'equivalenza semplice tra simbolo e significato.

Il *terzo fattore* è la ridondanza multilingue che disperde il segnale sospetto su più canali semiotici simultaneamente. Un messaggio che combina arabo dialettale, francese informale, *emoji* e termini in lingua *hausa* non appartiene a nessuna delle categorie linguistiche che i sistemi di moderazione sono progettati per analizzare; esso si colloca in un interstizio semantico che sfugge alle categorie classificatorie precostituite, producendo un segnale di rumore che i classificatori automatici tendono a interpretare come contenuto innocuo o indecifrabile.

Il *quarto fattore* è la velocità adattativa del sistema. A differenza della crittografia convenzionale – i cui algoritmi sono relativamente stabili nel tempo e possono essere analizzati a fondo una volta identificati – il codice *emoji* evolve continuamente, incorporando nuovi simboli, modificando le convenzioni d'uso preesistenti e sviluppando varianti regionali in risposta ai tentativi di moderazione. Quando una piattaforma introduce filtri che identificano come sospette determinate sequenze *emoji*, le reti si adattano rapidamente, sostituendo le sequenze bloccate con combinazioni equivalenti. Questa plasticità adattativa è intrinseca alla natura semiotica del sistema: poiché il significato dell'*emoji* è determinato contestualmente, la sostituzione di un simbolo con un equivalente funzionale è un'operazione semanticamente elementare ma crittograficamente efficace[26].

ICWSM, 2016. Lo studio documenta come la stessa *emoji* possa essere interpretata in modo radicalmente diverso da mittente e destinatario.

[25] Cfr. F. KRALJ NOVAK ET AL., *Sentiment of Emojis*, cit. La polisemia è documentata come proprietà sistematica, non come eccezione, nell'uso delle *emoji* nelle comunicazioni digitali ad ampia scala.

[26] Cfr. D. SHAH, S. JAIN, T. BHATT, C. DE ARMAS, A. KARBASI, *Bridging Nodes and*

Il *quinto fattore* è la mimetizzazione nel flusso ordinario della comunicazione digitale. I canali che impiegano il codice migrante non si distinguono, nella loro morfologia esterna, da qualunque altro gruppo Facebook o canale Telegram frequentato da una popolazione giovanile; la presenza massiccia di *emoji* è prassi normale nella comunicazione digitale contemporanea e non costituisce, in sé, un segnale di anomalia. Il contenuto sospetto è celato non in una struttura crittograficamente opaca, ma nel significato che una comunità di pratica attribuisce a segni visivamente trasparenti. L'osservatore esterno vede esattamente ciò che vede sempre: giovani che comunicano con *emoticon*. Non vede il codice perché non conosce la chiave – e la chiave non è un algoritmo, ma un'appartenenza sociale, un sapere condiviso che non si impara su un manuale ma si acquisisce attraverso l'immersione nella rete.

5. *Implicazioni per l'intelligence e il monitoraggio digitale*

Le considerazioni sviluppate nei paragrafi precedenti hanno conseguenze dirette e rilevanti per i sistemi di monitoraggio dell'intelligence, sia nella dimensione della sicurezza interna – contrasto al traffico di esseri umani, alla disinformazione migratoria e alle reti criminali che operano lungo le rotte saheliane – sia in quella più ampia della sicurezza ibrida e della *cybersecurity*[27]. La principale implicazione è che i paradigmi analitici tradizionali – basati sull'identificazione di parole chiave testuali, sulla mappatura delle reti comunicative attraverso l'analisi del linguaggio scritto e sulla classificazione dei contenuti sospetti attraverso dizionari semantici precostituti – sono strutturalmente inadeguati di fronte a sistemi di comunicazione che operano nel dominio visivo-iconico.

Ciò non implica, naturalmente, che il monitoraggio dei codici migranti sia impossibile: implica,piuttosto, che esso richiede un approccio metodologico radicalmente diverso, strutturato su tre livelli complementari.

Il *primo livello* è quello dell'*etnografia digitale*. L'identificazione dei *pattern* di comunicazione *emoji* nelle reti migratorie non può essere af-

Narrative Flows: Identifying Intervention Targets for Disinformation on Telegram, in *arXiv preprint*,, 2024.

[27] Sul tema delle minacce ibride alla sicurezza nazionale e del ruolo della disinformazione digitale nel loro ambito, cfr. S. Sassi, A. Sterpa, a cura di, *Minacce ibride alla sicurezza nazionale. Disinformazione e migrazioni*, Editoriale Scientifica, Napoli, 2025.

fidata ad algoritmi di classificazione testuale: richiede un'analisi di tipo etnografico che permetta di ricostruire, attraverso l'osservazione prolungata delle comunità di pratica, il dizionario simbolico condiviso dai loro membri[28]. Tale dizionario non può essere costruito *a priori*, ma deve essere inferito *a posteriori* dall'analisi delle sequenze ricorrenti e delle associazioni contestuali – un lavoro che richiede competenze linguistiche e culturali specifiche, nonché una familiarità con i contesti sociali in cui il codice si sviluppa. Gli analisti dell'*intelligence* devono, in altri termini, «entrare» nelle comunità per comprendere le convenzioni simboliche che esse condividono.

Il *secondo livello* è quello dello sviluppo di strumenti tecnologici specificamente progettati per l'analisi multimodale. I sistemi di *computer vision* e di analisi delle sequenze pittografiche devono essere integrati con modelli di intelligenza artificiale addestrati su corpus di comunicazioni clandestine reali – non su corpus generici di testo scritto. Lo sviluppo di tali strumenti è attualmente in corso in diversi laboratori di ricerca internazionali, ma la sfida principale rimane quella dell'aggiornamento continuo: la velocità adattativa del codice migrante tende, almeno nel breve periodo, a precedere quella degli strumenti di rilevamento. La risposta a questa sfida non può essere soltanto tecnologica: deve integrare la componente etnografica descritta al primo livello con la capacità di aggiornare i modelli di classificazione in tempo reale.

Il *terzo livello* è quello della ridefinizione concettuale. L'analisi del codice migrante suggerisce la necessità di ripensare il concetto stesso di «crittografia» in senso funzionale piuttosto che algoritmico. Se per crittografia intendiamo non soltanto la trasformazione matematica di un testo in una sequenza di simboli computazionalmente inaccessibili, ma più in generale qualunque sistema di comunicazione che miri a trasmettere un contenuto a un destinatario selezionato rendendolo al contempo inaccessibile a soggetti terzi indesiderati, allora il codice *emoji* risponde pienamente a questa definizione funzionale, pur prescindendo completamente dalla dimensione algoritmica che caratterizza la crittografia convenzionale[29]. Questa ridefinizione funzionale non è meramente teorica: essa impone di ripensare le strategie di contrasto alla comunicazione clandestina

[28] Cfr. C. HINE, *Virtual Ethnography*, SAGE Publications, London, 2000. Il metodo dell'etnografia digitale è particolarmente adatto all'analisi di comunità di pratica online la cui coesione è determinata da convenzioni simboliche condivise piuttosto che da caratteristiche demografiche o geografiche.

[29] Sul concetto funzionale di crittografia e sulla sua applicazione a sistemi non al-

includendo, accanto alle tradizionali tecniche crittografiche e alle analisi linguistiche, strumenti specificamente progettati per l'analisi dei sistemi semiotici visivi e multimodali.

Il codice migrante si colloca, infine, in uno spazio ibrido che non appartiene pienamente né alla crittografia né alla steganografia. La crittografia convenzionale trasforma il messaggio rendendone il contenuto matematicamente inaccessibile, ma segnala l'esistenza della comunicazione – come si è osservato *supra*, al paragrafo 2. La steganografia cela l'esistenza del messaggio occultandolo in un vettore innocuo. Il codice migrante realizza qualcosa di diverso da entrambi: il messaggio è *visibile* ma il suo significato clandestino è *selettivamente inaccessibile* – opaco per i sistemi di sorveglianza, trasparente per i membri della rete. Si tratta di una forma comunicativa che non ha precedenti nella storia della crittografia convenzionale, e che richiede pertanto categorie analitiche genuinamente nuove.

Un'ultima considerazione merita attenzione sul piano etico e normativo. Le reti che impiegano il codice migrante non si compongono esclusivamente di trafficanti, disinformatori e organizzazioni criminali: esse includono anche i migranti stessi, che utilizzano questi strumenti per comunicare informazioni essenziali sulla propria sicurezza, per aggiornarsi sulle condizioni delle rotte, per mantenere i contatti con le famiglie nei paesi d'origine e per organizzare forme di mutuo soccorso tra pari. Un monitoraggio indiscriminato di questi canali rischia di intercettare comunicazioni di natura umanitaria accanto a quelle di natura criminale, sollevando questioni delicate sul bilanciamento tra esigenze di sicurezza e tutela dei diritti fondamentali degli individui in condizione di vulnerabilità strutturale[30]. La complessità etica di questo bilanciamento non può essere risolta con una semplificazione in senso puramente securitario: la ricerca accademica su questi fenomeni ha la responsabilità di mantenere una prospettiva plurale, che tenga conto sia delle necessità di contrasto alle attività criminali sia della tutela della dignità e dei diritti delle persone che – in quelle sequenze di *emoji*, in quei codici ibridi e translingui – cercano semplicemente una via verso una vita migliore.

goritmici di comunicazione clandestina, cfr. R. Anderson, *Security Engineering*, cit., pp. 3-25.

[30] Cfr. M. Empler, C. Capasso, *Metodi e tecniche di monitoraggio web*, cit., §§ 6-6.3, in cui vengono analizzate le implicazioni normative della raccolta di dati OSINT su popolazioni vulnerabili, con riferimento al GDPR e al Codice *Privacy* italiano.

I DATI PERSONALI COME INFRASTRUTTURA DELLA GUERRA COGNITIVA. ALCUNE PROPOSTE PER UNA RISPOSTA ISTITUZIONALE

Andrea Gatti[*]

1. *Le cornici normative per il contrasto alla guerra cognitiva: la convergenza tra privacy e cybersicurezza*

Quando si parla di guerra, il pensiero corre immediatamente alla sicurezza e, nel caso della guerra ibrida, alla cybersicurezza, di cui la dimensione cognitiva è generalmente considerata una componente. Una simile impostazione, tuttavia, rischia di essere riduttiva. In questo quadro, infatti, la tutela dei dati personali svolge una funzione non meno centrale, poiché non protegge soltanto una sfera privata in senso statico, ma presidia il potere dell'individuo di governare la circolazione delle informazioni che lo riguardano, decidendo autonomamente che cosa rendere accessibile e che cosa mantenere riservato. Proprio per questo la protezione dei dati e della privacy assume oggi il significato di tutela della proiezione identitaria e mentale della persona: essa salvaguarda non solo l'autodeterminazione informativa, ma anche le condizioni di integrità dell'identità individuale e di libertà cognitiva, tanto più nell'ambiente digitale, nel quale la raccolta, l'elaborazione e l'inferenza sui dati possono incidere direttamente sulla sfera psichica e decisionale del soggetto[1].

[*] Assegnista di ricerca in Diritto pubblico comparato nell'Università degli Studi di Padova e Consigliere giuridico della Vicepresidente del Garante per la Protezione dei Dati Personali.

[1] All'interno di questo contesto si inserisce anche la nota discussione sui neurodirit-

È vero che protezione dei dati personali e cybersicurezza differiscono quanto all'oggetto di tutela (diritto fondamentale, nel primo caso; interesse pubblico, nel secondo), tuttavia la loro convergenza – e direi quasi integrazione reciproca – è crescente: la cybersicurezza e i beni giuridici che essa protegge non riguardano solo il piano collettivo, ma incidono anche sulla fruizione dei diritti degli utenti e degli operatori economici. Se la reazione alle minacce *cyber* non è solo una questione "pubblicistica" o di "difesa nazionale", ma gioca altresì un ruolo fondamentale per la fruizione dei diritti fondamentali del cittadino – cioè è *garanzia* per tali diritti perché è intimamente connessa con la loro dimensione[2] – allo stesso modo anche la tutela dei dati personali sta diventando sempre più un'attività intrinsecamente polifunzionale. Nel momento in cui i dati diventano una risorsa economica e strategica, la protezione delle informazioni che riguardano la persona diventa essa stessa un interesse di rilevanza statale e democratica e l'aderenza alle norme in materia di trattamento dei dati personali aiuta a rafforzare la sicurezza dei sistemi, riducendo l'area di rischio informatico cui sono parzialmente esposti dati e informazioni rilevanti[3].

Lo stesso Regolamento europeo sulla protezione dei dati personali eleva la sicurezza a principio essenziale per la protezione dei dati, adottando un approccio sostanziale che presuppone come chi tratta dati si attivi per garantire la sicurezza delle reti e dell'informazione (spec. artt. 24, 25 e 32).

Più in particolare, quando si parla di preservazione dei dati, tanto di quelli personali che quelli non personali, nell'ottica della sicurezza informatica si fa riferimento a tre dimensioni che è necessario garantire che corrispondono a loro volta alle tre finalità della normativa di protezione dei dati: l'*integrità* (i dati devono essere completi e trattati in modo accurato); la *disponibilità* (i dati sono accessibili e fruibili su richiesta dei sog-

ti, situazioni giuridiche soggettive di vantaggio correlate all'impiego dei nuovi strumenti offerti dalle neuroscienze. Per un approfondimento, M. IENCA, R. ANDORNO, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sciences Society and Policy*, 2017, spec. pp. 13 ss. Cfr. anche F. CIRILLO, *Neurolaw, Neurorights and Neuroprivacy: Theoretical and Constitutional Issues*, in *MediaLaws*, n. speciale 1, 2024, pp. 212 ss.

[2] Non senza ragione c'è chi sostiene che la *cybersecurity* possa essere qualificata come diritto fondamentale, v. A. DI CORINTO, Data commons: privacy *e* cybersecurity *sono diritti umani fondamentali*, in *Rivista Italiana di Informatica e Diritto*, n. 1, 2022, pp. 31-37.

[3] Sul punto, v. anche G. D'IPPOLITO, G. DI MARTINO, *La privacy come elemento della cybersicurezza*, in *Consumerism 2021 – Quattordicesimo rapporto annuale*, 2021, pp. 12-20, su www.consumersforum.it.

getti interessati); la *riservatezza* (i dati sono accessibili solo da parte dei soggetti autorizzati). Tutte dimensioni che, in ultima analisi, sono comuni sia alla cybersicurezza che alla *privacy*.

Ciò implica chiaramente una forza di resistenza diversa nel momento del bilanciamento tra interessi; tuttavia, pur nella diversità di funzioni e obiettivi tra *cybersecurity* e protezione dei dati personali, emerge una loro sinergia, espressa anche dal punto di vista normativo da una costante e significativa simmetria in termini di prassi, istituti e procedure che accomunano il GDPR, le direttive NIS 1 e 2 (rispettivamente Direttiva UE n. 2016/1148 e Direttiva UE n. 2022/2555), il *Cybersecurity Act* (Regolamento UE n. 2019/881) e il *Cyber Resilience Act* (Regolamento UE n. 2024/2847).

Tutti gli ambiti disciplinari dedicano particolare attenzione al tema della sicurezza del trattamento e all'adozione delle adeguate misure di una sua garanzia e, di conseguenza, impongono obblighi (alle imprese o agli Stati membri) in materia di custodia dei dati, affinché gli operatori di servizi essenziali e i fornitori di servizi digitali adottino – pena rilevanti sanzioni – misure preventive adeguate ai rischi. Peraltro, per quanto riguarda la sicurezza cybernetica, la disciplina è quasi interamente mutuata da quella della protezione dei dati personali[4]. È infatti il GDPR ad avere per primo innalzato l'esigenza di sicurezza del trattamento a principio generale (art. 5, par. 1, lett. f.) e tale concetto incontra un'affinità – persino stilistica – con il *Cyber Resilience Act*. Non è un caso che anche l'*Ai Act* (Regolamento UE n. 2024/1689) abbia esplicitamente incluso i criteri della sicurezza *privacy* tra i requisiti essenziali di sicurezza per l'immissione nel mercato dei prodotti digitali[5]. Perciò ritengo che valga la pena di tenere in particolare riferimento la disciplina privacy come primo e fondamentale presidio non solo per l'identità e i diritti della personalità degli individui, ma anche, sebbene indirettamente, per l'architettura complessiva della sicurezza dello Stato.

[4] Cfr. Capo IV GDPR ed artt. 20-25 Direttiva UE n. 2022/2555 (NIS-2).

[5] Peraltro, l'istituzione di sistemi europei di certificazione della sicurezza informatica, la definizione di priorità strategiche sono appunto preordinate e la creazione di un "mercato della cybersicurezza" (il *digital single market*) sono appunto orientati a mettere i singoli soggetti in grado di fare la scelta più consapevole del livello di rischio in caso di acquisto di servizi o prodotti di TIC.

2. *Le novità della guerra cognitiva e perché essa è sempre* data-driven

La vera causa di ogni cosa è nel suo fine. Nella guerra cognitiva questa massima diventa quasi una regola metodologica. Per comprendere i bisogni alla base della lotta contro la guerra ibrida che le autocrazie stanno conducendo contro le nostre democrazie bisogna innanzitutto capire cosa si vuole raggiungere nella "guerra" contro la guerra ibrida.

Partiamo innanzitutto dal ricordare che nel lessico strategico contemporaneo, "guerra ibrida" e "disinformazione" indicano un insieme di pratiche che non mirano soltanto a distruggere infrastrutture o a conquistare territori, ma a erodere la coesione sociale, la fiducia istituzionale e la capacità decisionale collettiva. La guerra cognitiva è un conflitto che mira a danneggiare non le infrastrutture civili e militari, ma quelle "sociali" a partire, appunto, dalle coscienze e lo fa attraverso tecniche di propaganda sempre più sofisticate. Questa è la guerra che a noi giuristi dovrebbe interessare di più perché, rispetto ai paradigmi finora adottati in materia di libertà di informazione, introduce categorie e strumenti nuovi per affrontare i quali è necessario superare gran parte dell'impostazione finora seguita con riferimento alla libertà di informazione.

Si notano così due novità che riguardano l'una, l'inquinamento del sistema informativo e, l'altra, la trasformazione dell'ambiente informativo.

Sotto il primo aspetto, è stato ormai accertato il raffinamento delle tecniche di propaganda[6]. La guerra cognitiva segna il passaggio dalla propaganda dichiarativa e contenutisticamente univoca a tecniche di manipolazione informativa ambientale, reticolare e mimetica, orientate non già alla persuasione su un singolo enunciato, bensì alla compromissione delle condizioni di possibilità del discorso pubblico democratico. Il suo effetto tipico è, infatti, la produzione strategica di dubbio, contraddizione e disorientamento, mediante lo sfruttamento delle vulnerabilità cognitive ed emotive della sfera pubblica[7]. Lo scopo è, così, la destabilizzazio-

[6] A. STERPA, *La difesa della democrazia dalle minacce ibride. Teorie della comunità, dell'autorità, del potere e migrazioni: elementi per un'analisi strategica della "guerra tiepida"*, Editoriale Scientifica, Napoli, 2025. Ma anche S. SASSI, *Disinformazione contro Costituzionalismo,* Editoriale Scientifica, Napoli, 2021, nonché il contributo in questo volume.

[7] Sulla disinformazione come mera messa in dubbio delle informazioni ufficiali e fattuali delle istituzioni democratiche al fine di eroderne l'integrità e la credibilità, OECD, *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, 2024. In particolare le analisi si concentrano sul modello di disinformazione russo e lo descrivono

ne delle condizioni epistemiche della democrazia, cioè dei presupposti minimi che consentono una formazione libera e consapevole dell'opinione pubblica e della volontà politica, e la menomazione indiretta di beni costituzionali quali la sicurezza nazionale, la pace sociale, il pluralismo informativo, la fiducia nelle istituzioni e l'integrità formazione del processo democratico. Negli ordinamenti democratici, l'opinione pubblica è un processo la cui qualità dipende da condizioni strutturali come il pluralismo delle fonti, la trasparenza degli intermediari, la possibilità di critica e controllo, la circolazione di argomenti e, non da ultimo, una sfera di autonomia personale in cui ciascuno possa formare convinzioni senza essere permanentemente classificato e ridotto a un *target* di sistemi che funzionano peraltro in modo opaco[8].

Ed è qui che si inserisce il secondo (e forse più importante) aspetto e fattore di novità della guerra cognitiva, cioè l'organizzazione di ambienti di percezione e di comportamento adatti alla più efficace ricezione della disinformazione e lo fa attraverso la combinazione tra profilazione automatizzata – ormai spinta fino alla psicografia – e *targeting* politico. La profilazione, cioè l'analisi e la valutazione degli aspetti di una persona fisica in modo da prevederne il comportamento futuro, è la precondizione tecnica della persuasione "su misura" dal momento che tramite essa si tende a restituire contenuti che possono far breccia nell'interesse e nella sensibilità del soggetto, spesso accostandoli a contenuti simili a quelli già consumati[9]. L'idea che i dati possano essere piegati politicamente e, dunque, diventare arma della guerra cognitiva va però formulata con precisione. Non si tratta di sostenere che ogni profilazione produca automaticamente manipolazione, ma di riconoscere che essa, per sua natura, è orientata all'influenza e, nel farlo, tende a ridurre la complessità del

come una propaganda rapida, massiva, contraddittoria e priva di coerenza, efficace anche attraverso "offuscazione e "confusione" (RAND, Information Enviroment, in www.rand.org, 2021.

[8] Sull'impatto che la società digitale produce in relazione a tali fattori, tra la numerosa dottrina, v. già C.R. Sunstein, *#Repubblic. La democrazia nell'epoca dei social media*, il Mulino, Bologna, 2017, spec. pp. 20 ss. e 127 ss.; S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Bari, 1997, pp. 47 ss. Recentemente, A. Simoncini, E. Longo, *Digital Constitutionalism and Fundamental Rights: Reconfiguring Liberty and Power*, in *The Oxford Handbook of Digital Constitutionalism*, Oxford University Pres, Oxford, 2026, pp. 1-21.

[9] Sulla questione si consenta un rinvio a A. Gatti, *Profilazione e diritti fondamentali. Modelli a confronto: Europa, USA, America Latina*, Editoriale Scientifica, Napoli, 2025, in part. pp. 33 ss.

dibattito e la capacità di scelta dell'utente, restringendone l'orizzonte cognitivo fino, talvolta, a condizionarne il comportamento[10].

Ma la guerra cognitiva, grazie al trattamento automatizzato dei dati personali, non cambia soltanto sotto il profilo qualitativo, vale a dire diffondendo contenuti disinformanti con maggiore precisione di analisi e capacità di convincimento, bensì anche sotto quello che riguarda il mezzo o, meglio, l'infrastruttura. Se in epoca analogica la propaganda utilizzava canali "mediati" (la linea editoriale di un giornale, il palinsesto di un canale, ecc.) e, dunque, "riconoscibili", oggi essa sfrutta e persino organizza ambienti di ricezione e percezione adatti alla più efficace ricezione di tali contenuti attraverso la combinazione tra profilazione automatizzata e *targeting* politico.

Questa è la seconda novità che merita di essere approfondita.

3. *I luoghi della guerra cognitiva* data-driven*: i* social network *e la nuova infrastruttura della persuasione*

Quando si afferma che l'IA diviene una "superficie di controllo" tra utente e sistema, lo si intende nel senso che essa opera come infrastruttura attraverso cui vengono modulati la pressione persuasiva e la soglia di attenzione, fino a ridisegnare interi percorsi decisionali. Se la profilazione automatizzata costituisce una delle infrastrutture della guerra cognitiva, ne segue che la risposta istituzionale deve considerare non solo i contenuti, ma anche i luoghi e le architetture attraverso cui tale pressione si esercita.

È stato al proposito già ampiamente rilevato dalla dottrina il ruolo dei *social network* nella creazione di ambienti di proliferazione della guerra cognitiva[11]. Attraverso il veicolo dei *social*, spazi solo apparentemente

[10] A. PIN, *Libertà di coscienza e intelligenza artificiale*, in *Coscienza e libertà*, 2024, pp. 145-156.

[11] «La formazione del consenso politico ed elettorale sia sempre più marcatamente influenzata dall'uso dei *social networks* e come, attraverso di essi, soggetti organizzati perseguano il fine di orientare le posizioni politiche dei singoli attraverso messaggi "targettizzati" e preordinati a "colpire" la parte più moderata e indecisa del corpo elettorale», così A. CARDONE, *Profilazione a fini politico-elettorali e tenuta della democrazia rappresentativa: una lezione per le riforme istituzionali e per la regolazione del pluralismo democratico in Rete*, in A. ADINOLFI, A. SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Editoriale Scientifica, Napoli, 2022, pp. 131-146, spec. p. 134. Dello stesso tenore

neutri e solo apparentemente non mediati che fondano sui dati personali la loro catena di valore[12], le tre matrici operative "classiche" del metodo della guerra cognitiva, vale a dire la ripetizione intensiva, l'attivazione emotiva e l'apparenza di consenso[13], trovano il miglior propulsore perché esse sono già inglobate in un ecosistema che, per sua natura, le trasforma in segnali computazionali e premia i contenuti che attivano reazioni, in particolare quelli eccitanti o divisivi. La "questione TikTok" è divenuta paradigmatica perché porta in superficie ciò che in altri contesti tende a rimanere sottotraccia, che cioè dati personali e algoritmi di raccomandazione non sono soltanto risorse economiche, ma componenti di una tecnologia geopolitica di carattere strategico[14]. L'oggetto del contendere non è la singola informazione riferibile all'utente, bensì l'architettura complessiva che si forma attraverso la raccolta sistematica di tracce com-

anche C. Casonato, *L'intelligenza artificiale e il diritto pubblico comparato ed europeo* e L.G. Sciannella, *Intelligenza artificiale, politica e democrazia*, entrambi in *DPCE online*, n. 1, 2022, rispettivamente pp. 169-179 e pp. 337-348.

[12] Sul *rule of platforms* come «ordine giuridico dell'algoritmo», v. ancora A. Sterpa, *La difesa della democrazia dalle minacce ibride*, cit., spec. pp. 57 ss., il quale utilizza appunto tale espressione per intendere il sistema in cui l'algoritmo esercita una funzione ordinatrice che tende a competere con la funzione ordinatrice del diritto.

[13] Con la ripetizione intensiva non si punta soltanto a "convincere", ma a rendere un contenuto familiare. L'effetto di familiarità riduce la soglia critica: ciò che è ripetuto appare "normale", e ciò che è normale appare plausibile. Con l'attivazione emotiva vengono preferiti i contenuti che attivano la soglia di attenzione come quelli che suscitano paura, indignazione, minaccia, appartenenza, umiliazione, risentimento. L'utilizzo dell'emozione diventa un vettore perché massimizza le reazioni, i commenti e le condivisioni che aiutano il contenuto a circolare e a monetizzare. Infine si dota il contenuto di apparenza di consenso facendo credere che il messaggio giunga da molte fonti apparentemente diverse (account distinti di utenti comuni o *micro-influencer*, *repost*, pagine di giornale, ecc.), generando così un effetto di convergenza e, di conseguenza, di "prova sociale": se molti lo dicono, sarà vero. La pluralità apparente è spesso costruita senza autenticità attraverso bot e reti artificiali.

[14] Secondo una ricerca del Network Contagion Research Institute (NCRI) e Rutgers, *A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese*, in networkcontagion.us, 2023, che ha analizzato i rapporti degli hashtag tra Instagram e TikTok su argomenti giudicati sensibili per il Governo cinese, mentre i rapporti di visualizzazioni su argomenti non sensibili (ad esempio sulla cultura pop) generalmente seguivano i rapporti degli utenti (~2:1), le visualizzazioni sugli argomenti sensibili, fossero per questioni nazionali/regionali o internazionali, presentavano valori molto più alti (>10:1). Queste anomalie emergono in maniera costante ed evidente: l'hashtag "*I-stand-for-Ukraine*", ad esempio, appare avere una visualizzazione 13 volte inferiore rispetto allo stesso hashtag di Instagram. Mentre quello "*I-stand-for-Kashmir*", più di 600 volte rispetto a quello di Instagram (13 ss.).

portamentali e la loro elaborazione in capacità di previsione, selezione e, in ultima analisi, influenza. Sempre con riferimento al caso TikTok negli Stati Uniti, dalla dichiarazione della piattaforma come "*foreign adversary controlled*" allo svilente mercanteggiamento per la sua cessione, esso appare la prova lampante della strumentalità bellica del *social* cinese: la decisione sulla vendita di TikTok è stata assunta non dall'azienda ma direttamente dal Governo cinese.

Ma il riverbero del piano individuale investe anche la dimensione collettiva attraverso un ulteriore effetto collaterale della profilazione: la creazione delle cc.dd. *echo chambers*, bolle informative in cui l'utente riceve solo le informazioni sartoriali adeguate alle sue inclinazioni (mentre non riceve quelle dissonanti). Nel continuo e quasi esclusivo confronto con idee politiche ad esse affini si creano le cc.dd. *filter bubbles*[15] – fenomeno possibile soltanto in presenza di un tracciamento preciso dei gusti, delle preferenze e delle vulnerabilità dell'individuo – si alimenta quella che è stata efficacemente definita *bubble democracy*: una democrazia ghettizzata e "customizzata", dalla quale trae apparente beneficio il cliente-elettore, al quale viene "offerto" il prodotto politico adatto a lui, sottraendolo ad un confronto con posizioni diverse dalla propria originaria posizione di partenza[16]. Questo meccanismo, che potremmo definire di "segregazione algoritmica", ha già inciso profondamente sugli equilibri politici e ideologici, soprattutto nelle democrazie post-moderne, alimentando dinamiche di polarizzazione con cui molti Paesi oggi fanno i conti. Ne

[15] Vale a dire delle "bolle" informative in cui l'utente, rinchiuso, riceve solamente notizie e commenti conformi alle proprie opinioni e pregiudizi. Così già E. PARISIER, *The Filter Bubble: What the Internet Is Hiding from You*, Penguin, New York, 2011.

[16] Lo circostanziano, tra gli altri, G. DA EMPOLI, *La rabbia e l'algoritmo*, Marsilio, Venezia, 2017, pp. 20-21: «In termini politici l'avvento dei *big data* è paragonabile all'invenzione del microscopio punto in passato sulla base di sondaggi sempre aleatori i comunicatori politici potevano prendere di mira grandi aggregazioni demografiche o professionali giovani gli insegnanti della scuola pubblica le casalinghe così via appunto oggi i big data permettono di rivolgere al singolo elettore un messaggio personalizzato sulla base delle sue caratteristiche individuali. Ciò consente una comunicazione molto più efficace e razionale, ma solleva anche un certo numero di problemi». Così anche A. SORO, *Persone in Rete. I dati tra poteri e diritti*, Fazi, Roma, 2018, spec. p. 30: «Il web tende a riproporci contenuti informativi analoghi a quelli già consultati, generando così una spirale autoconfermativa che finisce con il limitare, paradossalmente, lo spettro di informazione quindi la stessa possibilità di opinioni diverse. Il rischio, insomma, è quello di una sorta di autismo informativo: ovvero la tendenza a informarsi soltanto da fonti inclini a confermarci le nostre pregresse convenzioni, ostacolando ogni possibilità di riscontro su false notizie o credenze».

consegue che cittadini inseriti nella medesima comunità politica finiscono per maturare visioni molto diverse su una pluralità di temi, senza un reale confronto reciproco. Ma se le *filter bubbles* e le *echo chambers* sono sicuramente qualificabili come effetti collaterali dell'economia del dato, esse possono altresì trasformarsi in dispositivi di vulnerabilizzazione cognitiva tanto dell'utente-cittadino, più permeabile a narrazioni distorsive, tanto della politica in sé[17].

4. *Dati personali, consenso democratico e libertà di formazione dell'opinione pubblica*

Il 4 aprile 2024 il Microsoft Threat Analysis Center (MTAC) ha pubblicato un *report* sulle principali minacce informatiche alla stabilità dei paesi democratici provenienti dall'Asia e ai mezzi perseguiti per darne seguito. Tra i vari episodi, nel documento si illustra come la Cina avesse provato ad influenzare le elezioni di Taiwan del gennaio dello stesso anno e come, dal settembre 2023, abbia cercato di inquinare, attraverso falsi *account social* e *bot* di disinformazione, le elezioni presidenziali americane dell'autunno 2024. Falsi utenti di *social media* che impersonificavano elettori americani, in realtà gruppi informatici affiliati al Governo cinese, prima di essere bloccati hanno pubblicato messaggi con un alto profilo politico e provocatorio che, come afferma il report, richiamavano «*nearly exclusively about US domestic issues – ranging from American drug use, immigration policies, and racial tensions*»[18]. I troll non si limitavano a postare o a condividere video, *meme* o infografiche, ma interagivano con gli utenti che a loro volta li commentavano. L'obiettivo diretto che essi perseguivano era quello della disinformazione e della provocazione in modo da incrementare le già forti divisioni sociali nel Paese. Ma l'aspetto inte-

[17] Il rischio risiede nella creazione di una c.d. *dog whistle politics*, in cui il segnale di richiamo non è per tutti percepibile o non lo è per tutti nello stesso modo. Cfr. I. Haney-López, *Dog whistle politics: How coded racial appeals have reinvented racism and wrecked the middle class*, Oxford University Press, Oxford, 2014.

[18] Microsoft Threat Analysis Center, *Same targets, new playbooks: East Asia threat actors employ unique methods, spec. 11,* in *Microsoft Threat Intelligence,* aprile 2024*,* ma anche China tests US voter fault lines and ramps AI content to boost its geopolitical interests, in *Clint Watts – General Manager, Microsoft Threat Analysis Center*, 4 aprile 2024. In realtà un'operazione simile era già stata scoperta da Meta nel 2023 quando migliaia di falsi profili operati dalla Cina millantavano di essere cittadini statunitensi per commentare post su politica con l'obiettivo di polarizzare l'informazione.

ressante ai nostri fini è piuttosto il loro obiettivo indiretto: interagendo con gli utenti, chiedendo loro opinioni sui temi politici da essi condivisi, sul loro supporto ad un candidato piuttosto che ad un altro, il Governo cinese, secondo l'istituto di ricerca, avrebbe raccolto e analizzato in modo dettagliato la demografia e le preferenze degli elettori americani, per poi concentrare altri tipi di attività persuasive negli *swing* States.

Questo episodio, tra i tanti che si potrebbero ricordare, ci introduce ad un altro aspetto di rilievo costituzionale in riferimento alla profilazione nella sua forma di *microtargeting*, quello che riguarda la tenuta democratica e l'inquinamento nei processi formativi dell'opinione pubblica. Le criticità si legano, in particolare, all'evoluzione delle stesse tecniche di profilazione, focalizzate inizialmente sul modello di profilazione individuale e, successivamente, anche grazie ai vantaggi dei *big data* (e dunque attraverso un trattamento interamente automatizzato), orientate su modelli di analisi di massa. Questo ovviamente non interessa soltanto la coscienza del singolo elettore, ma incide sulla manipolazione dell'aggregazione del consenso e sul corretto funzionamento della democrazia rappresentativa.

La questione si può declinare in numerosi sotto-ambiti, ma per quel che ci riguarda ci si soffermerà ai pericoli riguardanti la formazione della volontà popolare in senso stretto. Qui i *big data* possono fungere da elementi di controllo "dall'alto", ottimizzando la capacità di raggiungere determinati utenti o gruppi di utenti attraverso il *microtargeting*, oppure possono essere influenzati "dal basso", attraverso le condotte degli utenti che li modellano (v. § seguente).

Sotto il primo profilo, quello del *microtargeting*, richiamando in parte quanto già accennato nel § 2, vediamo che l'influenza avviene attraverso l'indirizzamento di comunicazioni e notizie appositamente selezionate (non raramente anche già alterate) verso destinatari individuati tramite il trattamento predittivo. Questo condizionamento avviene attraverso l'accesso e l'utilizzo dei dati personali che permette di selezionare i grandi *trend* da offrire ai cittadini. L'invio di notizie manipolate non deve rivolgersi all'intero elettorato passivo (ed anzi, meglio che non lo faccia perché, nei grandi numeri, ci sarebbe chi potrebbe facilmente smentirle): è strategicamente più vantaggioso portarle a conoscenza di insiemi ideologicamente omogenei che si suppone essere particolarmente sensibili ai temi e dunque meno disposti a leggerle con spirito critico. Tale pratica molto si avvicina ad una pervasiva pubblicità subliminale[19].

[19] P. CIARLO, *Democrazia, partecipazione popolare e populismo al tempo della rete*, cit.,

Ma c'è di più: è verosimile che lo sviluppo tecnologico ci consenta di portare questa linea di sviluppo a ben più estreme conseguenze. Si nota già oggi che la profilazione supportata dalla psicometria e dalle neuroscienze "droga" la coscienza collettiva portando a qualcosa che non va molto lontano dalla psicopolitica teorizzata dal filosofo Han: «I *big data* rendono leggibili, forse, i nostri desideri, dei quali noi stessi non siamo espressamente coscienti. In effetti in determinate circostanze sviluppiamo inclinazioni che si sottraggono alla nostra coscienza; spesso non sappiamo neppure perché all'improvviso compare in noi un certo bisogno[20]».

I *big data*, o meglio, i loro "*big interpreters*", accedono al regno dell'inconscio e "denudano" il nostro cervello.

Il rischio che se ne ricava non si limita alla mera deformazione della reale estensione del quadro delle singole opinioni e visioni politiche degli utenti-cittadini rispetto a fatti specifici, ma assume carattere sistematico e si traduce tanto in un indebolimento della c.d. *situation awareness* dei cittadini stessi – cioè della loro capacità di percepire, comprendere e prevedere elementi critici del proprio ambiente per prendere decisioni informate – quanto in una "balcanizzazione" della stessa vita politica[21],

p. 7. A mettere in relazione il *microtargeting* pubblicitario (e la pubblicità subliminare) con quello elettorale, B-C. Han, *Infocrazia. Le nostre vite manipolate dalla rete*, Einaudi, Torino, 2021. Non a caso è stato dimostrato come laddove l'utente prenda consapevolezza di essere sottoposto a pratiche di personalizzazione per influenzare il proprio comportamento elettorale, e laddove venga percepito come una manipolazione, ciò produce ricadute molto negative sulla fiducia verso la legittimazione e l'integrità e del processo elettorale e decisionale democratico ma allo stesso tempo, come una sorta di reagente psicologico, può accrescere l'interesse nell'adottare un approccio critico e proattivo verso la politica. Così C. Bennett, *Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?*, in *International Data Privacy Law*, 6(4), 2016, 261-275, 270. J. Matthes, M. Hirsch, M. Stubenvoli, A. Binder, S. Kruikemeier, S. Lecheler, L. Otto, *Understanding the democratic role of perceived online political micro-targeting: longitudinal effects on trust in democracy and political interest*, in *Journal of Information Technology & Politics*, 19:4, 2022, pp. 435-448, spec. p. 439.

[20] B-C. Han, *Psiscopolitica*, Nottetempo, Roma, 2016.

[21] Cfr. ancora E. Parisier, *The Filter Bubble*, cit., ma soprattutto C.R. Sunstein, *#Republic.*, cit., spec. pp. 16, 19 e 79 ss., che definisce due poteri degli attori digitali, da una parte quello degli utenti di filtrare ciò che vedono, dall'altra quello delle piattaforme di assecondare i gusti degli utenti sulla base di ciò che di loro conoscono, come i due maggiori rischi per la libertà di parola in una società che si autogoverna. È sempre Sunstein a parlare di *echo-chambers* (camere di risonanza) o *information cocoonos* (bozzoli informativi) come modi che assecondano l'estremismo violento («le persone con idee affini si aizzano a vicenda in un crescendo di rabbia, le conseguenze possono essere assai pericolose»). Recentemente, in Italia, G. Fontana, *Sfera pubblica digitale e democrazia*

con un impatto negativo sugli equilibri e sulla pace sociali. L'utilizzo della profilazione da parte della disinformazione, ad esempio, può alimentare il fenomeno dell'*hate speech* e gli episodi di intolleranza. Ciò avviene perché la creazione di "bolle" informative favorisce dinamiche di auto-rafforzamento tra i consociati e abbassa le soglie di autocontrollo, rendendo più probabile l'esternazione di posizioni estreme che, in un contesto esposto a fonti più pluralistiche, sarebbero più facilmente contenute o, quanto meno, sottoposte a critica.

5. *La (disinter)mediazione dei contenuti nella personalizzazione algoritmica basata su dati personali*

Il secondo profilo accennato nel paragrafo precedente, l'influenza degli utenti "dal basso" attraverso le condotte che loro stessi modellano (o pensano di modellare), ha a che fare con un ulteriore fenomeno sfruttabile nella guerra cognitiva, quello della (apparente) disintermediazione dei contenuti.

Dopo la loro raccolta e la loro analisi, la massa di dati aggregati (personali e non) a disposizione di ogni piattaforma – inclusi il numero assoluto di *like*, le condivisioni, le parole chiave utilizzate nei commenti e le generali caratteristiche dei gruppi di utenti – viene tradotta in "*trending topics*", sorte di indicatori che rivelano i "contenuti rilevanti" per gli utenti. Come già detto, gli utenti vedono direttamente ciò che a loro interessa o può interessare.

Sotto tale aspetto l'algoritmo viene utilizzato per disintermediare le comunicazioni rispetto agli attori tradizionali dell'informazione e, così, creare nuovi canali che sfuggono al controllo. Tutto ciò, ad un primo sguardo, fa apparire la profilazione automatizzata più democratica rispetto al mondo intermediato perché dà all'utente la possibilità di approfondire i propri interessi e, in relazione ad essi, ottimizzare la propria conoscenza e, tuttavia rispetto all'intermediazione umana (persino quella faziosa e disinformante), si pongono ulteriori elementi di criticità da non trascurare.

C'è innanzitutto una eliminazione o, quantomeno, una sostituzione degli esperti dell'informazione. Mentre i giornalisti professionisti o alcune istituzioni selezionano le notizie in base a regole e prassi professionali,

nell'Unione europea. Prime considerazioni intorno alla dichiarazione europea sui diritti e i principi digitali, in *La trasformazione digitale in Europa. Diritti e principi*, 2023, pp. 35-74, spec. pp. 43 ss.

su molte piattaforme di contenuto, a partire da TikTok, Youtube e X, i cc.dd. *content creators* si propongono come opinionisti e persino cultori di geopolitica o di strategia militare. Sebbene molti di questi profili siano proposti da persone informate e in buona fede, alcuni di questi canali possono (e sono in effetti) utilizzati da soggetti politici ostili all'Europa per far veicolare scientemente, da *influencer* prezzolati (o persino da semplici bot come avviene su X o su TikTok), messaggi artificiosamente destabilizzati per le nostre democrazie. Gli utenti "sensibili", come già detto, vengono raggiunti proprio attraverso l'utilizzo dei dati personali rivelatori delle loro preferenze. Qui però si affacciano almeno due questioni ulteriori.

La prima criticità, con riguardo la disinformazione operata da *influencer*, riguarda la peculiare elusività sul piano regolatorio della figura: tale soggetto opera, infatti, in una zona grigia che spesso lo sottrae all'applicazione delle regole tradizionalmente poste a presidio dell'informazione professionale, pur consentendogli di incidere in modo significativo sulla formazione dell'opinione pubblica, anche mediante la diffusione di contenuti disinformativi. Si apre qui il più ampio problema dell'individuazione dei presupposti e dei criteri necessari per l'applicazione della normativa volta a contrastare la disinformazione; questione, tuttavia, che esula dall'oggetto specifico del presente saggio. L'idea è che i messaggi circolano spesso come comunicazione "tra pari" e non da fonti professionali ufficiali, e così facendo essi possano sottrarsi più facilmente alle verifiche, ai *fact-checking* e, dunque, alle responsabilità. «È una mia opinione», essi potrebbero dire e così si riespande in massimo grado la portata della libertà di manifestazione del pensiero.

Ma l'uso della profilazione algoritmica può anche comportare una totale assenza di intermediazione umana. In questo caso è l'algoritmo stesso ad eliminare tale mediazione e a porsi come "esperto" nel campo dell'informazione e della politica, come avviene per i *Large Language Models* o per alcuni profili di app sociali come TikTok quando esso si propone come canale di informazione. È però più che possibile (ed anzi in molti casi è già stato dimostrato) che, nel caso di app cinesi o di alcune app americane, all'informazione venga sovraordinato un interesse (politico, militare o economico) che si vuole promuovere e ciò costituisce uno dei varchi principali attraverso cui si inseriscono le operazioni di guerra cognitiva[22]. Le risposte di *Deepseek* o i video "informativi" di

[22] Cfr. P. Qiu, S. Zhou, E. Ferrara, *Information suppression in large language models: Auditing, quantifying, and characterizing censorship in DeepSeek*, in *Information Sciences*,

TikTok non solo sono ideologicamente orientati e limitati, ma le informazioni da essi raccolte entrano in possesso della Repubblica popolare cinese che poi le potrà usare (le userà) per ulteriori operazioni di guerra ibrida.

Un'ulteriore complicazione risiede nel fatto che, conoscendosi assai meno l'*iter* decisorio dell'algoritmo di quello umano, l'opacità nella fase di selezione dei contenuti ne risulta aggravata e, anche quando la scelta è presentata come prodotto delle attività degli utenti, essa avviene anche sulla base di codici che sono pienamente identificabili[23]. Quindi, anche se le risultanze fossero genuinamente la somma delle interazioni degli utenti senza alcuna manipolazione a monte, rimane il rischio che le scelte su cosa mostrare all'utente o non siano chiare o dipendano solo dall'interesse aziendale. E ciò comporta che, nel migliore dei casi, verrà privilegiata la mera popolarità del contenuto sul suo valore (la profilazione non ci dà la risposta migliore per noi, ma quella che risulta più conveniente)[24] con le conseguenze dannose, in termini di sicurezza, che diremo nel paragrafo seguente.

Volume 724, 2026, 1 ss.; ma anche Parlamento europeo, *TikTok and EU regulation: Legal challenges and cross-jurisdictional insights* (Briefing), in www.europarl.europa.eu. giugno 2025, pp. 4-5.

[23] Guardiamo ad esempio al caso di TikTok: secondo una ricerca del Network Contagion Research Institute (NCRI) e Rutgers, *A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese*, in networkcontagion.us, dicembre 2023, che ha analizzato i rapporti degli hashtag tra Instagram e TikTok su argomenti giudicati sensibili per il Governo cinese, mentre i rapporti per argomenti non sensibili (ad esempio, politica generale e cultura pop) generalmente seguivano i rapporti degli utenti (~2:1), i rapporti per gli argomenti sensibili, fossero per questioni nazionali/regionali o internazionali, presentavano valori molto più alti (>10:1). Queste anomalie emergono in maniera costante ed evidente: l'hashtag "I-stand-for-Ukraine", ad esempio, appare avere una visualizzazione 13 volte inferiore rispetto allo stesso hashtag di Instagram. Mentre quello "I-stand-for-Kashmir", più di 600 volte rispetto a quello di Instagram (13 ss.).

[24] Un problema che in parte fuoriesce dall'oggetto del presente lavoro, ma che appare rilevante su un piano etico e giuridico (l'interesse della società democratica), riguarda la "qualità" delle risposte. Pensiamo al funzionamento di Chat GPT: le risposte dell'algoritmo sono generate attraverso algoritmi di *machine learning* basati su un vasto corpus di dati testuali presenti nel database che sono la somma delle informazioni e degli input condivisi dagli utenti sul web. Quanto questo, talvolta, possa rispettare l'integrità accademica e il rispetto dei principi alla base del nostro ordinamento politico-costituzionale non è sempre chiaro.

6. *La fusione tra guerra cognitiva e modello di business: il profitto come acceleratore dell'ideologia*

La personalizzazione delle opzioni offerte all'individuo si accompagna, paradossalmente, a un processo di spersonalizzazione del soggetto stesso. Ciò accade perché le azioni individuali, una volta registrate, cessano di essere considerate nella loro dimensione propria di "attività" e vengono invece tradotte in dati suscettibili di valorizzazione economica. È questo il fenomeno della c.d. dataficazione, che consiste nella progressiva trasformazione delle condotte umane e, in ultima analisi, degli stessi individui, in oggetti informazionali, ossia in sequenze di dati riconducibili a categorie predeterminate e trattabili in funzione di finalità predittive, commerciali o di indirizzamento comportamentale[25]. In tale contesto, una delle trasformazioni più rilevanti dell'ultimo decennio è rappresentata dalla convergenza tra i meccanismi della guerra cognitiva e quelli propri dell'economia dell'attenzione, la quale, a sua volta, si alimenta delle logiche dell'economia del dato. Tale convergenza segna un passaggio di particolare rilievo anche sul piano causale, poiché moltiplica i fattori che accrescono la capacità espansiva e penetrativa delle operazioni di influenza cognitiva.

Non ci si trova più davanti a una propaganda che utilizza mezzi commerciali come meri strumenti, bensì a un sistema in cui il modello di *business* e la dinamica ideologica si sostengono a vicenda. L'incentivo economico premia ciò che cattura l'attenzione, polarizza, indigna, mobilita; ne consegue che la comunicazione politica più aggressiva o identitaria – metodo principale della guerra cognitiva russa e cinese contro l'occidente – trovi una corsia preferenziale, in quanto maggiormente conforme alle metriche che presiedono alla visibilità, alla circolazione e alla monetizzazione dei contenuti.

Il risultato è un mutamento quasi rivoluzionario di paradigma per cui oggi non è solo l'ideologia a trascinare il business (quel determinato contenuto piace a quel determinato utente), ma anche il business a trascinare l'ideologia, generando ecosistemi di contenuti dove la radicalizzazione è al tempo stesso mezzo e fine. In questo quadro, non è neppure necessario che chi produce o diffonde contenuti estremi vi creda poiché ciò che conta è il rendimento in termini di visualizzazioni, interazioni e, dunque,

[25] J.v. Dijck, T. Poell, M. De Waal, *The Platform Society. Public Values in a Connective World*, Oxford University Press, Oxford, 2018, spec. 35 ss. Ma anche M. Ferraris, *Documanità. Filosofia del mondo nuovo*, Laterza, Bari, 2021, pp. 39 ss.

ricavi. Il rischio è quindi di rinforzare inconsapevolmente e mimeticamente, attraverso influencer e *repost*, la macchina bellica russa, cinese o di quelle forze che, all'interno dell'occidente, mirano al sovvertimento dell'ordine liberal-democratico attuale attraverso la produzione di un effetto di consenso diffuso che è uno dei cardini della guerra cognitiva.

Alla commistione tra interesse economico e interesse politico, si affianca infine un'ultima conseguenza, la frammentazione e la diluizione delle responsabilità. Rispetto a questo fenomeno, una risposta di taglio costituzionalistico non può che partire dal rilievo che la "zona grigia" non è un mero difetto tecnico, bensì un effetto strutturale dell'ecosistema digitale poiché è la catena stessa di produzione dell'influenza che, distribuendo i poteri, al tempo stesso li diluisce. Per evitare che l'ordinamento si limiti a inseguire il fenomeno, occorrerebbe ricondurre la disciplina a un bilanciamento esplicito tra *privacy*, libertà di manifestazione del pensiero e pluralismo (art. 21 Cost.) e libertà dell'iniziativa economica (art. 41 Cost.). La demonetizzazione del contenuto è senz'altro la strada più efficace. Un'ulteriore via potrebbe essere quella di lavorare sui *trend* e sulle raccomandazioni in coordinamento con le grandi piattaforme, facendo in modo che alcuni profili non siano raccomandati e, dunque, modulando la visibilità e la selezione del pubblico. Entrambi questi sistemi posseggono anche dei lati oscuri in quanto rischiano di produrre un effetto di autocensura che investe le opinioni in quanto tali.

7. *La privacy come difesa della democrazia: possibili soluzioni* de iure condendo

Il tratto davvero nuovo che emerge dall'uso dei dati personali alla guerra cognitiva risiede non tanto nel fatto che i sistemi "profilino di più", ma nel fatto che la profilazione sia divenuta l'infrastruttura della personalizzazione e del coordinamento dei dati e del loro valore.

Non dobbiamo cadere nell'equivoco che la profilazione permetta una reale disintermediazione dell'informazione e dunque la "liberazione della conoscenza" solo per il fatto che noi "scegliamo" cosa vedere. Tutt'altro: per usare un'espressione di Maurizio Ferraris, la Rete è "mobilitazione" più che "emancipazione"[26], non fornisce di per sé liberazione, come si riteneva all'inizio, ma invita semplicemente ad agire e capitalizza le azioni compiute e in questo si configura come uno strumento di dominio.

[26] M. FERRARIS, *Documanità*, cit., pp. 37 ss.

Appare però difficile porre limiti alla possibilità di profilazione, poiché sui *social* essa è ormai quasi inestricabilmente legata con la libertà di informazione, in particolare nella sua dimensione "passiva"[27] (sebbene vi sarebbe da riflettere se gli utenti, con i loro *like* e *repost* che drogano ed eccitano l'algoritmo non stiano esercitando anche una informazione "attiva" rispetto ai contenuti politici e informativi con cui interagiscono).

In questo quadro della minaccia ibrida le tutele "a valle" – vale a dire i rimedi individuali, le sanzioni e gli obblighi di trasparenza e di enforcement caso per caso – risultano strutturalmente tardive. Se, come si è detto, la guerra cognitiva mira soprattutto a modellare l'ambiente informativo, la "infrastruttura" per colpire le scelte collettive, è necessario altresì intervenire anche "a monte".

Si possono delineare alcune soluzioni che, sul piano sistematico, appaiono ragionevoli.

Innanzitutto la prima che appare quella di ridurre la superficie d'attacco, per prendere in prestito un termine dalla cybersicurezza: dal momento che la disponibilità di dati personali è un moltiplicatore di capacità operativa (più esteso è il tracciamento, più raffinate e ampie diventano le campagne di influenza), la riduzione delle informazioni esposte, vale a dire l'applicazione dei principi GDPR di minimizzazione e limitazione della finalità intesi come vincoli sistemici contro l'accumulazione illimitata e la riusabilità opportunistica dei dati, appare senz'altro utile.

Una seconda linea consiste nel rafforzare i presidi di trasparenza, segnalando ad esempio in maniera chiara e obbligatoria la ragione per cui un utente vede quel determinato contenuto, cioè rendendo l'utente edotto e consapevole che è stato profilato e che quel contenuto è il risultato di una certa profilazione. Bisogna considerare che la trasparenza non è una questione puramente bilaterale. Non c'è solo il decisore algoritmico che nasconde informazioni per difendere un proprio interesse e il soggetto profilato che reagisce per tutelare a propria volta un altro interesse personale. Nella profilazione e, in generale, nell'utilizzo dei dati personali per scopi politici, entrano in gioco gli altri interessi di carattere generale che abbiamo su esposto (spec. §§ 3 e 4) e che costituiscono un'ulteriore ragione per incentivare richieste di maggior trasparenza[28].

[27] Per un approfondimento sul sovvertimento della dimensione di comunicazione nei *social* e le sue ricadute sulla disinformazione, v. C. CAPASSO, *"Algo-sicurezza" terrorismo, contesto digitale e dinamiche costituzionali*, Editoriale Scientifica, Napoli, 2025, spec. pp. 222 ss.

[28] In proposito esistono interessanti esempi di natura comparata, come alcune diret-

Una terza linea è quella di ridurre o in certi casi vietare del tutto l'utilizzabilità della profilazione in campo politico, al di là delle ipotesi che riguardano la formale pubblicità politico-elettorale che già trovano regolazione nella cornice normativa europea. In particolare, il legislatore europeo ha disposto nel DSA (Regolamento UE n. 2022/2065) e, soprattutto, nel Regolamento sulla pubblicità politica (Regolamento UE n. 2024/900, in vigore dall'ottobre 2025) vari obblighi lungo la filiera della pubblicità politica (tra cui vi sono regole di trasparenza e di identificabilità dei finanziatori), motivandoli esplicitamente con il rischio di manipolazione e interferenze esterne nel sistema democratico europeo. Ad oggi le piattaforme hanno preferito non misurarsi con il Regolamento, non permettendo l'utilizzo del servizio a chi ne fa richiesta.

Ma per la guerra cognitiva, il punto non è la pubblicità politica in sé, bensì la (dis)informazione politica in quanto tale che gode della combinazione di *targeting* individualizzato, di forti criteri inferenziali (valoriali, emotivi e, talvolta, persino psicografici), dell'opacità dei parametri di selezione e, infine, della c.d. "scalabilità", cioè della possibilità di diffonderla su grandissima scala e rapidamente.

Resta dunque il problema della sua regolazione, atteso che il Regolamento UE n. 2024/900 non si applica né a opinioni espresse a titolo personale né ai contenuti editoriali e pertanto non regola il contenuto degli annunci.

Ci si può legittimamente domandare se, letto attraverso le categorie del diritto costituzionale, esso non assuma i tratti di un problema giuridicamente rilevante. Al contrario, personalmente mi pare che vietare o restringere fortemente il *micro-targeting* politico individuale su contenuti politici, consentendo invece forme di *targeting* "ampio" (contestuale o per macro-aree che non dipendono dall'inferenza con il profilo dell'utente), risponda anzi proprio ad una *ratio* costituzionale chiara, legittima e in astratto prevalente sugli altri interessi oggetti di bilanciamento, quella di preservare il mercato delle idee da plurime e non verificabili fonti di

tive del Tribunale Superiore Elettorale (TSE) brasiliano da cui sembra derivare, da una prospettiva democratica e di corretto svolgimento delle elezioni, il principio secondo cui il divieto di manipolazione debba essere ormai considerato un dovere fondamentale connesso allo sfruttamento dei dati personali in ambito politico-elettorale. C'è ovviamente da capire quali sono i limiti tra influenza legittima e manipolazione. Cfr. TSE, *Resolución n. 23.610/*2019. Per la dottrina, A. GARRIGUES WALKER, L.M. GONZÁLEZ DE LA GARZA, *El derecho a no ser engañado. Y cómo nos engañan y nos autoengañamos*, Aranzadi, Pamplona, 2020, spec. pp. 153 ss.

informazione che possono minacciare la sicurezza dello Stato e i diritti dell'individuo.

Una terza direttrice, di tutela "a monte", forse la più incisiva, è la teorizzazione di un diritto generale e, in certi casi, non opponibile e dunque assoluto a non essere profilati. Tale potestà deve naturalmente soggiacere al presentarsi di determinate condizioni. Si potrebbe, ad esempio, distinguere tra profilazione del profilo e profilazione della personalità (laddove ci siano dati che rappresentano il nucleo della propria identità e, dunque, idonei alla sua estrinsecazione) e, per ciascuna situazione, pensare ad una forza di resistenza diversificata, in particolare laddove essa sfrutti situazioni di vulnerabilità (minori) o opacità (una finalità non dichiarata). Si potrebbe altrimenti distinguere non a partire dalla situazione soggettiva dell'utente/interessato, quanto della finalità oggettiva del servizio di profilazione offerto dalla piattaforma/titolare (o co-titolare) del trattamento. Quando la profilazione è finalizzata al *micro-targeting* per ottenere o destinare informazione politica, allora è necessario uno statuto rafforzato fino al divieto[29].

La pensabilità di una tale norma prescrittiva non si àncora solo ai divieti e agli obblighi dell'art. 22 GDPR, né solo a quegli *ex* artt. 5 e 5 *AI Act*, ma anche al dovere previsto dall'art. 38 DSA di offrire un'opzione di raccomandazione di contenuto alternativa non basata su profilazione. Se queste norme e la loro *ratio* non sono destinate a rimanere una facoltà meramente nominale dell'utente-cittadino, allora l'opzione di permettere una non-profilazione *by default* non può essere accantonata, dal momento che la trasparenza, da sola, non neutralizza la logica della persuasione micro-targettizzata algoritmica.

[29] In questa prospettiva, il punto non è proclamare un nuovo diritto in senso retorico, bensì qualificare come diritto una situazione favorevole già ricavabile, per argomentazione, da principi e frammenti normativi: compito tipico della dottrina e della giurisprudenza è individuare la posizione protetta, i correlativi obblighi di sfavore e il livello di garanzia. Il diritto a non essere profilati si colloca allora nello *status libertatis* e, più precisamente, nella libertà "in entrata": non soltanto libertà di decidere cosa rivelare, ma libertà di formarsi senza essere esposti a un condizionamento personalizzato, opaco e cumulativo, idoneo a reificare la persona riducendola a bersaglio di tecniche di influenza. È quanto ho già più ampiamente sostenuto in A. Gatti, *Profilazione e diritti fondamentali*, cit., spec. pp. 351 ss.

DALLA DIPLOMAZIA DEI GABINETTI ALLA GUERRA COGNITIVA: DIRITTO INTERNAZIONALE, OPINIONE PUBBLICA E TRASFORMAZIONE DEL CONFLITTO

Eliana Augusti[*]

1. *Agli albori di un diritto "nuovo": guerra, pace e* ius commercii

La costruzione del diritto internazionale moderno trovò nel secondo Ottocento un momento di consolidamento decisivo[1]: la relativa stabilizzazione degli equilibri europei aveva reso possibile una più nitida definizione delle relazioni tra soggetti che si riconoscevano reciprocamente come eguali e indipendenti. Il diritto delle genti, rielaborando e in parte oltrepassando la lezione groziana dello *ius belli ac pacis*[2], si presentava ora come un diritto interstatale rinforzato, fondato sulla «coscienza giuridica comune» radicata nei paradigmi dell'europeità e della cristianità[3], e so-

[*] Professoressa in Storia del diritto medievale e moderno nell'Università del Salento.

[1] Per una ricostruzione rinvio a L. NUZZO, *Origini di una scienza. Diritto internazionale e colonialismo nel XIX secolo*, Klostermann, Frankfurt am Main, 2012; G. GOZZI, *Diritti e civiltà. Storia e filosofia del diritto internazionale*, il Mulino, Bologna, 2010; G. FORMIGONI, *Storia della politica internazionale nell'età contemporanea*, Il Mulino, Bologna, 2006; A. OSIANDER, *The State System of Europe 1640-1990. Peacemaking and the Conditions of International Stability*, Oxford University Press, Oxford, 1994. Centrale resta M. KOSKENNIEMI, *The Gentle Civilizer of Nations: The Rise and Fall of International Law 1870-1960*, Cambridge University Press, Cambridge, 2002.

[2] H. GROTIUS, *De iure belli ac pacis* (1625), Liberty Fund, Indianapolis, 2005.

[3] A proposito della "coscienza giuridica comune", mi sia permesso di rinviare a E. AUGUSTI, *Questioni d'Oriente. Europa e Impero Ottomano nel Diritto Internazionale dell'Ottocento*, Edizioni Scientifiche Italiane, Napoli, 2013, p. 95 ss. La dottrina ottocentesca operò nello spazio scientifico dell'*Institut de droit international*. Costituito per iniziativa del belga Gustave Rolin-Jaequemyns l'8 settembre del 1873 a Gand, l'*Institut* ebbe tra i suoi obiettivi quello di favorire il progresso del diritto internazionale, formulare

stenuto da una dottrina che, nel richiamarsi ad un non meglio precisato «standard di civiltà», individuava intanto nello Stato-nazione non solo la forma compiuta dell'organizzazione politica, ma anche il criterio implicito di accesso alla comunità internazionale[4].

In questo orizzonte, pace e guerra vennero progressivamente ricondotte entro una medesima architettura normativa. La pace cessò di coincidere con la mera assenza di ostilità, configurandosi piuttosto come effetto di un ordine giuridico in via di organizzazione, intrecciato alle dinamiche del commercio e alle prime forme di cooperazione internazionale. Essa non si presentava, dunque, come valore assoluto: la sua tenuta dipendeva da un equilibrio variabile tra interessi e principi di sicurezza, libertà e giustizia che il diritto era chiamato a comporre senza poterli stabilizzare definitivamente. La guerra, senza essere eliminata, veniva progressivamente inscritta entro forme riconoscibili: abbandonata la giustificazione confessionale a un orizzonte premoderno, andò consolidandosi come *guerre en forme*, anche grazie all'elaborazione dottrinale e ai primi tentativi di codificazione[5]: una guerra dichiarata, dunque, regolata e inscritta entro procedure che ne garantivano la qualificazione giuridica[6]. La distinzione tra uso legittimo della forza ed esercizio arbitrario della violenza prese forma attraverso la progressiva articolazione dello *ius ad bellum* e

i principi generali della scienza e perseguire la consacrazione ufficiale di quelli condivisi. Vedi su questo ancora L. NUZZO, *Origini di una scienza*, cit., pp. 137-153; KOSKENNIEMI, *The Gentle Civilizer of Nations*, cit., p. 39 ss.; ora anche V. GENIN, *Le laboratoire belge du droit international. Une communauté épistémique et internationale de juristes (1869-1914)*, Académie Royale de Belgique, Bruxelles, 2018.

[4] Il riferimento implicito alla nazione come "monade" del diritto internazionale è a Pasquale Stanislao Mancini. Vedi sul punto ancora L. NUZZO, *Da Mazzini a Mancini: il principio di nazionalità tra politica e diritto*, in *Giornale di Storia Costituzionale*, 2007, p. 174.

[5] Si pensi al *Lieber Code*: F. LIEBER, *Instructions for the Government of Armies of the United States in the Field* (General Orders No. 100, Adjutant General's Office, 1863), U.S. Government Printing Office, Washington, 1898. Vedi S. MANNONI, *Potenza e ragione. La scienza del diritto internazionale nella crisi dell'equilibrio europeo (1870-1914)*, Giuffrè, Milano, 1999, pp. 149 ss.

[6] Cf. E. DE VATTEL, *Le droit des gens ou principes de la loi naturelle appliqués à la conduite et aux affaires des nations et des souverains* (1758), J.P. Aillaud, Paris, 1835. Vedi W. RECH, *Enemies of Mankind. Vattel's Theory of Collective Security*, Martinus Nijhoff Publishers, Leiden, 2013. Per una breve ricostruzione su diritto e guerra fino all'età contemporanea, vedi A.A. CASSI, *Diritto e guerra nell'esperienza giuridica europea tra medioevo ed età contemporanea*, in A. SCIUMÈ (a cura di), *Il diritto come forza. La forza del diritto. Le fonti in azione nel diritto europeo tra medioevo ed età contemporanea*, Giappichelli, Torino, 2012, pp. 7-32.

dello *ius in bello*, cui si affiancò, almeno *in nuce*, una riflessione sulla fase successiva al conflitto. La guerra, per quanto *extrema ratio*, veniva così ricondotta entro l'ordine giuridico, regolata nei suoi presupposti, nelle sue modalità e nei suoi effetti: il diritto che aspirava a limitarla ne riconosceva al tempo stesso la persistente funzionalità. Così era, almeno, nello spazio euro-americano[7], *inter christianos*, dove l'eguaglianza formale tra Stati consentiva di applicare con relativa coerenza le categorie emergenti; al di fuori di questo perimetro, la qualificazione giuridica dell'uso della forza si faceva invece più incerta e selettiva. Nei confronti degli Stati e dei territori collocati ai margini della *communitas* internazionale, la guerra continuava a manifestarsi attraverso pratiche che sfuggivano alle forme codificate, combinandosi con dispositivi di intervento, influenza, espansione e controllo, non di rado giustificati attraverso la degradazione giuridica di spazi e sovranità, ricondotti alla logica della disponibilità (*res nullius*). In tali contesti, la distinzione tra uso legittimo e arbitrario della forza risultava di fatto rimodulata, attenuata perfino, adattandosi alle esigenze di proiezione esterna delle potenze europee. In questo scarto tra universalizzazione dichiarata e applicazione differenziata si radicò una delle tensioni strutturali del diritto internazionale ottocentesco, destinata a riemergere, sotto forme diverse, nelle configurazioni successive.

Sullo sfondo di questa costruzione si mantenne, tuttavia, un principio dalle genealogie antiche, destinato a ridefinire le condizioni di possibilità dell'ordine stesso: lo *ius commercii*, declinazione moderna dello *ius communicationis*[8]. Già nel sedicesimo secolo, con Francisco de Vitoria, il diritto di comunicare, viaggiare e commerciare si era presentato come espressione originaria della socialità umana, fondato sulla possibilità di stabilire relazioni tra comunità politiche diverse, al netto dell'opera evangelizzatrice. Ugo Grozio ne aveva offerto una formulazione più sistematica: nel *Mare liberum*, il commercio era stato assunto come principio fondamentale del diritto delle genti, a partire dall'idea che nessun popolo potesse essere escluso dal rapporto con gli altri. La circolazione di uomini, beni e risorse non costituiva soltanto un fatto economico, ma

[7] Cf. C. Schmitt, *Il nomos della terra nel diritto internazionale dello «jus publicum europaeum»* (1974), Adelphi, Milano, 1991.

[8] Cf. L. Lacchè (a cura di), *«Ius gentium ius communicationis ius belli». Alberico Gentili e gli orizzonti della modernità. Atti del Convegno di Macerata in occasione delle celebrazioni del quarto centenario della morte di Alberico Gentili (1552-1608), Macerata, 6-7 Dicembre 2007*, Giuffrè, Milano, 2009. Rispetto al rapporto tra *ius communicationis* e *ius commercii* rinvio a E. Augusti, *Migrare come abitare. Una storia del diritto internazionale in Europa tra XVI e XIX secolo*, Giappichelli, Torino, 2022, p. 27 ss.

una condizione strutturale di equilibrio tra scarsità e abbondanza, tra differenze e interdipendenze[9]. Questa linea di pensiero trovò una rielaborazione decisiva alla fine del Settecento, quando il diritto di entrare in relazione con altri popoli venne qualificato in termini più rigorosamente giuridici. I diritti kantiani di visita e di ospitalità[10], intesi come facoltà di presentarsi e di non essere trattati ostilmente in territorio straniero, non si fondavano su un dovere di accoglienza illimitata, ma su un principio minimo di accesso reciproco, necessario alla possibilità stessa di rapporti tra comunità. Il venire in contatto effettivo tra i popoli non rispondeva a un'esigenza filantropica o morale, ma a una condizione giuridica della convivenza internazionale: una pretesa limitata, ma esigibile, che rendeva possibile la comunicazione e lo scambio, contribuendo alla stabilizzazione delle relazioni. In questo senso, il commercio poteva ben configurarsi come dispositivo capace di ridurre il ricorso alla guerra, offrendo una via alternativa alla regolazione dei rapporti internazionali: non tanto come semplice fattore di interdipendenza economica, quanto come espressione di un principio giuridico di relazione, entro il quale il conflitto, pur non escluso, veniva progressivamente ricondotto a forme di interazione più stabili. Eppure, proprio in questa promessa si annidava una tensione strutturale. Il principio che sul piano teorico si presentava come apertura universale operò, nella prassi, come uno dei principali vettori dell'espansione europea. Lo *ius commercii* non sostituì la guerra, ma ne accompagnò la metamorfosi: giustificò l'accesso forzato ai mercati, sostenne l'imposizione di regimi giuridici differenziati, contribuì alla costruzione di legalità asimmetriche, fuori e dentro lo spazio euro-americano[11]. In questo assetto anche la pace cambiava forma, assumendo sempre più chiaramente quella di una tregua, da rinegoziare di volta in volta, a seconda degli equilibri (e degli interessi) in gioco.

2. *Universalismo, diseguaglianza e "*organized hypocrisy*"*

Di fronte alle trasformazioni indotte dall'espansione dei traffici, il diritto non poteva tuttavia sottrarsi a una funzione di adeguamento. I «nuovi bisogni della civiltà moderna», osservava Pasquale Fiore nel 1865,

[9] U. GROZIO, *Mare liberum* (1609), Liguori, Napoli, 2007, p. 109.

[10] Mi sia permesso rinviare ancora a E. AUGUSTI, *Migrare come abitare*, cit., p. 15 ss.

[11] Vedi ancora attuali le riflessioni di D. ZOLO, *Chi dice umanità. Guerra, diritto e ordine globale*, Einaudi, Torino, 2000.

avrebbero dovuto trovare risposta tanto nel diritto quanto nel commercio internazionale[12]. Partendo dall'assunto per cui la "coscienza giuridica comune", confinata com'era entro i limiti del *nomos* europeo, non fosse più sufficiente a sostenere un'auspicabile universalizzazione del diritto internazionale[13], Fiore tentava un'apertura ottimistica, coerente con i bisogni del suo tempo: meglio sarebbe stato, a suo avviso, ragionare in termini di "comunanza", non come dato acquisito dunque per storia o valori condivisi, ma come processo graduale di adesione alla società delle nazioni. In questa prospettiva, l'eguaglianza tra gli Stati non costituiva un punto di partenza, ma un obiettivo eventuale, destinato a maturare nel tempo. Tale impostazione prendeva atto di una realtà che il diritto non poteva più ignorare. Le profonde disomogeneità tra i soggetti della comunità internazionale, lungi dal rimanere sullo sfondo, vennero progressivamente tematizzate e sistematizzate.

Se nella riflessione settecentesca, basti pensare al dibattito sulla disuguaglianza tra gli uomini, tali differenze erano ancora oggetto di una critica rivolta alle forme storiche dell'organizzazione sociale e politica, nell'Ottocento esse vennero sempre più reinterpretate come dati strutturali, suscettibili di classificazione e gerarchizzazione. Un sapere etnologico in rapida espansione, la cosiddetta "scienza delle razze", da Lewis Morgan ad Arthur de Gobineau, contribuì a fissare tali differenze entro schemi apparentemente oggettivi, trovando ampia circolazione anche negli ambienti giuridici attraverso le elaborazioni di James Lorimer e Joseph Hornung, su tutti[14]. In questo passaggio, la diseguaglianza cessava di

[12] P. Fiore, *Nuovo diritto internazionale pubblico secondo i bisogni della civiltà moderna*, Casa Editrice e Tipografia degli Autori-Editori, Milano, 1865, p. 58 ss.

[13] Mi sia permesso rinviare sul punto a E. Augusti, *Modernità, «First Global Competition» e Diritto internazionale universale tra Sette e Ottocento*, in A. Sciumé, A.A. Cassi, E. Fusar Poli (a cura di), *History&Law Encounters,* Giappichelli, Torino, 2021, pp. 77-93.

[14] M.J. Lorimer, *The Institutes of the Law of Nations*, William Blackwood and Sons, Edinburgh and London, 1883, I, p. 101 «No modern contribution to science seems destined to influence international politics and jurisprudence to so great an extent as that which is known as ethnology or the sciences of races», p. 93; Id., *La doctrine de la reconnaissance, fondement du droit international,* in *Revue de droit international et de législation comparée*, 1884, p. 335. Lorimer aveva teorizzato un'articolazione dell'umanità, precedente al fenomeno politico, rappresentabile per cerchi concentrici: in ordine decrescente si trovavano l'umanità civilizzata, l'umanità barbara e quella selvaggia. A connotare questi tre aspetti dell'umanità contribuivano senz'altro il fattore razza e quello, affine, del grado di sviluppo all'interno della stessa razza. Secondo Lorimer il grado di civiltà di un popolo, poiché collegato all'appartenenza ad una razza anziché ad un'altra, non pote-

essere problema da spiegare per diventare presupposto da assumere, incrinando la *fictio* di un'eguaglianza originaria su cui il diritto interstatale aveva costruito la propria grammatica formale. D'altro canto, un diritto internazionale limitato ai soli Stati "cristiani e civili" d'Europa e d'America, come ancora aveva sostenuto Henri Wheaton nel 1836[15], risultava ormai incompatibile con l'estensione globale delle relazioni economiche e politiche[16]. L'universalizzazione del diritto appariva necessaria, ma non poteva che realizzarsi entro condizioni differenti e differenziate.

La soluzione indicata da Fiore si collocava precisamente in questo scarto. La progressiva estensione del diritto internazionale sarebbe avvenuta attraverso la diffusione della scienza, della civiltà e, soprattutto, del commercio, capaci di favorire, progressivamente, l'adesione a un linguaggio giuridico condiviso, quella "comunanza" a cui alludeva. Il diritto positivo dei trattati avrebbe costituito il luogo di questa mediazione: uno spazio nel quale soggetti ancora diseguali avrebbero potuto entrare in relazione, riconoscendosi entro un quadro comune, pur senza eliminare immediatamente le differenze[17]. In questa costruzione *in divenire*, la pace, ancora una volta, non si configurava come un dato, ma come il risultato di un processo di integrazione progressiva, nel quale il diritto operava insieme come argine, come strumento di regolazione e come vettore di trasformazione. Un'apertura, dunque, che non eliminava le asimmetrie, le riorganizzava.

L'accesso al diritto dei trattati e, con esso, alla comunità internazionale, risultava però di fatto condizionato all'avvio di processi di adegua-

va essere affatto trascurato ai fini di una partecipazione alla società internazionale. Vedi anche J. HORNUNG, *Civilisés et Barbares*, in *Revue de droit international et de législation comparé*e, 1885, pp. 1-18, 447-470, 539-560; 1886, pp. 188-206, 280-298.

[15] «The International law of the [civilized,] Christian nations of Europe and America, is one thing; what which governs the intercourse of the Mohammedan nations of the East with each other, and with Christian, is another and a very different thing», così H. WHEATON, *Elements of International Law with a sketch of the History of the Science*, Lea&Blanchard, Philadelphia, 1836, p. 45. Il ragionamento di Wheaton era la sintesi della dottrina del suo tempo: vedi T. VON SCHMALZ, *Das europäische Völker-Recht*, Dunker&Humblot, Berlin (1817), Keip, Frankfurt am Main, 1970; J.L. KLÜBER, *Droit des gens moderne de l'Europe*, Libraire de J.G. Cotta, Paris, 1819; fino a P. PRADIER-FODÉRÉ, *Traité de droit international public Européen & Américain suivant les progrès de la science et de la pratique contemporaines*, A. Durand et Pedone-Lauriel éditeurs, Paris, 1885.

[16] J. OSTHERAMMEL, N.P. PETERSSON, *Storia della globalizzazione*, il Mulino, Bologna 2005, pp. 193-228, qualificano questa fase come «first global competition» .

[17] Cf. D. KENNEDY, *International Law and the Nineteenth Century: History of an Illusion*, in *Nordic Journal of International Law*, 1996, pp. 385-420.

mento agli *standard* europei[18]. Nei contesti non occidentali[19], l'adozione di modelli giuridici e istituzionali d'importazione, promossa da *élite* locali e sostenuta dall'azione di funzionari e consulenti occidentali, divenne il presupposto del riconoscimento internazionale. Dalle riforme delle *Tanzimât* nell'Impero ottomano al Siam post-Bowring, dalla Persia del *Dâr ol-Fonun* alla Cina del *Self-Strengthening Movement*, fino al Giappone della Restaurazione Meiji[20], tali processi risposero a una logica che Thomas Naff avrebbe efficacemente sintetizzato nella formula del *to change or to perish*[21]: non imitazione passiva, ma strategia di sopravvivenza in un sistema strutturalmente diseguale.

In questo quadro, la distinzione tra Stati "civili" e "non-civili", che ancora alla fine dell'Ottocento Antoine Pillet sistematizzava nella scala evolutiva proposta da Lorimer, fornì la giustificazione teorica di una partecipazione differenziata all'ordine internazionale e alla risoluzione dei conflitti che da quella sarebbero derivati[22]. L'eguaglianza formale veniva così preservata sul piano dei principi, mentre sul piano delle pratiche si affermavano dispositivi di direzione, controllo e amministrazione che ne riducevano l'effettività. La sovranità non era negata, ma riorganizzata[23]:

[18] A. Rapisardi-Mirabelli, *Storia dei trattati e delle relazioni internazionali*, Istituto per gli Studi di Politica Internazionale, Milano, 1940, p. 188 ss.

[19] In particolare, A.W. Heffter, *Le droit international de l'Europe*, Cotillon et fils, Paris, 1873, p. 38, distingueva, nell'ordine storico universale, tra Stati orientali e Stati europei: «l'état oriental est celui de la résignation et du servage, dans le quel le despotisme ou l'oligocratie s'est alliée à la hiérarchie».

[20] Cf. S. Horowitz, *International Law and State. Transformation in China, Siam, and the Ottoman Empire during the Nineteenth Century*, in *Journal of World History*, 2004, pp. 445-486; T. Kayaoğlu, *Legal Imperialism: Sovereignty and Extraterritoriality in Japan, the Ottoman Empire, and China*, Cambridge University Press, Cambridge, 2010. Vedi anche B. Bowden, *The Empire of Civilization: The Evolution of an Imperial Idea,* The University of Chicago Press, Chicago, 2009. Per una lettura critica dei *legal transplant* mi sia concesso rinviare a E. Augusti, *Un diritto possibile. Storie, teorie e prassi di modernità tra comparazione e globalizzazione*, in *Forum Historiae Iuris*, 23.06.2016, pp. 1-37. Cf. anche F. Rugge, *Il «contesto intransigente». Appunti sulla storia di un postulato*, in Id. (a cura di), *Il trasferimento internazionale dei modelli istituzionali*, il Mulino, Bologna, 2012, p. 89.

[21] T. Naff, *The Ottoman Empire and the European States System*, in H. Bull, A. Watson (a cura di), *The Expansion of International Society*, Oxford University Press, Oxford, 1984, p. 160.

[22] A. Pillet, *Le Droit International Public. Ses éléments constitutifs, son domaine, on objet*, in *Revue Général de Droit International Public*, 1894, p. 24.

[23] Così anche Kayaoğlu, *Legal Imperialism*, cit., pp. 17 ss.; diffusamente, G. Simpson, *Great Powers and Outlaw States: Unequal Sovereigns in the International Legal Order*, Cambridge University Press, Cambridge, 2004; A. Anghie, *Finding the Peripheries: Sover-*

riconosciuta nella forma, veniva rimodulata nella sostanza secondo gradi e condizioni variabili. Il modello westphaliano, fondato sull'autonomia e sulla non ingerenza, continuava a operare in modo relativamente coerente entro lo spazio europeo-americano, ma risultava selettivamente sospeso nei confronti degli Stati non-europei[24]. Da questa tensione tra universalismo dichiarato e applicazione differenziata emersero configurazioni ibride, nelle quali la sovranità si presentava come incompleta o condizionata, fino a cristallizzarsi in categorie intermedie, come quella, emblematica, della "semi-sovranità", che rendevano "giuridicamente pensabile" una gerarchia altrimenti difficilmente ammissibile[25].

In questa divaricazione si manifestò un tratto strutturale dell'ordine internazionale moderno, successivamente colto dalla riflessione contem-

eignty and Colonialism in Nineteenth-Century International Law, in *Harvard International Law Journal*, 1999, pp. 1-71.

[24] S.D. KRASNER, *Westphalia and All That*, in J. GOLDSTEIN, R.O. KEOHANE (a cura di), *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change*, Cornell University Press, Ithaca, 1993, pp. 235-264. La sospensione del modello corrispondeva al confinamento dell'esperienza giuridica degli Stati orientali a un tempo sospeso della storia. La «negazione della contemporaneità» (la *coevalness*) era la traduzione di questa nuova grammatica: grazie a un semplice scarto temporale tra Occidente e non-Occidente, territori e popolazioni dei cosiddetti «nuovi mondi» furono dislocati in un altro tempo ed «esp[ulsi] dai territori della storiografia occidentale, [...] semplicisticamente liquidati come stagnanti o senza storia» (vedi L. NUZZO, *Autonomia e diritto internazionale. Una lettura storico-giuridica*, in *Quaderni fiorentini*, 2014, p. 656. Il resto del mondo era il luogo del "non ancora" (*not yet*) ingiunto da qualcuno a qualcun altro, del non essere ancora abbastanza civilizzato per autogovernarsi. Prima della sfida per l'autonomia sarebbe trascorso un intervallo storico necessario di sviluppo e civilizzazione (o, per essere precisi, di dominio ed educazione, coloniali). John Stuart Mill (J.S. MILL, *Saggio sulla libertà* (1859), Mondadori, Milano, 1981) qualificò queste nazioni fuori dal tempo e dallo spazio come "rozze", confinandole in un'immaginaria sala d'aspetto della storia: «il colonizzatore raccomandava a[i] colonizzat[i] di aspettare [lì] il momento giusto». Avanziamo tutti verso la medesima destinazione, sosteneva Mill, ma alcuni popoli arriveranno prima degli altri (vedi sul punto D. CHAKRABARTY, *Provincializzare l'Europa*, Meltemi, Roma, 2004, pp. 22-23). Il mondo altro, come la colonia, divenne uno «spazio in ritardo», uno spazio sospeso, uno spazio molteplice che legittimava valutazioni e legislazioni differenti, anche e soprattutto di un altro tempo, a seconda della sua diversa natura (ancora L. NUZZO, *La colonia come eccezione. Un'ipotesi di transfer*, in *Rechtsgeschichte*, 2006, p. 3). E per l'Europa il tempo del "non ancora" era il tempo del premoderno. Cf. anche J. FABIAN, *Time and the Other: How Anthropology Makes its Object*, Columbira University Press, New York, 1983; per un'analisi più articolata rinvio sul punto a E. AUGUSTI, *Modernità, «First Global Competition» e Diritto internazionale universale*, cit., p. 87 ss..

[25] A.G. HEFFTER, *Le droit international de l'Europe*, cit., p. 40.

poranea nella nozione di *organized hypocrisy*[26]: la distanza tra principi dichiarati e pratiche effettive non costituiva un'anomalia contingente, ma un elemento costitutivo del sistema. In essa si annidava il "lato oscuro" del diritto internazionale[27]: un diritto che, mentre prometteva reciprocità, organizzava la diseguaglianza; che, mentre si proponeva di limitare la guerra, ne redistribuiva le forme, proiettandole oltre il momento dell'ostilità e inscrivendole nella costruzione stessa dell'ordine.

3. Diplomazia e giurisdizione consolare: governare la differenza

Mentre l'ordine internazionale ottocentesco si costruiva attraverso dispositivi giuridici capaci di organizzare l'asimmetria senza dichiararla, le prassi diplomatiche sostanziavano la piena operatività di tale logica. La diplomazia moderna, lungi dal limitarsi a riflettere un assetto già dato, nonostante i tentativi di arginamento attuati dalla scienza del diritto internazionale, si "rifunzionalizzava" su un doppio binario che, paradossalmente, ne amplificava la portata. Da un lato, essa consolidava la propria dimensione classica di legazione: il diritto di inviare e ricevere rappresentanti continuava a segnare la soglia dell'appartenenza alla società internazionale, inscrivendosi nel paradigma dell'eguaglianza sovrana che, proprio nella formula diplomatica, trovava la sua espressione più visibile e ritualizzata. Non è un caso che, in questa stes-

[26] Già S.D. Krasner, *Westphalia and All That*, cit., p. 235: «The basic organizing principle of sovereignty – exclusive control over a given territory – has been persistently challenged by the creation of new institutional forms that better meet specific material needs»; quindi, Id., *Sovereignty: Organized Hypocrisy*, Princeton University Press, Princeton, 1999, p. 69.

[27] Cf. L. Nuzzo, *Origini di una scienza*, cit., pp. 223-286. La riflessione più recente sul "dark side" del diritto internazionale converge nel mettere in luce come esso non operi stabilmente quale limite al potere, ma come campo intrinsecamente ambivalente in cui norme e principi risultano strutturalmente indeterminati e permeabili agli interessi statali, storicamente intrecciati a pratiche di dominio e gerarchizzazione globale e segnati da una persistente matrice eurocentrica che solo più di recente è stata oggetto di critica e rielaborazione in chiave pluralistica (vedi in particolare Y. Onuma, *When was the Law of International Society Born? An Inquiry of the History of International Law from an Intercivilizational Perspective*, in *Journal of the History of International Law*, 2000, pp. 54-66), mentre il linguaggio giuridico, lungi dal neutralizzare il conflitto, continua a costituirne una delle principali modalità di espressione e legittimazione, rivelando così una tensione costitutiva tra aspirazione universalistica e funzione politica che ne delimita ancora oggi i confini operativi.

sa fase, la riflessione giuridica, da Carl von Martens alla manualistica ottocentesca italiana, insistesse sulla necessità di una professionalizzazione dell'ufficio diplomatico, concepito non più come luogo speciale di mera intermediazione politica, ma come sapere tecnico capace di operare all'interno di un linguaggio giuridico sempre più complesso, strutturato e condiviso[28].

Accanto a questa dimensione formale, tuttavia, si sviluppò una seconda funzione, che si esercitava negli interstizi dell'ordine e ne rivelava la natura selettiva: fu sul terreno della giurisdizione consolare che l'ambivalenza della diplomazia (e del diritto internazionale) si fece manifesta. Nei contesti non-europei, e in particolare negli Stati cosiddetti "orientali", nel solco dei processi di ammodernamento istituzionale già citati, avanzati su modello occidentale, si andarono a consolidare, in continuità con le esperienze commerciali medievali, le pratiche capitolari, grazie alle quali si confermavano tutte le prerogative dei consoli *in loco*. Il console, in Oriente, non si limitava a "rappresentare": egli esercitava poteri giurisdizionali, amministrativi e di protezione sui cittadini europei (e ora anche americani), andando così a incidere direttamente sulla configurazione della sovranità e sulla giurisdizione territoriale[29]. Attraverso il sistema delle capitolazioni prima e dei cosiddetti *unequal treaties* poi[30],

[28] C. VON MARTENS, *Le guide diplomatique. Précis des droits et des fonctions des agents diplomatiques et consulaires suivi d'un Trait. des Actes et Offices divers qui sont du ressort de la Diplomatie, accompagné de pièces et documents proposés comme exemples*, F.A. Brockhaus, Leipzig, 1866, III, pp. 6-7. Per F.P. CONTUZZI, *Del nuovo indirizzo scientifico e pratico del diritto internazionale: prolusione al corso d'insegnamento pronunziata nella R. Università di Macerata nel d. 13 novembre 1881*, Stabilimento Tipografico A. Perrotti, Napoli, 1882, p. 14, «Il diritto internazionale della Restaurazione nasceva dagli sforzi della diplomazia e ad essa era destinato». Rinvio su questo a E. AUGUSTI, *Crimea 1853-1856. La guerra attesa e la costruzione di un nuovo ordine mediterraneo*, in L. BRUNORI, C. CIANCIO, E.C. TAVILLA (a cura di), *Italia-Francia Allers-Retours: Luttes et revendications – Lotte e rivendicazioni* in *Historia et Ius, Collana di Studi di Storia del diritto medievale e moderno*, 2025, Collettanee, p. 122.

[29] Mi sia concesso rinviare a E. AUGUSTI, *La giurisdizione consolare in Oriente: dal primato genovese alla sparizione. Spunti per una riflessione*, in V. LAVENIA (a cura di), *Alberico e Scipione Gentili nell'Europa di ieri e di oggi. Reti di relazioni e cultura politica*, in *Atti della Giornata Gentiliana in occasione del IV centenario della morte di Scipione Gentili (1563-1616). San Ginesio, 16-17 settembre 2016*, Edizioni Università di Macerata, Macerata, 2018, pp. 153-189.

[30] M. CRAVEN, *What Happened to Unequal Treaties? The Continuities of Informal Empire*, in *Nordic Journal of International Law*, 2005, p. 380; rinvio anche a E. AUGUSTI, *From Capitulations to Unequal Treaties: The Matter of an Extraterritorial Jurisdiction in the Ottoman Empire*, in *Journal of Civil Law Studies*, 2011, pp. 285-307.

in applicazione del principio della personalità del diritto[31], intere porzioni di "spazio" giuridico venivano sottratte alla giurisdizione locale dei sovrani orientali e sottoposte a regimi normativi esterni. Il principio di territorialità non veniva formalmente negato, ma sospeso eccezionalmente nella sua operatività concreta.

La storiografia più recente ha mostrato come tale dispositivo non potesse essere ridotto a un'anomalia marginale, ma dovesse essere piuttosto compreso come parte integrante dell'ordine internazionale ottocentesco[32]. Il diritto consolare si collocava infatti in una zona intermedia, una *grey zone* tra diritto internazionale e diritto coloniale, configurandosi come uno spazio di interferenza (e influenza) nel quale la distinzione tra interno ed esterno, tra sovranità e subordinazione, risultava sistematicamente rinegoziabile[33]. Formalmente giustificato dalla necessità di garantire sicurezza e commercio, esso operava come strumento di penetrazione giuridica e controllo, rendendo possibile una presenza che era al tempo stesso normativa e politica. La diplomazia occupava questo punto di tensione. Essa continuava a rappresentare l'eguaglianza tra gli Stati, ma al tempo stesso ne organizzava la limitazione, rendendo praticabile una gerarchia che non veniva mai esplicitamente tematizzata dal diritto e che, nella sua indeterminatezza, prolungava ad un tempo incerto il raggiungimento dello "standard di civiltà" e, dunque, il superamento dell'eccezione e il pieno riconoscimento *inter pares*.

4. *Opinione pubblica, cooperazione e riconfigurazione del conflitto*

È sullo sfondo delle asimmetrie che avevano segnato l'ordine internazionale ottocentesco e che avevano collocato una parte rilevante degli Stati non-europei in una posizione intermedia, tra la promessa di un riconoscimento formale e la minaccia di un degradamento alla condizione precedente, che si colloca una trasformazione destinata a incidere ulte-

[31] Cf. N. Süsa, *The Historical Interpretation of the Origin of the Capitulations in the Ottoman Empire*, Hopkins Press, Baltimore, 1930.

[32] L. Nuzzo, *Origini di una scienza*, cit., p. 169 ss.; per un'analisi più aperta e dettagliata rinvio a E. Augusti, *Storie e storiografie dei Consolati in Oriente tra Otto e Novecento*, in *Historia et ius*, 2017, pp. 1-17.

[33] Per F. Ferrara, *Manuale di diritto consolare*, Cedam, Padova, 1936, p. 16, «queste Capitolazioni nella loro sostanza contenevano delle vere abdicazioni alla sovranità territoriale, in favore degli Stati stranieri, in quanto si riconosceva ad essi il potere di giurisdizione entro il loro territorio». Vedi L. Nuzzo, *Origini di una scienza*, cit., p. 169 ss.

riormente sulla struttura stessa del diritto internazionale. Il passaggio alla cooperazione non determinò il superamento di tali diseguaglianze, né realizzò quella piena integrazione che la retorica dell'ammodernamento poteva lasciare intravedere; esso ne implicò piuttosto una riorganizzazione entro forme nuove, nelle quali la partecipazione al sistema restava condizionata e graduata.

A partire dalla seconda metà del secolo, alcuni interessi fino ad allora qualificati come strettamente nazionali vennero progressivamente riformulati come interessi comuni, suscettibili di essere trattati come "generali". Tale slittamento non comportò l'abbandono delle logiche di potenza, già stabilizzate nella *primacy* del concerto europeo[34], ma ne accompagnò un riassetto operativo: cooperazione, intervento e protezione (*garentia*), soprattutto nella loro declinazione collettiva, si affermarono come strumenti ordinari di gestione dell'ordine, offrendo al tempo stesso nuove modalità di inclusione e criteri rinnovati di differenziazione tra gli Stati. L'accesso alla cooperazione si configurò sempre più come esito di un processo, piuttosto che come presupposto, subordinato all'adeguamento a *standard* giuridici e istituzionali definiti nello spazio euro-americano. Anche in questo contesto, il contributo dell'*Institut de Droit International,* fondato a Gand nel 1873, svolse una funzione di particolare rilievo. L'Istituto non si limitò a riflettere le trasformazioni in atto, ma contribuì a organizzarle sul piano concettuale, promuovendo un diritto internazionale inteso come disciplina scientifica autonoma, capace di sottrarsi almeno in parte alle contingenze dell'azione diplomatica. Attraverso la produzione di risoluzioni, progetti di codificazione e prese di posizione su questioni quali, in particolare, la neutralità, l'arbitrato, il controllo degli stranieri o le emergenze sanitarie, esso favorì la costruzione di un lessico condiviso e il progressivo orientamento della dottrina verso una "de-nazionalizzazione" di ambiti tematici fino ad allora trattati in chiave esclusivamente statuale. In tal modo, contribuì a rendere praticabile una forma di cooperazione che pur inscritta, come dicevamo, entro rapporti di forza persistenti, si presentava come spazio di coordinamento stabile tra ordinamenti giuridici differenti, in cui anche interessi materiali, non ultimi quelli commerciali, trovavano una mediazione più strutturata. Questo sviluppo si radicò in un cambio di passo di ampia portata: l'intensificazione dei traffici, lo sviluppo delle infrastrutture, la crescente interdipendenza economica e l'emergere di questioni che eccedevano la dimensione bilaterale del confronto, portarono anche la diplomazia ad

[34] Rinvio sul punto a E. AUGUSTI, *Questioni d'Oriente*, cit., p. 200 ss.

assumere una funzione rinnovata di cerniera, questa volta tra equilibrio e cooperazione. Le pratiche multilaterali, dalle conferenze sanitarie internazionali ai regimi sulla navigazione, fino alle Conferenze dell'Aia, Parigi e Berlino[35], si intensificarono senza d'altronde alterare gli assetti della "prima competizione globale". È all'interno di questa configurazione che si produsse un ulteriore spostamento, destinato a incidere sulle stesse condizioni di legittimazione dell'azione internazionale.

L'ordine delineato, già filtrato dai lavori dell'*Institut* e dalla nascente dottrina giusinternazionalistica, non poteva più essere governato, giocoforza, entro i circuiti ristretti delle cancellerie, ma si andava progressivamente esponendo a uno spazio discorsivo più ampio, nel quale la stabilità delle decisioni dipendeva non soltanto dalla loro correttezza formale, ma anche dalla loro intelligibilità e dalla loro capacità di essere sostenute pubblicamente. In questo slittamento, che affondava le sue radici in forme precoci di comunicazione intellettuale transnazionale[36] e che la riflessione successiva avrebbe ricondotto alla formazione di una sfera pubblica come ambito intermedio tra Stato e società[37], la crescita della stampa, la diffusione dei quotidiani e la circolazione delle idee contribuirono alla formazione di uno spazio nel quale le decisioni internazionali venivano progressivamente esposte, discusse e rielaborate. Tale sfera non si limitava a riflettere le scelte politiche, ma interveniva nella loro costruzione, ridefinendo il rapporto tra decisione, diritto e consenso. In questa funzione di mediazione tra sapere e potere, il diritto internazionale venne progressivamente tradotto in un linguaggio più accessibile, reso disponibile a forme più ampie di circolazione e mobilitazione. Un ruolo decisivo fu svolto dalla stampa periodica e quotidiana: riviste come la *Revue des Deux Mondes* (1829), la *Revue de droit international et de législation comparée* (1869) e, in ambito italiano, *Il Filangieri* (1876), accanto a organi a forte proiezione politico-istituzionale come *Le Moniteur Universel* (1789) e a quotidiani a larga diffusione quali *The Times* (1785), *Le Figaro* (1826) o la *Neue Freie Presse* (1864), contribuirono a rendere visibili le dinami-

[35] Per una riflessione più articolata sul ruolo delle Conferenze internazionali, rinvio a E. Augusti, *'Frontiere aperte' e assistenza agli stranieri: il ruolo delle Conferenze internazionali in Europa tra Otto e Novecento* in M.S. Testuzza, E. De Cristofaro (a cura di), *TEMPI DIFFICILI. Crisi e trasformazioni otto novecentesche tra storia e diritto*, Collana "Storie del diritto", Bonanno Editore, Acireale, 2023, pp. 49-70.

[36] Il riferimento è alla cosiddetta "repubblica delle lettere". Vedi lo studio di M. Fumaroli, *La repubblica delle lettere*, Adelphi, Milano, 2018.

[37] Cf. J. Habermas, *Storia e critica dell'opinione pubblica* (1962), Laterza, Roma-Bari, 2001.

che internazionali, ampliandone il pubblico e incidendo sulle modalità di percezione delle relazioni e dei conflitti. Parallelamente, associazioni e movimenti pacifisti, dalla *London Peace Society* (1816) ai congressi degli "Amici della pace" tra il 1848 e il 1851, fino all'*Inter-Parliamentary Union* (1889) e all'*International Peace Bureau* (1891), contribuirono a strutturare un'opinione pubblica sensibile ai temi della guerra e della pace, introducendo forme di pressione che, pur non traducendosi in vincoli giuridici immediati, incidevano concretamente sul contesto decisionale[38].

Il punto decisivo non fu soltanto l'emergere di un controllo esterno sull'azione dei governi, ma la trasformazione delle condizioni entro cui tale azione veniva concepita: la guerra, la pace, l'intervento e la mediazione cessarono di essere categorie interamente governabili entro il solo lessico diplomatico e giuridico, risultando sempre più esposte a processi di mobilitazione, identificazione e partecipazione collettiva. In tale contesto, la guerra non venne espunta dall'ordine giuridico, ma sottoposta a una crescente esigenza di giustificazione. Alle forme codificate della *guerre en forme* si affiancarono registri ulteriori, dominati dal linguaggio della necessità, della tutela, dell'equilibrio, della responsabilità, attraverso cui l'uso della forza venne reso compatibile con un orizzonte di legittimità più ampio. L'istituto dell'intervento si collocò precisamente in questo spazio: non come eccezione esterna all'ordine, ma come pratica interna ad esso, capace di attenuare la discontinuità tra legalità e forza[39]. La formula *on behalf of* rese visibile tale spostamento, orientando la legittimazione verso la tutela di interessi qualificati, presentati come condivisi o superiori. Il diritto internazionale non si limitò così a qualificare l'azione, ma contribuì a strutturarne le condizioni di intelligibilità.

Il conflitto cambiava registro, continuando a operare sul piano dei rapporti di forza, ma sempre più anche su quello della rappresentazione e della costruzione del consenso. Il coinvolgimento delle *élite*, dei ceti borghesi e, progressivamente, delle masse non si tradusse soltanto in una ricezione

[38] Cf. C. PANATTONI, *Considerazioni sul diritto della pace e della guerra, sopra i Congressi degli Amici della pace, tenuti in Francoforte ed in Londra*, Firenze, 1851. Per una ricostruzione più dettagliata, rinvio a E. AUGUSTI, *Questioni d'Oriente*, cit., pp. 283-288.

[39] Cf. G. ROLIN-JAEQUEMYNS, *Note sur la théorie du droit d'intervention, a propos d'une lettre de M. le professeur Arntz*, in *Revue de droit international et de législation comparée*, 1876, p. 673. Per un'analisi e una ricostruzione della storiografia sull'istituto dell'intervento, mi sia concesso rinviare a E. AUGUSTI, *L'intervento europeo in Oriente nel XIX secolo: storia contesa di un istituto controverso*, in L. NUZZO, M. VEC (a cura di), *Constructing International Law. The Birth of a Discipline*, Vittorio Klostermann, Frankfurt am Main, 2012, pp. 277-330.

passiva delle decisioni, ma incise sui processi stessi di formazione della volontà politica. Le mobilitazioni collettive, i movimenti nazionali e le spinte insurrezionali si inscrissero in questo quadro, contribuendo a trasformare guerra e pace in oggetti di investimento simbolico e di partecipazione diffusa. Non si trattava soltanto di una più ampia esposizione del conflitto allo sguardo pubblico, ma di una modificazione delle condizioni stesse entro cui esso veniva pensato, sostenuto e rappresentato. Proprio in questo passaggio si colse un effetto ulteriore. La mobilitazione non investiva soltanto l'azione politica, ma anche le forme della comunità cui essa veniva riferita. Le appartenenze collettive, i linguaggi della nazione e le pratiche di partecipazione contribuirono a dare consistenza a quadri statuali e territoriali sempre più presentati come unità coerenti[40], benché sorretti da processi di attivazione, selezione e produzione simbolica. L'universalizzazione del diritto internazionale non si dispiegò, dunque, su un terreno neutro: si accompagnò alla progressiva naturalizzazione di tali quadri, assumendoli come presupposti dell'ordine proprio mentre essi si andavano storicamente costruendo. La guerra, intanto, cessava di apparire soltanto come evento giuridicamente qualificabile o diplomaticamente gestibile, divenendo un fenomeno la cui efficacia dipendeva anche dalla capacità di mobilitare percezioni, orientare il consenso e produrre adesione. Il piano dell'azione si intrecciava così stabilmente con quello della sua costruzione pubblica.

5. Tecnologie, disumanizzazione e guerra cognitiva

La trasformazione appena delineata, nella quale il conflitto si intreccia stabilmente con la sua costruzione pubblica e con i processi di mobilitazione e consenso, trova una prima formulazione critica nella riflessione contemporanea sulle "ragioni della guerra". In questa prospettiva, è stato osservato come il ricorso a categorie apparentemente universali-

[40] Rinvio a E. Augusti, *Ripensare la nazione ottocentesca. Vecchi e nuovi paradigmi tra storia, diritto e globalità*, in M. Meccarelli (a cura di), *Reading the crisis. Legal, Philosophical and Literary Perspectives*, Editorial Dykinson, Madrid, 2017, pp. 65-97; Id., *Verso la nazione. Un itinerario concettuale tra Sette e Ottocento*, in F. Lamberti, M.L. Tacelli, U. Villani Lubelli (a cura di), *Diritto, storia, istituzioni.* Liber amicorum *Giancarlo Vallone*, Collana del Dipartimento di Scienze Giuridiche, tomo II, Edizioni Scientifiche Italiane, Napoli, 2024, pp. 109-138. Cf. S. Halperin, *Imperial city states, National States and Post-National Spatialities*, in S. Halperin, R. Palan (a cura di), *Legacies of Empire. Imperial Roots of the Contemporary Global Order*, Cambridge University Press, Cambridge, 2015.

stiche come "umanità", "intervento", "sicurezza", non si fosse limitato (e tutt'ora non si limiti) a qualificare l'azione, ma avesse operato come dispositivo di legittimazione capace di dissimulare la persistenza di interessi strategici e materiali. La guerra tendeva così a presentarsi come razionale, selettiva, "intelligente": non più soltanto scontro tra eserciti, ma strumento flessibile di governo dei rapporti internazionali. Questa riconfigurazione rende visibile oggi un ulteriore passaggio. La guerra non si limita più a essere giustificata attraverso il diritto, né è resa accettabile nello spazio dell'opinione pubblica, ma viene progressivamente progettata per operare all'interno di tali spazi, incidendo sulle loro condizioni di formazione.

Alla fine del secolo scorso, Danilo Zolo mostrava come le strategie di destabilizzazione, l'induzione di situazioni di instabilità nei contesti politicamente più esposti, l'attacco indiretto alle democrazie liberali e alle loro forme di legittimazione, così come la competizione per il controllo di snodi strategici e "corridoi" di transito, avessero fatto del conflitto una pratica integrata, nella quale dimensione militare, diplomatica, economica e politica risultassero inseparabili. Il controllo delle risorse e delle infrastrutture torna oggi a collocarsi al centro della dinamica conflittuale, mentre il diritto continua a operare come linguaggio di traduzione e di giustificazione. Le categorie elaborate in ambito strategico quali *hybrid warfare*, *grey zone operations*, *multi-domain operations*, *information warfare*[41], per citarne alcune, registrano sul piano operativo questa trasformazione, evidenziando come il conflitto si sviluppi ormai simultaneamente su livelli differenti, non ultimi quello informativo e cognitivo[42]. La distinzione tra guerra e non-guerra tende così a sfumare, lasciando emergere una condizione di conflittualità "diffusa", collocata al di sotto delle soglie

[41] Le categorie elaborate in ambito strategico, dalla nozione di *hybrid warfare*, sistematizzata da F.G. HOFFMAN, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, 2007, alle più recenti dottrine di *multi-domain operations* sviluppate in ambito NATO e statunitense, registrano la progressiva integrazione tra dimensione militare, economica e informativa del conflitto, evidenziando come esso si sviluppi ormai su piani simultanei e interdipendenti. Vedi anche M.J. MAZARR, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, US Army War College Press, Carlisle Barracks, 2015.

[42] Cf. E. CALCAGNO, *Taking Multi-domain Operations from Theory to Practice*, in *Documenti IAI,* 2026, pp. 1-29; P. DOBIAS, K. CHRISTENSEN, *The 'Grey Zone' and Hybrid Activities*, in *Connections: The Quarterly Journal*, 2022, pp. 41-54; vedi ora A. STERPA, *La difesa della democrazia dalle minacce ibride. Teorie della comunità, dell'autorità, del potere e migrazioni: elementi per un'analisi strategica della "guerra tiepida"*, Editoriale Scientifica, Napoli, 2025.

tradizionali della dichiarazione formale. In tale configurazione, ancora una volta, la guerra non scompare, ma si distribuisce, si diluisce, si rende meno riconoscibile. È in questo contesto che la dimensione cognitiva assume un rilievo centrale.

Il conflitto non si gioca più soltanto sul terreno dell'azione, sul campo, ma su quello della percezione, della narrazione e della costruzione del consenso. La produzione di senso diventa parte integrante della condotta delle ostilità: incidere sulle modalità con cui un evento è percepito, interpretato e condiviso significa intervenire direttamente sulle condizioni della decisione politica. La guerra non si limita a utilizzare la comunicazione, ma la incorpora come proprio ambiente operativo. L'impatto delle tecnologie digitali e la globalizzazione dei circuiti informativi intensificano ulteriormente tale processo. Non si tratta di strumenti esterni, ma di fattori che incidono sulle condizioni stesse di possibilità del conflitto. La diffusione capillare dei dispositivi di informazione e condivisione produce una forma di "simultaneità cognitiva" che altera il rapporto tra individuo, comunità e ordine giuridico. Ciò che accade diviene immediatamente visibile, ma non per questo più intelligibile: la sovraesposizione informativa frammenta la percezione, rendendo difficile la costruzione di un senso unitario degli eventi. Ne deriva quella «parcellizzazione delle opinioni – ha scritto Alessandro Sterpa – con un crescente ruolo dell'esegesi, individuale ma solitaria»[43], che finisce paradossalmente per produrre la de-responsabilizzazione dello stesso soggetto connesso, il quale "segue" per "restare informato", senza che a tale esposizione corrisponda una effettiva capacità di comprensione o di presa sul reale. L'esposizione continua ai flussi informativi non incide dunque soltanto sulle modalità della percezione, ma contribuisce a ridefinire le forme stesse della soggettività giuridica: accanto ai criteri classici di appartenenza, si delinea un livello ulteriore, qui proposto, in termini problematici, come *ius digitalis*[44], nel quale l'individuo si colloca all'interno di circuiti glo-

[43] A Sterpa, *La difesa della democrazia dalle minacce ibride*, cit., p. 39.

[44] L'espressione *ius digitalis* è qui impiegata non per designare un ambito del diritto positivo relativo alle tecnologie, bensì in senso teorico, quale categoria interpretativa volta a cogliere una modalità emergente di soggettivazione giuridica connessa all'esposizione degli individui a circuiti globali di informazione, comparazione e riconoscimento mediati digitalmente. In tale prospettiva, essa non si configura come alternativa ai criteri classici di appartenenza (*ius sanguinis*, *ius soli*, *ius religionis*), ma come livello ulteriore che si affianca ad essi, incidendo sulle forme di percezione e di legittimazione del diritto in contesti globalizzati. Pur trovando riscontri indiretti nelle riflessioni contemporanee sulla trasformazione della normatività e della soggettività nelle società digitali (E. Fourneret, B.

bali di informazione, comparazione e riconoscimento che ne orientano aspettative, giudizi e forme di partecipazione. È anche attraverso questo livello che si ristrutturano le condizioni di legittimazione del conflitto, sempre più dipendenti dalla gestione della percezione e dalla costruzione del consenso.

Il passaggio successivo è rappresentato, dunque, dalla "disumanizzazione" del conflitto, non soltanto come effetto della distanza fisica, già evidente nelle tecnologie militari, ma come conseguenza di una più profonda trasformazione delle condizioni della percezione. La sofferenza diviene accessibile senza essere necessariamente condivisa; l'esposizione non implica partecipazione; la prossimità informativa non si traduce in prossimità morale. Già la riflessione moderna aveva colto questo scarto tra visibilità e coinvolgimento, tra conoscenza dell'evento e assunzione di responsabilità: uno scarto che la contemporaneità tende ad amplificare. La responsabilità, in tale contesto, si disperde lungo catene decisionali e rappresentative sempre più complesse, ma anche lungo pratiche diffuse di fruizione che trasformano l'osservazione in surrogato dell'azione, rendendo possibile una partecipazione a distanza che non incide sulle condizioni effettive del conflitto[45]. La guerra, resa "intelligente", dicevamo, per l'investimento di risorse cognitive, competenze specialistiche, ricerche tecnologiche e informatiche, oltre che per le complesse e raffinate elaborazioni strategiche[46], e mediata, tende a sottrarsi alla sua dimensione immediatamente esperibile, senza per questo perdere la propria capacità distruttiva. In questo, il diritto internazionale si trova a operare entro uno spazio profondamente mutato. Se il conflitto si dispiega come competizione per il controllo delle risorse, delle infrastrutture e delle percezioni, e se la legittimazione precede e condiziona l'azione, la

YVERT, *Digital Normativity: A Challenge for Human Subjectivation*, in *Frontiers in Artificial Intelligence*, 2020, pp. 1-27; J.E. COHEN, *Between Truth and Power*, Oxford University Press, Oxford, 2019; M. HILDEBRANDT, *Smart Technologies and the End(s) of Law*, Edward Elgar Publishing, Cheltenham, 2015, la nozione qui proposta non intende introdurre un nuovo istituto, ma offrire una chiave di lettura coerente con le genealogie della soggettività giuridica ricostruite dalla storiografia del diritto internazionale, alla luce della crescente rilevanza della dimensione cognitiva nei processi di legittimazione del conflitto.

[45] Il riferimento è in particolare alle riflessioni di A. SMITH, *The Theory of Moral Sentiments*, Andrew Millar in the Strand, London, 1761. Per H. ARENDT, *Sulla rivoluzione* (1965), Edizioni di comunità, Milano, 1996, pp. 79-85: «La politica della pietà [ ] mobilita i sentimenti di un pubblico di spettatori», inducendolo a sostituire all'azione diretta forme di intervento a distanza, quali il parlare o il contribuire economicamente, senza incidere sulle condizioni effettive dell'azione politica.

[46] D. ZOLO, *Chi dice umanità*, cit., p. 41.

funzione del diritto non può più essere pensata esclusivamente in termini di regolazione dell'uso della forza. Essa è chiamata a confrontarsi con un contesto nel quale il confine tra norma, decisione e narrazione tende a farsi incerto, e nel quale la guerra continua a trasformarsi senza mai uscire dall'orizzonte giuridico che pretende di contenerla.

6. *Conclusioni*

Se osservato in prospettiva storica, il percorso qui ricostruito non segnala tanto una trasformazione lineare della guerra, quanto la persistenza di un problema che attraversa l'intera modernità giuridica internazionale. Fin dalle sue prime sistemazioni, il diritto delle genti si è misurato con l'esigenza di rendere compatibile l'uso della forza con un ordine che intendeva disciplinarlo, senza tuttavia poterlo espungere dal proprio orizzonte. Nel secondo Ottocento questa esigenza trovò una formulazione particolarmente articolata. La definizione della *guerre en forme*, l'elaborazione delle categorie dello *ius ad bellum* e dello *ius in bello*, insieme allo sviluppo delle pratiche cooperative, contribuirono a stabilizzare un assetto nel quale il conflitto risultava al tempo stesso ammesso e regolato. Ma lo stesso movimento che ne affinava la forma ne rendeva più incerta la delimitazione. L'apertura della comunità internazionale, attraverso trattati, commercio e processi di adattamento istituzionale, ampliò lo spazio delle relazioni, moltiplicando le occasioni di contatto e, con esse, le linee di frizione. La circolazione, già posta a fondamento dello *ius commercii*, operò così come principio ambivalente: fattore di integrazione e, insieme, generatore di tensioni, anche in relazione al controllo delle risorse e delle direttrici strategiche lungo le quali essa si dispiegava. La diplomazia, in questo, continuò a svolgere una funzione di cerniera tra diritto e potere, ma entro condizioni mutate. L'emersione di uno spazio pubblico più ampio, alimentato dalla stampa e dalle prime forme di mobilitazione collettiva, non sottrasse il conflitto alla decisione statale, ma ne modificò le condizioni di legittimazione, esponendolo progressivamente a processi di discussione e rappresentazione che eccedevano lo spazio delle cancellerie.

Alcuni tratti del quadro contemporaneo appaiono, in questa prospettiva, meno come cesure che come riorganizzazioni di lungo periodo. La difficoltà di ricondurre il conflitto a una dichiarazione formale, la sua articolazione su piani molteplici e la crescente opacità delle catene decisionali ripropongono problemi già emersi nella costruzione dell'ordine internazionale ottocentesco. La nozione di "guerra tiepida", proposta dalla

recente dottrina in termini descrittivi, consente di leggere una condizione nella quale la violenza, lungi dallo scomparire, si riorganizza all'interno dello stesso spazio normativo che ne disciplina e, al tempo stesso, rende possibile l'esercizio. Tale configurazione si colloca in continuità con le trasformazioni già evidenziate: la guerra, resa "intelligente" dall'integrazione tra dimensione militare, economica, informativa e cognitiva, tende a operare al di sotto delle soglie tradizionali della dichiarazione formale, incidendo sulle condizioni della decisione politica prima ancora che sul piano dell'azione. Il diritto internazionale, in questo quadro, non si limita a qualificare l'uso della forza, ma contribuisce a organizzarne l'intelligibilità, inscrivendolo entro un orizzonte di accettabilità che si costruisce anche sul terreno della percezione e del consenso. Le tecnologie e i circuiti informativi globali non introducono una frattura, ma intensificano dinamiche già presenti. La dimensione cognitiva del conflitto, la sua produzione di senso, la costruzione del consenso, la gestione della sua percezione, si integrano sempre più strettamente con quella operativa, fino a incidere sulle stesse condizioni di intelligibilità dell'azione. La circolazione delle informazioni, la dis-informazione e le possibilità aperte dall'intelligenza artificiale contribuiscono a configurare un ambiente nel quale la rappresentazione non si limita a riflettere il conflitto, ma ne diviene parte costitutiva. Non è privo di rilievo che il conflitto venga oggi ricondotto a forme ibride, nelle quali strumenti militari, diplomatici, economici e comunicativi si combinano, rendendo meno netta la distinzione tra guerra e gestione strategica delle relazioni. La diplomazia, intanto, non si limita a prevenire o a chiudere il conflitto, ma ne accompagna lo svolgimento, articolandosi lungo registri che includono la comunicazione pubblica e forme di interazione mediate.

Il diritto internazionale continua così a operare in uno spazio instabile. Da un lato, fornisce criteri di qualificazione e, almeno in parte, di contenimento dell'uso della forza; dall'altro, contribuisce a renderne intelligibili le condizioni di esercizio, inscrivendolo entro un orizzonte di accettabilità storicamente determinato. Il rischio, già percepibile nelle esperienze ottocentesche, è che la distanza tra limite e legittimazione si riduca fino a diventare difficilmente distinguibile, soprattutto quando il linguaggio del diritto accompagna dinamiche che trovano altrove le proprie ragioni materiali e strategiche[47]. Il ricorso alla storia consente

[47] Cf. D. GRIMM, *Die Zukunft der Verfassung II. Auswirkungen von Europäisierung und Globalisierung*, Suhrkamp Verlag, Frankfurt am Main, 2012, pp. 219-226; T. GRECO, *Pace. Critica della ragione bellica*, Laterza, Roma-Bari, 2024, pp. 15-38.

di sottrarre il fenomeno della guerra tanto a letture contingenti quanto a interpretazioni teleologiche. Le crisi non segnano necessariamente regressioni, né garantiscono sviluppi progressivi: appartengono a processi più ampi, la cui direzione non può essere presupposta[48]. La questione del limite, centrale nella costruzione moderna dell'ordine internazionale, riemerge così come problema aperto: non un dato acquisito, ma un'esigenza da rinnovare, entro un quadro nel quale il diritto è chiamato a confrontarsi con forme della forza che tendono a eccedere i dispositivi predisposti per contenerle[49].

La guerra non può essere assunta come esito necessario né come dispositivo fisiologico delle relazioni internazionali. Se la storia del diritto internazionale ne mostra la persistente presenza entro l'ordine giuridico, evidenzia al tempo stesso il carattere problematico, e mai definitivamente risolto, del tentativo di ricondurla entro forme di giustificazione e contenimento. In questa tensione, che la riflessione contemporanea ha ricondotto anche ai processi di legittimazione simbolica del conflitto[50], si colloca la postura critica che il diritto è chiamato a mantenere.

Le trasformazioni più recenti non si esauriscono in adattamenti tecnici, ma impongono un rinnovato sforzo di qualificazione. Le formule che emergono nel discorso pubblico, dalla cosiddetta *war diplomacy* alle più elusive pratiche di *social diplomacy*, veicolate e amplificate dai circuiti mediatici e digitali, segnalano una ridefinizione dei confini tra conflitto, comunicazione e relazione internazionale. Non si tratta soltanto di nuove modalità operative, ma di un ambito nel quale la distinzione tra uso della forza, gestione della crisi e costruzione del consenso tende a farsi meno nitida. Il problema non è più soltanto stabilire quando e come la guerra possa dirsi giuridicamente qualificabile, ma verificare se le categorie tradizionali del diritto internazionale siano ancora in grado di restituire senso a pratiche che si collocano ai loro margini o che ne sfruttano consapevolmente le ambiguità. È su questo terreno che si misura oggi la responsabilità del giurista: non nel registrare le trasformazioni in atto, né nel fornirne un linguaggio di mera giustificazione, ma nel mantenere uno spazio critico capace di interrogare le condizioni di legittimità dell'azione internazionale. Da questo punto di vista, il riferimento all'*Institut de Droit International* conserva un valore che va oltre il contesto della sua fondazione: indica la possibilità di uno spazio di riflessione scientifica

[48] J. Huizinga, *La crisi della civiltà*, Einaudi, Torino, 1972, pp. 45-60.
[49] M. Cacciari, *Il potere che frena*, Adelphi, Milano, 2013, pp. 23-35; 87-102.
[50] F. Fornari, *Psicoanalisi della guerra*, Feltrinelli, Milano, 1966, pp. 21-45.

che, pur confrontandosi con la realtà, non si esaurisca nella sua immediata traduzione normativa. In un ordine attraversato da forme di conflittualità diffuse, ibride e difficilmente qualificabili, il compito del diritto non consiste nell'assorbirle, ma nel renderne visibili i limiti, contribuendo a ridefinire le condizioni entro le quali la forza possa ancora essere sottoposta a giudizio.

LA SICUREZZA NAZIONALE NELLA REPUBBLICA FEDERALE TEDESCA: STRATEGIE DI DIFESA E TENUTA ISTITUZIONALE

Ubaldo Villani Lubelli[*]

1. *La ridefinizione della sicurezza tedesca tra fine della potenza civile e nuove vulnerabilità sistemiche*

La Repubblica Federale Tedesca (RFT) è nata e si è consolidata istituzionalmente su un preciso imperativo categorico: il ripudio strutturale del militarismo e l'ancoraggio irrevocabile all'architettura multilaterale occidentale. Fin dalla sua fondazione nel 1949, il sistema politico tedesco ha tradotto il trauma della Seconda guerra mondiale e della Shoah in una complessa impalcatura costituzionale e culturale. La Legge Fondamentale (*Grundgesetz*) è stata concepita non solo per impedire derive autoritarie interne attraverso meccanismi di democrazia protetta (*streitbare Demokratie*)[1], ma anche per limitare fortemente la proiezione di potenza

[*] Professore in Storia delle istituzioni politiche nell'Università del Salento.

[1] Cfr. K. LOEWENSTEIN, *Militant Democracy and Fundamental Rights*, I, in *American Political Science Association*, 1937, pp. 422-423; S. CECCANTI, *Le democrazie protette e semi-protette da eccezione a regola. Prima e dopo le Twin Towers*, Giappichelli, Torino, 2004; A. DI GIOVINE, *Democrazie protette e protezione della democrazia*, Giappichelli, Torino, 2005; W. LOEWER, *Wehrhafte Demokratie*, in: C. HILLGRUBER, C. WALDHOFF (a cura di), *60 Jahre Bonner Grundgesetz*, Bonn University Press, 2010, pp. 65-86; U. SCHLIESKY, *Die wehrhafte Demokratie des Grundgesetzes*, in J. ISENSEE, P. KIRCHHOF (a cura di) *Handbuch des Staatsrechts*, Bd. XII, C.F. Müller, Heidelberg, 2014, pp. 841-862, in part. 854; S. TYULKINA, *Militant Democracy. Undemocratic Political Parties and Beyond*, Routledge, Londra, 2015; M. THIEL, *The "Militant Democracy" Principle in Modern Democracies*, Ashgate Pub., Farnham, 2016; A. MALKOPOUPOU, L. NORMAN, *Three Models*

dello Stato verso l'esterno. Da questa cornice è scaturito il paradigma della Germania come potenza civile (*Zivilmacht*): uno Stato che ha delegato gran parte della propria sicurezza territoriale all'ombrello della NATO e degli Stati Uniti, affidando la propria strategia di stabilizzazione geopolitica all'interdipendenza economica, culminata storicamente nella *Ostpolitik* inaugurata da Willy Brandt e, più recentemente, nel principio del *Wandel durch Handel* (cambiamento attraverso il commercio) nei confronti della Federazione Russa e in parte anche della Cina.

Un altro pilastro della tenuta istituzionale e democratica tedesca dal dopoguerra a oggi è rappresentato da un fondamento immateriale di natura pre-politica: la *Erinnerungskultur* (la cultura della memoria). La rielaborazione pubblica delle colpe storiche ha costituito un collante identitario della Repubblica Federale. Questo consenso sul passato ha generato quel patriottismo costituzionale (*Verfassungspatriotismus*)[2] che ha permesso a una nazione divisa, e poi riunificata, di riconoscersi in un complesso set di valori democratici condivisi, ponendo una barriera istituzionale invalicabile contro il ritorno del nazionalismo radicale.

La combinazione di questi profili ha garantito decenni di stabilità, anche se è progressivamente andata incontro a un parziale sfaldamento. L'invasione russa dell'Ucraina nel febbraio 2022 ha agito da detonatore di contraddizioni già latenti, costringendo Berlino a una brutale e repentina presa di coscienza. Il discorso sulla *Zeitenwende* (cambiamento d'epoca), pronunciato dal Cancelliere Olaf Scholz al Bundestag il 27 febbraio 2022, ha segnato formalmente la fine dell'illusione post-storica tedesca. Dal punto di vista istituzionale, questa cesura si è tradotta nell'urgente necessità di ripensare l'intero apparato difensivo, concretizzatasi inizialmente nello stanziamento di un fondo speciale (*Sondervermögen*)

of Democratic Self-Defence: Militant Democracy and Its Alternatives, in *Political Studies*, 2018, 442-458; R. TARCHI, *Democrazia e istituzioni di garanzia*, in *RivistaAic*, 3/2018, pp. 994-995; E. CATERINA, *La metamorfosi della "democrazia militante" in Germania. Appunti sulla sentenza NPD del Tribunale costituzionale federale e sulla successiva revisione dell'art. 21 della Legge fondamentale*, in *Diritto Pubblico Comparato ed Europeo*, 1/2018, pp. 239-258; M. FUHRMANN, *Antiextremismus und wehrhafte Demokratie. Kritik am politischen Selbstverständnis der Bundesrepublik Deutschland*, 2019; M. CALAMO, SPECCHIA, *Un prisma costituzionale, la protezione della Costituzione: dalla democrazia "militante" all'autodifesa costituzionale*, in *Diritto Pubblico Comparato ed Europeo*, 1/2021, pp. 92-129; A. GATTI, *Liberal Democracies and Religious Extremism. Rethin- king Militant Democracy through the German Constitutional Experience*, in *Diritto Pubblico Comparato ed Europeo*, 1/2021, pp. 131-152.

[2] La letteratura sul tema è molto estesa, cito qui solo J.-W. MUELLER, *Verfassungspatriottismus*, Suhrkamp Verlag, Berlino, 2024.

di cento miliardi di euro per il riequipaggiamento della *Bundeswehr*, le cui capacità operative erano state drasticamente ridotte nei decenni successivi alla fine della Guerra Fredda.

Eppure, limitare l'analisi della crisi di sicurezza tedesca alla sola dimensione militare e convenzionale risulterebbe fuorviante. La pubblicazione nel giugno 2023 della prima Strategia di Sicurezza Nazionale (*Nationale Sicherheitsstrategie*)[3] nella storia della RFT dimostra come le istituzioni tedesche abbiano dovuto adottare il concetto di sicurezza integrata. Le democrazie occidentali, e la Germania in modo particolare, si trovano oggi ad affrontare minacce asimmetriche che sfuggono alle tradizionali categorie della deterrenza militare. Lo scenario odierno è dominato da una conflittualità ibrida, all'interno della quale potenze straniere ostili, *in primis* la Federazione Russa, operano al di sotto della soglia del conflitto armato convenzionale. Questo si traduce in attacchi cibernetici contro infrastrutture critiche, sorveglianza fisica e disturbo tramite droni su siti sensibili, e, soprattutto, in massicce operazioni di disinformazione e guerra cognitiva.

È esattamente in questa faglia, nel punto di intersezione tra la minaccia esogena e la debolezza endogena, si inserisce il caso di studio della Germania odierna e che risulta paradigmatico per comprendere la più ampia crisi delle democrazie occidentali perché evidenzia come l'efficacia di un attacco ibrido esterno sia direttamente proporzionale al grado di frammentazione del tessuto sociale e politico interno. L'offensiva cognitiva e infrastrutturale trova, infatti, un terreno straordinariamente fertile in un Paese che sta vivendo una profonda erosione del proprio mito fondativo: la dissoluzione della memoria storica condivisa.

L'infrastruttura culturale su cui si è retta la Repubblica Federale mostra segni di cedimento sistemico. Il progressivo allontanamento temporale dagli eventi del Novecento, unito alle tensioni derivanti dai processi di globalizzazione e alle recenti crisi sistemiche, ha generato un vuoto identitario in cui si sono inserite nuove forze politiche di rottura. L'ascesa del partito di destra radicale *Alternative für Deutschland* (AfD) rappresenta il sintomo istituzionale e politico maggiormente dirompente di questa crisi. La strategia di AfD non si limita alla capitalizzazione del dissenso socio-economico o alla feroce strumentalizzazione della crisi migratoria esplosa nel 2015, ma si spinge fino al cuore del consenso repubblicano: la richiesta di una revisione radicale della storia tedesca. Il tentativo di

[3] Il testo della Strategia nazionale è disponibile sul sito *www.nationalesicherheitsstrategie.de*

relativizzare le responsabilità storiche relative alla Prima e alla Seconda guerra mondiale, così come il recente dibattito sul colonialismo in Africa, non costituiscono mere provocazioni intellettuali, ma precise operazioni politiche volte a scardinare il fondamento valoriale dello Stato federale.

In questo quadro di inedita complessità, la sicurezza nazionale smette di coincidere esclusivamente con la difesa dei confini territoriali, sovrapponendosi drammaticamente al concetto di tenuta istituzionale. La convergenza oggettiva tra l'azione destabilizzante di attori statuali esterni e il revisionismo politico interno crea una morsa che minaccia la resilienza della democrazia tedesca.

2. *Il nuovo fronte: guerra ibrida e vulnerabilità infrastrutturale nella Repubblica Federale*

Il mutamento del paradigma di sicurezza nazionale tedesco, innescato dalla *Zeitenwende*, non si esaurisce nella ridefinizione degli organici e delle dotazioni della *Bundeswehr* né nella mera quantificazione del riarmo convenzionale. La Germania si trova oggi a dover fronteggiare una forma di conflittualità che sfugge alle categorie tradizionali della deterrenza militare e si colloca stabilmente al di sotto della soglia del conflitto armato classico. Se durante la Guerra fredda la minaccia esistenziale appariva tangibile, geograficamente localizzata e militarmente definita – si pensi al *Fulda Gap* come ipotetico asse di penetrazione sovietica nel cuore della RFT –, l'odierna architettura della sicurezza deve misurarsi con un avversario dai contorni fluidi, capace di combinare strumenti cinetici e non cinetici in una strategia di logoramento di lunga durata.

La Federazione Russa rappresenta, in questo quadro, l'attore che più chiaramente ha sviluppato una dottrina del conflitto ibrido, vale a dire una forma di ostilità asimmetrica e multidominio che integra pressione energetica, attacchi cibernetici, sabotaggio, operazioni informative e interferenza politica. L'obiettivo non consiste necessariamente nel provocare un confronto militare aperto, bensì nel rallentare la capacità decisionale dello Stato bersaglio, amplificarne le vulnerabilità sistemiche e logorarne progressivamente la coesione democratica. Proprio per questo, la scelta di operare in una persistente zona grigia, al di sotto della soglia di attivazione dei meccanismi classici della deterrenza collettiva, costituisce un tratto strutturale della minaccia e non un suo elemento accessorio.

Per comprendere la specifica esposizione della Repubblica Federale, è opportuno scomporre la minaccia lungo tre assi di vulnerabilità tra loro

strettamente interdipendenti: la dimensione fisica e del sabotaggio delle infrastrutture critiche; il dominio cibernetico; lo spazio cognitivo-informazionale. In ciascuno di questi ambiti, gli sviluppi degli ultimi anni hanno mostrato quanto la Germania, anche a causa delle scelte compiute nel lungo dopoguerra, si trovi in una posizione particolarmente sensibile. L'elevato grado di industrializzazione, la dipendenza da catene di approvvigionamento complesse, la tardiva blindatura dei sistemi digitali e la fiducia coltivata per decenni in un duraturo dividendo della pace hanno prodotto un'infrastruttura materiale e organizzativa non concepita per resistere a campagne di sabotaggio sistematico o a offensive cibernetiche condotte da attori statuali ostili.

In primo luogo, la protezione delle infrastrutture critiche (*Kritische Infrastrukturen, KRITIS*) è divenuta una priorità dichiarata delle istituzioni di sicurezza interna. Secondo la definizione adottata nella strategia federale di protezione delle *KRITIS*, rientrano in tale categoria quelle organizzazioni e quelle strutture che rivestono un'importanza essenziale per il funzionamento del bene comune statale e il cui guasto o la cui compromissione possono produrre carenze di approvvigionamento di lunga durata, gravi perturbazioni della sicurezza pubblica o altre conseguenze di rilievo sistemico. Il tema, pertanto, non investe soltanto la resilienza economica, ma tocca direttamente la continuità dell'ordine pubblico, la capacità di governo delle crisi e la fiducia collettiva nella tenuta dello Stato.

L'economia tedesca, per la sua natura di potenza esportatrice e per il suo elevato livello di industrializzazione e digitalizzazione, risulta strutturalmente esposta. Il sabotaggio dei gasdotti Nord Stream nel settembre 2022 ha rappresentato, sotto questo profilo, un trauma materiale e simbolico, poiché ha reso evidente la vulnerabilità delle reti sottomarine dalle quali dipendono flussi energetici e comunicazioni strategiche. A esso si sono affiancati atti di minore intensità ma di alto impatto sistemico, come il danneggiamento deliberato di cavi in fibra ottica della *Deutsche Bahn* nell'ottobre 2022, nonché il moltiplicarsi di sorvoli non autorizzati tramite droni su infrastrutture sensibili, porti, terminali energetici e siti militari.

Proprio su questo terreno, gli sviluppi più recenti mostrano un'evoluzione significativa della minaccia. Nel marzo 2026 il Ministero federale dell'Interno e per la *Heimat* (BMI) ha qualificato espressamente le minacce ibride come una forma di aggressione multidimensionale che richiede un coordinamento politico-strategico permanente tra federazione, *Länder* e autorità di sicurezza. La stessa amministrazione federale

individua ormai nel BMI il punto nodale del coordinamento governativo contro le minacce ibride, a conferma del fatto che la protezione delle infrastrutture critiche non può più essere trattata come questione meramente settoriale o tecnico-amministrativa, ma deve essere letta quale componente centrale della sicurezza nazionale.

In secondo luogo, il fronte della conflittualità si è spostato in modo massiccio nel dominio cibernetico. Storico, in questo senso, resta l'attacco alla rete informatica del *Bundestag* del 2015, attribuito al gruppo APT28, associato all'intelligence militare russa. Quell'episodio ha segnato uno spartiacque, perché ha mostrato come il cuore della sovranità parlamentare tedesca fosse tecnologicamente permeabile. Negli anni successivi, e con un'intensità ulteriormente accresciuta dopo l'inizio della guerra contro l'Ucraina, gli attacchi si sono estesi a ministeri, governi regionali, partiti politici e grandi imprese, inclusi attori rilevanti per l'industria della difesa e per il *Mittelstand*.

I rapporti annuali del *Bundesamt für Sicherheit in der Informationstechnik* (BSI) descrivono ormai da tempo la situazione della sicurezza informatica in Germania come altamente tesa e persistentemente critica. Il problema non risiede soltanto nel numero degli incidenti, ma nella loro qualità strategica: operazioni di esfiltrazione di dati, attacchi *ransomware*, campagne di *hack-and-leak* e infiltrazioni nei sistemi di comunicazione pubblici e privati puntano a dimostrare l'impotenza dello Stato nel garantire la protezione del proprio ecosistema amministrativo e produttivo.

Tuttavia, è nello spazio cognitivo-informazionale che la Repubblica Federale incontra oggi la sua vulnerabilità più insidiosa. La guerra ibrida si manifesta qui come *weaponization of information*, ossia come uso strategico dell'informazione al fine di manipolare il dibattito pubblico, radicalizzare divisioni preesistenti e delegittimare le istituzioni democratiche e i media tradizionali. Il BMI qualifica espressamente la disinformazione diretta o indirettamente controllata da Stati esteri come componente a pieno titolo delle minacce ibride, soprattutto quando essa mira a influenzare l'opinione pubblica, a dividere la società e a indebolire la capacità di autodifesa democratica del Paese.

Dopo il 24 febbraio 2022, il Ministero dell'Interno ha registrato una netta intensificazione della disinformazione russa in Germania. L'obiettivo dichiarato di queste campagne, secondo la stessa valutazione governativa, consiste nel condizionare il dibattito interno sul sostegno a Kyiv, esacerbare conflitti sociali già esistenti e alimentare la sfiducia verso le istituzioni. In risposta a tale dinamica è stata istituita, sotto la guida del BMI, una *Task Force* contro la disinformazione e altre minacce ibride,

incaricata di coordinare il contrasto all'influenza straniera nello spazio informativo e di rafforzare, in particolare, la protezione dei processi elettorali.

La Germania sperimenta così, in forma particolarmente densa, la trasformazione contemporanea del concetto di sicurezza: dalla difesa dei confini territoriali alla protezione di un ecosistema infrastrutturale, digitale e cognitivo esposto a interferenze costanti. È in questa prospettiva che la guerra ibrida cessa di poter essere descritta come mera minaccia esterna e diventa il catalizzatore di tensioni interne, il punto di saldatura tra logoramento dell'ordine internazionale, vulnerabilità delle infrastrutture critiche ed erosione della fiducia democratica.

3. *La frattura interna: crisi della* Erinnerungskultur *e ascesa di AfD*

L'efficacia della guerra ibrida e della disinformazione descritte non può essere compresa se analizzata esclusivamente come una variabile esogena. Le campagne di destabilizzazione cognitiva operano anche mettendo in discussione una sfera pre-politica come la *Erinnerungskultur* (cultura della memoria) e il processo, inesauribile e istituzionalizzato, della *Vergangenheitsbewältigung* (fare i conti con il passato). È proprio il progressivo sgretolamento di questo fondamento identitario a costituire, altresì, una grave frattura interna della Germania contemporanea, offrendo il fianco alle ingerenze esterne e alimentando l'ascesa di forze politiche come *Alternative für Deutschland* (AfD).

Per decenni, il paradigma repubblicano tedesco si è fondato su un patriottismo costituzionale (*Verfassungspatriotismus*) che poneva al centro dell'identità nazionale l'assunzione delle responsabilità storiche per i crimini del nazionalsocialismo e la Shoah. Questa memoria condivisa, faticosamente conquistata attraverso decenni di dibattiti pubblici – si pensi allo storico *Historikerstreit* (la controversia degli storici) degli anni Ottanta o alle mostre sui crimini della *Wehrmacht* negli anni Novanta –, ha funzionato come il principale deterrente istituzionale contro ogni forma di estremismo di destra e di sciovinismo nazionalista.

Oggi, tuttavia, questa narrazione coesiva è in profonda crisi. La dissoluzione della memoria condivisa è il risultato di dinamiche molteplici. In primo luogo, vi è un fattore anagrafico ineluttabile: la scomparsa dei *Zeitzeugen* (i testimoni oculari), che trasforma la memoria viva in storia musealizzata, inevitabilmente più fredda e contestabile. In secondo luogo, l'emergere di una società post-migrante ha reso più complessa la

trasmissione di una memoria incentrata esclusivamente sulle colpe storiche tedesche a nuove generazioni di cittadini i cui background familiari affondano in geografie e traumi differenti. Su questo terreno già friabile si è innestata una latente insofferenza, diffusa in segmenti non marginali della società, verso il cosiddetto *Schuldkult* (il culto della colpa): un desiderio di normalizzazione nazionale e di tracciare una linea definitiva sul passato (*Schlußstrichdebatte*).

È in questa crisi culturale e identitaria che si inserisce l'ascesa di *Alternative für Deutschland*. Nata nel 2013 come formazione di professori ed economisti euroscettici, in opposizione ai salvataggi finanziari nell'Eurozona, l'AfD ha subito una rapida e radicale mutazione genetica. Il catalizzatore assoluto di questa trasformazione è stata la crisi migratoria del 2015. La decisione della Cancelliera Angela Merkel di non chiudere i confini di fronte a centinaia di migliaia di rifugiati, sintetizzata nel celebre motto *Wir schaffen das* (Ce la faremo), ha provocato una cesura drammatica nel consenso politico tedesco.[4] La percezione di una perdita di controllo statale sui confini e sulla sicurezza interna è stata strumentalizzata dall'AfD, che si è riposizionata come partito populista di destra radicale, anti-immigrazione e identitario. La crisi del 2015 ha fornito all'AfD il propellente elettorale, permettendole di radicarsi profondamente, soprattutto nei *Länder* dell'Est (l'ex DDR), dove la transizione post-1989 aveva lasciato pesanti strascichi di deindustrializzazione e risentimento verso le élite occidentali.[5]

Tuttavia, derubricare l'AfD a un mero partito *single-issue* concentrato sulla xenofobia o sulla reazione ai flussi migratori significa sottovalutarne la reale minaccia istituzionale. Il nucleo ideologico del partito, guidato dalle sue correnti più estreme (come il *Flügel*, formalmente sciolto ma politicamente egemone, guidato da figure come Björn Höcke), mira a una vera e propria rivoluzione culturale che passa per un revisionismo storico spregiudicato. L'obiettivo politico è recidere le radici della *Erinnerungskultur* per riabilitare un nazionalismo tedesco escludente (il concetto etnico di *Volksgemeinschaft*, la comunità di popolo).

Le esternazioni dei leader del partito delineano una strategia revisionista coerente e stratificata. Emblematica è la dichiarazione di Alexander

[4] Per una ricostruzione storica degli eventi Rimando ad A. MERKEL, *Libertà!*, Rizzoli, Milano, 2024, pp. 496-512 e a W. SCHAEUBLE, *Erinnerungen. Mein Leben in der Politik*, Klett-Cotta, Stoccarda, 2024, pp. 540-547.

[5] Cfr. I.-S. KOWALCZUK, *Shock da Libertà. La Germania, l'Est e l'ascesa dell'estremismo*, Donzelli, Roma, 2025.

Gauland, che definì il nazismo e Hitler solo «un po' di sterco di uccello in oltre mille anni di storia tedesca di successo», o il famigerato discorso di Höcke a Dresda nel 2017, in cui definì il Memoriale dell'Olocausto a Berlino un «monumento della vergogna», chiedendo una «svolta di 180 gradi nella politica della memoria».

L'operazione revisionista dell'AfD si spinge ben oltre il nazionalsocialismo, mirando a decostruire l'intero spettro delle responsabilità storiche tedesche per ridefinire il posizionamento geopolitico e morale della Germania contemporanea. Riguardo alla Prima guerra mondiale, circoli intellettuali vicini al partito rigettano la consolidata tesi della responsabilità primaria dell'Impero Guglielmino (la *Fischer-Kontroverse*), promuovendo una narrazione in cui la Germania fu vittima di un accerchiamento da parte delle potenze dell'Intesa. Riguardo alla Seconda guerra mondiale, la retorica dell'AfD tende costantemente a enfatizzare le sofferenze civili tedesche – come i bombardamenti alleati su Dresda o le espulsioni dai territori orientali (*Vertriebene*) – operando una tacita equiparazione tra aggressori e vittime che relativizza l'unicità dei crimini nazisti.

Ancora maggiormente rivelatrice, e spesso sottovalutata dagli osservatori internazionali, è l'offensiva dell'AfD sul tema del colonialismo tedesco in Africa (in particolare in Namibia e in Africa Orientale). Mentre le istituzioni federali, i musei e la storiografia ufficiale negli ultimi anni hanno avviato un doloroso processo di riconoscimento dei crimini coloniali – culminato nel 2021 con le scuse formali della Germania alla Namibia per il genocidio dei popoli Herero e Nama –, l'AfD si è mossa nella direzione diametralmente opposta. Attraverso interrogazioni parlamentari e documenti programmatici, il partito ha esaltato i presunti aspetti civilizzatori del colonialismo tedesco, minimizzando le violenze di massa e contestando aspramente le restituzioni di beni culturali (come i Bronzi del Benin) e i risarcimenti. Questa strenua difesa dell'Impero coloniale non è un vezzo accademico, ma un tassello fondamentale di una guerra culturale (*Kulturkampf*): difendere il colonialismo serve a respingere le moderne istanze anti-razziste e post-coloniali, rafforzando l'idea di un'Europa forte, suprematista e non gravata da complessi di colpa verso il Sud Globale.

La saldatura tra questo revisionismo interno e la guerra ibrida esterna costituisce oggi il principale dilemma per la sicurezza nazionale della Repubblica Federale. L'AfD è diventata, consciamente o per convergenza di interessi, il vettore oggettivo della narrazione russa in Germania. L'antiamericanismo, il rifiuto del liberalismo occidentale, la richiesta di fine delle sanzioni contro Mosca, il blocco degli aiuti militari all'Ucraina

e l'esaltazione di un modello di società tradizionale e autoritaria trovano perfetta consonanza tra le propagande di Mosca e di gran parte del partito estremista tedesco.

Di fronte a questa minaccia sistemica, le istituzioni della democrazia militante (*streitbare Demokratie*) tedesca sono state costrette a reagire, mobilitando i propri strumenti di difesa costituzionale. L'Ufficio federale per la protezione della Costituzione (*BfV*) ha classificato intere sezioni regionali dell'AfD (in Sassonia, Turingia e Sassonia-Anhalt) e la sua organizzazione giovanile (*Junge Alternative*) come comprovatamente estremiste di destra (*gesichert rechtsextrem*), ponendole sotto sorveglianza dell'intelligence. Tuttavia, la criminalizzazione e la sorveglianza istituzionale, pur necessarie, si scontrano con la realtà politica di un partito che in ampie zone del Paese sfiora o supera il 30 per cento dei consensi, ponendo la democrazia tedesca di fronte a un paradosso: come difendere l'ordine costituzionale e la sicurezza dello Stato quando una parte rilevante del corpo elettorale sostiene e vota forze politiche che puntano a smantellare le fondamenta morali e storiche su cui quello stesso Stato è edificato? La risposta a questo interrogativo ha spinto la Repubblica Federale a una vasta riorganizzazione delle proprie strategie di difesa e di tenuta istituzionale.

4. *La reazione dello Stato: architettura di difesa e sicurezza integrata di fronte alla minaccia multidimensionale*

La convergenza tra aggressione ibrida esterna e frammentazione identitaria interna ha posto la Repubblica Federale di fronte alla più profonda crisi di sicurezza dalla sua fondazione. La consapevolezza che il modello della *Zivilmacht* e il quasi integrale affidamento all'ombrello NATO e all'interdipendenza economica non fossero più sufficienti a garantire la sicurezza dello Stato ha innescato una reazione istituzionale di ampiezza inedita. Tale reazione non si esaurisce in un mero adeguamento tecnico degli strumenti militari, ma implica un ripensamento complessivo dell'architettura di sicurezza nazionale, che il governo ha concettualizzato, con la Strategia di Sicurezza Nazionale del giugno 2023, nei termini di una *Integrierte Sicherheit* fondata sui tre pilastri della *Wehrhaftigkeit*, della *Resilienz* e della *Nachhaltigkeit*.

Il primo pilastro di questa reazione riguarda la dimensione materiale e militare. Dopo il 1990, la *Bundeswehr* era stata progressivamente ridimensionata e riconfigurata come forza di intervento limitata, orientata

prevalentemente a missioni di gestione delle crisi all'estero; la sospensione della coscrizione nel 2011 aveva poi accentuato questa tendenza. Con il discorso sulla *Zeitenwende* del 27 febbraio 2022, il Cancelliere Scholz ha segnato una cesura netta, annunciando la creazione di un *Sondervermögen* di cento miliardi di euro destinato al riequipaggiamento delle Forze armate, successivamente approvato dal *Bundestag* nel giugno 2022. Il Fondo speciale è stato concepito per colmare gravi criticità accumulate in decenni di sottofinanziamento e per consentire alla Germania di avvicinarsi stabilmente all'obiettivo del 2 per cento del PIL in spesa per la difesa secondo i parametri NATO.

Sul piano interpretativo, il *Sondervermögen* non può essere letto come una semplice voce aggiuntiva del bilancio ordinario della difesa, né come un incremento stabilmente acquisito della capacità finanziaria dello Stato. Esso costituisce piuttosto uno strumento straordinario, giuridicamente separato dall'*Einzelplan 14* e sottratto ai vincoli ordinari del freno al debito *Schuldenbremse*, concepito per finanziare programmi di riarmo di particolare rilevanza e per consentire alla Germania di raggiungere, in media pluriennale, la soglia del 2 per cento del PIL. Proprio per questo, il fondo va interpretato come un acceleratore temporaneo: nel breve periodo esso ha permesso di colmare lacune strutturali accumulate in decenni di sottofinanziamento; nel medio periodo, tuttavia, esso rende evidente il problema della sostenibilità strutturale della svolta, poiché una volta esaurito il *Sondervermögen* il mantenimento degli stessi livelli di spesa potrà avvenire solo attraverso un corrispondente rialzo del bilancio ordinario o mediante nuove eccezioni al regime fiscale vigente. Ne consegue che il fondo speciale, più che risolvere definitivamente la questione del riarmo tedesco, ne mette in luce il nodo politico fondamentale: trasformare un eccezionale sforzo di ricostruzione delle capacità militari in una postura finanziaria e strategica durevole. In questo senso occorre distinguere tra il *Sondervermögen Bundeswehr* inaugurato dal governo Scholz nel 2022 e le innovazioni fiscali e di bilancio intervenute con il nuovo esecutivo insediatosi nel 2025. Il fondo speciale da cento miliardi fu istituito come risposta immediata allo shock strategico prodotto dall'invasione russa dell'Ucraina e mantiene una destinazione specifica, rigidamente connessa al riequipaggiamento delle Forze armate. Il governo successivo non ha istituito un secondo *Sondervermögen* dedicato esclusivamente alla *Bundeswehr*, ha invece operato su un piano più ampio, ristrutturando il quadro finanziario generale degli investimenti pubblici e collocando la difesa entro una più estesa strategia di potenza, competitività e di investimenti infrastrutturali. La differenza tra le due fasi è dunque anche di

ordine politico-costituzionale. La *Zeitenwende* di Scholz aveva il carattere di una eccezione storica: un fondo straordinario, simbolicamente e giuridicamente separato dal bilancio ordinario. La fase politica apertasi nel 2025, al contrario, tende a normalizzare l'eccezione, spostando il baricentro dal semplice recupero delle capacità perdute a una più vasta trasformazione della Germania in attore capace di sostenere nel lungo periodo livelli di spesa, investimenti infrastrutturali e programmi industriali coerenti con una postura strategica di maggiore intensità.

Il nuovo fondo speciale da 500 miliardi è destinato in via primaria a infrastrutture e neutralità climatica, ma è rilevante anche per la sicurezza in senso lato. Esso opera come strumento orizzontale di politica economica e di investimento pubblico, dal quale possono derivare effetti indiretti ma significativi anche per la difesa, nella misura in cui rafforza reti logistiche, mobilità strategica, infrastrutture energetiche, digitali e industriali necessarie alla resilienza nazionale.

Quanto al bilancio 2026, l'integrazione tra i due piani va letta in termini funzionali, non contabili. Le spese strettamente militari continuano a poggiare, da un lato, sull'*Einzelplan 14* e, dall'altro, sulle residue disponibilità del *Sondervermögen Bundeswehr*, che insieme portano il volume complessivo della difesa tedesca oltre i 100 miliardi di euro. Il nuovo fondo da 500 miliardi, invece, non confluisce come tale nel bilancio della difesa, ma alleggerisce e ridefinisce il contesto materiale entro cui esso opera: investendo in infrastrutture civili e *dual use*, esso amplia la base logistica e produttiva della sicurezza nazionale e consente al governo di sostenere una crescita della spesa militare ordinaria senza far ricadere sull'*Einzelplan 14* l'intero onere della modernizzazione sistemica dello Stato.

Investimenti in Difesa – Germania 1990-2026[6]

Anno	**Spesa (Mld €)**	**% PIL**
	(prezzi correnti)	*(SIPRI/NATO)*
1990	36,8	2,52%
1991	33,2	2,00%
1992	31,5	1,86%
1993	29,4	1,69%

[6] Dati annuali: spesa in miliardi EUR (prezzi correnti) e quota % del PIL. Fonti: SIPRI, NATO, *Bundesministerium der Verteidigung*.

1994	28,0	1,55%
1995	27,5	1,50%
1996	26,8	1,47%
1997	26,2	1,41%
1998	26,0	1,39%
1999	24,3	1,40%
2000	24,0	1,36%
2001	24,5	1,32%
2002	24,4	1,33%
2003	24,4	1,32%
2004	24,1	1,27%
2005	23,2	1,07%
2006	24,5	1,13%
2007	25,5	1,17%
2008	27,0	1,22%
2009	26,8	1,30%
2010	27,2	1,23%
2011	29,0	1,20%
2012	28,3	1,12%
2013	30,2	1,16%
2014	34,6	1,18%
2015	32,4	1,12%
2016	35,1	1,13%
2017	36,7	1,17%
2018	38,5	1,17%
2019	43,2	1,26%
2020	45,6	1,37%
2021	46,9	1,32%
2022	50,3	1,38%
2023	55,6	1,52%
2024	77,8	2,12%
2025	86,5	2,30%
2026	108,2	2,80%

Sul piano qualitativo, le risorse del *Sondervermögen* sono state indirizzate verso l'acquisto di sistemi ritenuti essenziali per ristabilire la credibilità della deterrenza tedesca: tra essi i caccia F-35 per assicurare la continuità della *nuclear sharing* nell'ambito dell'Alleanza, il rafforzamento della difesa aerea, anche attraverso la partecipazione all'iniziativa *European Sky Shield*, e il potenziamento delle capacità terrestri, logistiche e di comando. Non meno rilevante è il riposizionamento strategico che accompagna tali scelte: l'impegno a schierare stabilmente una brigata tedesca in Lituania, intorno alla soglia di 4.000 militari, conferma la trasformazione della Germania in perno logistico e militare del fianco orientale della NATO. Tuttavia, come l'analisi sin qui svolta ha mostrato, un riarmo esclusivamente convenzionale risulterebbe insufficiente di fronte a una minaccia ibrida che si dispiega soprattutto nei domini digitale, infrastrutturale e cognitivo. Già nel 2017 la Bundeswehr aveva creato il *Kommando Cyber- und Informationsraum* (CIR), elevandolo a organizzazione militare autonoma. Dopo il 2022, la dimensione cibernetica della sicurezza è stata ulteriormente rafforzata attraverso il potenziamento delle competenze del CIR, del BSI e delle strutture di coordinamento interministeriale. In parallelo, il governo federale ha lavorato a una normativa quadro per la protezione delle infrastrutture critiche, il cosiddetto *KRITIS-Dachgesetz*, destinata a irrigidire gli standard di sicurezza fisica e digitale nei settori dell'energia, della sanità, della logistica, delle telecomunicazioni e dei trasporti.

In tale contesto, il più ampio patrimonio di linee guida elaborate dal BMI, dal BBK e dal BSI in materia di rischio e crisis management per le infrastrutture critiche acquista oggi una nuova centralità ed è strutturato in cinque fasi, dalla *Vorplanung* alla *Risikoanalyse*, dalle misure preventive al *Krisenmanagement* sino alla successiva valutazione. Esso mostra come la resilienza non possa essere ridotta a una categoria retorica, ma richieda procedure, responsabilità, catene decisionali e capacità organizzative ben definite. La novità del contesto attuale consiste nel fatto che questo apparato, originariamente pensato soprattutto per fronteggiare guasti tecnici, catastrofi naturali o crisi settoriali, deve ora essere adattato a minacce ibride intenzionali, multidominio e politicamente orientate.

Una delle aree in cui tale mutamento è più evidente riguarda la minaccia proveniente da sistemi aerei senza pilota. L'aumento di intercettazioni di droni non autorizzati su porti, terminali energetici, aeroporti e installazioni militari ha indotto la Germania a consolidare la propria architettura di difesa contro i vettori a bassa quota. Nel dicembre 2025 il BMI ha annunciato l'istituzione di un *Zentrum für Drohnenabwehr*, con-

cepito come hub nazionale per il coordinamento dell'analisi del rischio, lo sviluppo di capacità tecniche e la cooperazione tra *Bund, Länder* e gestori di infrastrutture critiche. La creazione di questo centro segnala il passaggio da una gestione episodica del fenomeno a una sua istituzionalizzazione quale problema permanente di sicurezza interna.

Parallelamente, sempre nel dicembre 2025, il Ministero dell'Interno ha rafforzato le capacità di analisi e allerta situazionale attraverso nuove strutture comuni di dati e valutazione, volte a migliorare l'individuazione precoce di *pattern* di attacco riconducibili a minacce ibride. Queste strutture, istituite per integrare flussi informativi provenienti da amministrazioni, autorità di sicurezza e altri attori rilevanti, rispondono all'esigenza di superare la storica frammentazione delle competenze e di fornire un quadro operativo più rapido nelle situazioni di crisi. In esse si coglie una delle trasformazioni più significative della sicurezza tedesca contemporanea: il passaggio da una logica settoriale e reattiva a una logica di coordinamento permanente, trasversale e anticipatoria.

La *Strategia di Sicurezza Nazionale* del 2023 si colloca in questa traiettoria e ha trovato, sotto il governo insediatosi nel 2025 (Governo Merz), un completamento istituzionale con la creazione di un Consiglio di Sicurezza Nazionale presso la Cancelleria, presieduto dal Cancelliere e composto dai principali ministri competenti per esteri, difesa, interno, finanze ed economia. A questo organo sono affidate funzioni di coordinamento politico della sicurezza integrata, di sviluppo delle strategie, di previsione e valutazione congiunta delle situazioni, nonché di indirizzo per la gestione delle crisi ibride e delle minacce alla sicurezza nazionale.

La dimensione cognitiva della reazione statale è altrettanto decisiva. Il BMI considera oggi la disinformazione eterodiretta una componente a pieno titolo delle minacce ibride, in particolare quando mira a manipolare l'opinione pubblica, dividere la società e indebolire la fiducia nelle istituzioni. Dopo l'inizio della guerra contro l'Ucraina, il Ministero ha registrato una sensibile crescita della disinformazione russa in Germania e ha istituito una *Task Force* contro la disinformazione e altre minacce ibride, con particolare attenzione alla protezione dei processi elettorali. A ciò si aggiungono iniziative volte a rafforzare la resilienza sociale e la competenza mediale, come il progetto *Jahr der Nachricht 2024* e il *Forum gegen Fakes*, dai quali il governo federale intende trarre elementi per una più ampia strategia di contrasto alla manipolazione informativa.

In questo quadro, la reazione dello Stato tedesco appare come un complesso processo di aggiornamento dell'*hardware* e del *software* della sicurezza. Da un lato, riarmo, cyber-difesa, protezione delle infrastrut-

ture critiche e nuove strutture di coordinamento; dall'altro, strategie nazionali, categorie giuridiche di contrasto, sorveglianza costituzionale, promozione della resilienza sociale e difesa del dominio informativo. Il problema di fondo, tuttavia, rimane aperto: fino a che punto una democrazia può supplire mediante strumenti amministrativi, legislativi e militari al progressivo logoramento del proprio fondamento culturale? Se la rigenerazione del consenso democratico e della cultura della memoria non accompagnerà il rafforzamento dell'apparato di sicurezza, la Germania rischierà di costruire una macchina difensiva sempre più sofisticata a protezione di una democrazia internamente indebolita.

Sul piano documentale, gli sviluppi più recenti confermano questa traiettoria di adattamento: il BMI ha progressivamente ricondotto in un medesimo quadro strategico la protezione delle *KRITIS*, il contrasto alla disinformazione, la difesa anti-drone e il coordinamento interistituzionale contro le minacce ibride. Ciò rafforza la lettura secondo cui, nel caso tedesco, la sicurezza nazionale tende ormai a configurarsi come funzione congiunta di capacità militari, resilienza infrastrutturale, prontezza amministrativa e tenuta dello spazio pubblico democratico.

5. Conclusioni: l'imprevedibilità del futuro democratico e la memoria come infrastruttura di sicurezza

Il percorso analitico sviluppato ha inteso dimostrare come la crisi della democrazia liberale trovi nella Repubblica Federale Tedesca un caso di studio di notevole interesse. L'architettura istituzionale e culturale su cui la Germania ha fondato la propria rinascita democratica post-1945 è oggi sottoposta a uno stress test senza precedenti, generato dalla perfetta e letale sovrapposizione tra vettori di minaccia esogeni ed endogeni. Per decenni, lo Stato tedesco ha coltivato un peculiare eccezionalismo pacifista e post-nazionale, nella convinzione che la brutale lezione della prima metà del Novecento avesse vaccinato per sempre la nazione contro i demoni del militarismo e del nazionalismo radicale. Questa presunzione di immunità, tradottasi nel paradigma della potenza civile (*Zivilmacht*) e nell'affidamento all'interdipendenza economica globale (*Wandel durch Handel*), si è infranta contro la cruda realtà del ritorno della guerra di aggressione sul continente europeo e l'esplosione della conflittualità ibrida multidominio.

Il nucleo della vulnerabilità tedesca non risiede esclusivamente nella sua storica impreparazione militare convenzionale o nella pur grave dipendenza energetica accumulata negli anni. Il vero punto di cedimento,

quello che rende la Germania contemporanea il ventre molle della stabilità europea, è di natura pre-politica e identitaria. La sicurezza nazionale, tradizionalmente intesa come difesa dei confini territoriali e protezione degli asset strategici, si è inesorabilmente fusa con il concetto di tenuta istituzionale e coesione democratica. In questo mutato scenario, l'offensiva ibrida russa – articolata attraverso lo spionaggio industriale, il sabotaggio cinetico tramite droni, la paralisi cibernetica delle infrastrutture critiche (*KRITIS*) e l'inquinamento sistematico dell'ecosistema informativo – non opererebbe con tale devastante efficacia se non trovasse un terreno interno già profondamente solcato da faglie socio-culturali. La minaccia ibrida, per sua stessa natura costitutiva, non crea ex novo le divisioni di un Paese, ma agisce come un moltiplicatore di forza sulle crepe preesistenti, incuneandosi nelle insicurezze collettive per disarticolare la fiducia tra governati e governanti.

Da questo punto di vista, si può affermare che il *Sondervermögen* del 2022 appartenga ancora alla logica del recupero, mentre la nuova cornice finanziaria del 2025-2026 risponde a una logica di consolidamento e di espansione. Il governo di Olaf Scholz (2021-2025) ha aperto la breccia, rendendo politicamente possibile il ritorno della difesa al centro della statualità tedesca; il governo Merz (2025-) sembra puntare a trasformare quella breccia in un nuovo paradigma di bilancio, nel quale riarmo, infrastrutture strategiche, sicurezza energetica, tecnologia e competitività industriale vengono ricondotti a un medesimo disegno di potenza pubblica.

Una crepa altrettanto profonda è rappresentata dalla crisi inesorabile della *Erinnerungskultur* (la cultura della memoria). La Germania ha fondato la propria legittimità repubblicana, il proprio patriottismo costituzionale (*Verfassungspatriotismus*), sull'assunzione incondizionata delle responsabilità per i crimini del nazionalsocialismo, per l'Olocausto e per la devastazione bellica del continente. Questo fondamento morale ha agito per decenni come un ancoraggio di sicurezza (*Sicherheitsanker*), un argine istituzionale che impediva il ritorno di ideologie eversive. Oggi, il collasso anagrafico della generazione dei testimoni (*Zeitzeugen*), l'emersione di una società post-migrante frammentata e le cicatrici non rimarginate della riunificazione tra Est e Ovest, hanno generato un vuoto di senso storico in cui si è inserito il radicalismo di destra.

L'ascesa di *Alternative für Deutschland* (AfD) non è interpretabile, in questa prospettiva, come una mera reazione populista alla crisi migratoria del 2015 o al malcontento economico derivante dalla recente policrisi[7].

[7] Rimando a: G.E. Rusconi, *Dove va la Germania. La sfida della nuova destra popu-*

Essa rappresenta un progetto politico di eversione culturale, un tentativo strutturato di rescindere il patto fondativo della Repubblica. Il revisionismo storico promosso dall'AfD e dai suoi ideologi di riferimento non si limita alla relativizzazione della Seconda guerra mondiale, ma si estende, come analizzato, fino alla riabilitazione del colonialismo tedesco in Africa, nel tentativo di ricostruire un'identità nazionale normalizzata, sciovinista e impermeabile ai complessi di colpa.

È in questo spazio di revisionismo che si consuma la saldatura fatale con l'aggressione ibrida esterna. La narrativa russa volta a destabilizzare le democrazie occidentali, screditare le istituzioni liberali e interrompere il sostegno all'Ucraina, trova nel partito di destra radicale un alleato oggettivo, se non un vero e proprio vettore (*Proxy*). Entrambi gli attori, pur muovendo da presupposti storici e geopolitici differenti, condividono lo stesso obiettivo tattico a breve e medio termine: la delegittimazione dell'ordine liberal-democratico e la decostruzione delle narrazioni storiche su cui tale ordine si regge. In questo senso, l'AfD agisce come l'infrastruttura politica interna che traduce la guerra cognitiva russa in prassi parlamentare ed elettorale, trasformando una minaccia esogena in un endemico collasso della tenuta istituzionale tedesca.

Di fronte a questa morsa senza precedenti, la reazione dello Stato federale è stata ampia e strutturalmente significativa. La Germania ha impresso una forte accelerazione al proprio riarmo ed ha adottato la prima Strategia di Sicurezza Nazionale della propria storia e ha intensificato gli strumenti di protezione delle infrastrutture critiche e dello spazio informativo. Un primo bilancio di questa colossale operazione di messa in sicurezza istituzionale non può dirsi privo di profonde ombre e contraddizioni. Vi è un disallineamento temporale e procedurale tra la rapidità mutevole delle minacce (dalle *bot-farm* russe ai sabotaggi tramite droni)

lista, il Mulino, Bologna, 2019; U. VILLANI-LUBELLI, *La Repubblica Federale tedesca e la difesa della democrazia (wehrhafte Demokratie) tra l'ascesa dell'estrema destra e crisi dei partiti tradizionali*, in *Nuovi Autoritarismi e Democrazia: Diritto, Istituzioni e Società*, pp. 229-248; ID., *Nationalism Against Europeanisation: The Challenge of Far-Right Populism for European Democracy. A Comparison of Italy and Gerany*, in C. LIERMANN TRANIELLO, M. SCOTTO, J. STEFENELLI (a cura di) *Stati Uniti d'Europa: Auspicio, incubo, utopia?/Vereinigte Staaten von Europea: Wunschbild, Alptraum, Utopie?*, Villa Vigoni Editore, Loveno di Menaggio, 2020, pp. 93-104, in part. 95-98; ID., *L'ascesa di Alternative für Deutschland. Origine e conseguenze politihe e istituzionali*, in L. RAPONE (a cura di), *Le destre europee nel XXI secolo. Eredità e mutamenti*, Carocci, Roma, 2026, pp. 143-160 (in corso di stampa). Per un profilo giornalistico ma molto accurato si veda T. MASTROBUONI, *La peste. Indagine sulla destra in Germania*, Feltrinelli, Milano, 2025.

e i macchinosi processi di adeguamento normativo di un sistema costituzionale concepito nel 1949 per prevenire l'eccessivo accentramento di potere esecutivo.[8]

Emerge, altresì, un limite epistemologico nella risposta governativa. La reazione si è finora concentrata quasi esclusivamente sul rafforzamento dell'acquisizione di sistemi d'arma, *firewall* digitali, leggi più restrittive sulla sicurezza delle reti e sorveglianza di polizia. Tuttavia, l'attuale crisi tedesca dimostra incontrovertibilmente che nessuna barriera cibernetica e nessuna brigata corazzata possono supplire al revisionismo della democrazia tedesca. Se una percentuale che oscilla tra il 20 e il 30 percento dell'elettorato (con picchi drammaticamente superiori nei *Länder* orientali) si riconosce in un'offerta politica che promuove una lettura revisionista della storia nazionale e simpatizza con narrazioni autocratiche straniere, l'approccio puramente repressivo o militare si rivela tragicamente insufficiente. L'utilizzo dell'intelligence per arginare un fenomeno elettorale di massa rischia, paradossalmente, di alimentare la retorica vittimistica del partito anti-sistema, confermando la narrativa di uno *Stato profondo* illegittimo che opprime la reale volontà popolare.

Alla luce di questi elementi strutturali, lo sviluppo a breve e medio termine della democrazia tedesca appare segnato da una radicale imprevedibilità. La Repubblica Federale si trova a un crocevia storico in cui le classiche dinamiche dell'alternanza democratica sono state sostituite da una polarizzazione asimmetrica che minaccia l'essenza stessa del patto repubblicano. Da un lato, le forze politiche tradizionali (dall'Unione CDU/CSU alla SPD, dai Verdi ai Liberali) tentano di erigere cordoni sanitari (*Brandmauer*) per escludere la destra radicale dalle leve del potere esecutivo. Dall'altro, il peso elettorale di AfD, soprattutto a livello regionale e locale, rende sempre più complessa la formazione di maggioranze coese e funzionali, costringendo i partiti moderati a coalizioni eterogenee che finiscono inevitabilmente per paralizzare l'azione di governo, esacerbando ulteriormente il malcontento dei cittadini e nutrendo il circolo vizioso della disaffezione democratica.

Un ulteriore elemento di imprevedibilità è dato dalla potenziale attivazione di misure estreme di tutela costituzionale. Nel dibattito pubblico e accademico tedesco ha ripreso vigore l'ipotesi di richiedere al Tribunale Costituzionale Federale (*Bundesverfassungsgericht*) lo scioglimento formale di *Alternative für Deutschland* ai sensi dell'articolo 21.2 della Legge

[8] Cfr. C. Masala, *Bedigt abwehrbereit. Deutschlands Schwäche in der Zeitenwende*, C.H. Beck, Monaco di Baviera, 2023.

Fondamentale (*Grundgesetz*): «*I partiti, che per le loro finalità o per il comportamento dei loro aderenti mirino ad attentare al libero e democratico ordinamento costituzionale o a sovvertirlo o a mettere in pericolo l'esistenza della Repubblica Federale di Germania sono incostituzionali. Sulla questione di incostituzionalità decide la Corte costituzionale federale*».

Sebbene formalmente giustificata dalle derive estremiste e dalle indagini dell'intelligence, una simile mossa comporterebbe un rischio politico incalcolabile: il bando di un partito che rappresenta milioni di elettori potrebbe innescare una crisi di rigetto extra-parlamentare di proporzioni vaste, alienando in modo forse definitivo un'intera fetta del Paese (in particolare nell'Est) dalle istituzioni democratiche. Allo stesso tempo, non si possono escludere scenari di resilienza. La società civile tedesca ha dimostrato, in più occasioni recenti, una sorprendente capacità di mobilitazione di massa in difesa dei valori democratici e contro le derive razziste e revisioniste della destra. Esiste un nucleo profondo e maggioritario del Paese che riconosce la gravità della posta in gioco e che preme per una rigenerazione del dibattito pubblico. Il successo o il fallimento di questa mobilitazione dipenderà dalla capacità della classe dirigente di andare oltre la mera gestione tecnocratica delle crisi. La *Zeitenwende* non potrà compiersi pienamente se rimarrà confinata all'ambito della politica di difesa o dell'ingegneria costituzionale; essa necessita di una parallela e urgente nuova capacità di formulare una nuova narrazione nazionale che tenga insieme il rigore della memoria storica e le sfide di una società multiculturale e interconnessa nel XXI secolo.

In conclusione, l'analisi del caso tedesco impone un ripensamento radicale delle categorie attraverso cui interpretiamo la sicurezza internazionale. L'eredità storica, la gestione della memoria e il consenso sui valori fondanti di una nazione non sono più declinabili come meri esercizi storiografici o dibattiti relegati alla sfera culturale. Nell'era delle minacce ibride e della guerra cognitiva permanente, il passato condiviso rappresenta a tutti gli effetti la prima e più importante infrastruttura critica di sicurezza nazionale. Una società che perde il consenso sulle proprie radici e sui propri limiti morali diviene un ecosistema altamente infiammabile, facilmente penetrabile da algoritmi ostili, droni spia e propagande autocratiche. La Repubblica Federale Tedesca ha dimostrato di aver compreso la necessità di armarsi materialmente per difendere l'Europa democratica. Affinché gli imponenti investimenti nella difesa convenzionale e cibernetica non si riducano alla costruzione di una difesa tecnologicamente avanzata ma potenzialmente aggirabile dall'interno, le istituzioni e la società tedesca dovranno riscoprire e rinvigorire il nucleo della loro identità democratica.

LA SFIDA DELLA DISINFORMAZIONE NELL'ECOSISTEMA DIGITALE EUROPEO

Silvia Sassi[*]

1. *Introduzione*

Nel contesto dell'attuale trasformazione digitale, la disinformazione si impone come uno dei fenomeni più rilevanti e problematici per gli ordinamenti giuridici contemporanei[1]. Essa non si limita ad incidere sulla qualità dell'informazione, ma investe direttamente le condizioni di funzionamento delle democrazie liberali, sollevando interrogativi altamente sensibili sul piano costituzionale[2], che richiedono un delicato equilibrio tra la tutela dei diritti fondamentali e la salvaguardia dell'ordine demo-

[*] Professoressa in Diritto pubblico comparato nell'Università degli Studi di Firenze.

[1] Il tema della disinformazione è stato ampiamente affrontato, data la sua interdisciplinarietà, sotto molteplici profili, da quello giusfilosofico a quello socio-politologico, finanche economico: cfr. G. PITRUZZELLA, O. POLLICINO, *Disinformation and Hate Speech. A European Constitutional Perspective*, Egea, Milano, 2020; L. Moran, *Fighting Disinformation,* 106 A.B.A. J. 20, 2020; T. GUERINI, *Fake News e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020; C.R. SUSTEIN, *Liars. Falsehood and Free Speech in Age of Deception*, OUP, Oxford, 2021; A. NICITA, *Il Mercato delle Verità. Come la disinformazione minaccia la democrazia*, il Mulino, Bologna, 2021; S. SASSI, *Disinformazione contro Costituzionalismo*, Editoriale Scientifica, Napoli, 2021; J. ATTALI, *Disinformati. Giornalismo e libertà nell'epoca dei social*, trad. it., Ponte alle Grazie, Milano, 2022; T. RID, *Misure attive. Storia segreta della disinformazione*, trad. it., Luiss Uni- versity Press, Roma, 2022; C. HASSEN, C. PINELLI, *Disinformazione e democrazia. Populismo, rete e regolazione*, Marsilio, Venezia, 2022; B.C. HAN, *Infocrazia*, trad. it., Einaudi, Torino, 2023; L. MCINTYRE, *On Disinformation. How to Fight for Truth and Protect Democracy*, MIT Press, Cambridge-MA, 2023.

[2] Problema esaminato con tratti chiaroscuri da P. COSTANZO, *Il fattore tecnologico e il suo impatto sulle libertà fondamentali*, in T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI, (a cura di), *Diritti e libertà in internet*, Milano, 2017; B. CARAVITA DI TORITTO, *Principi costituzionali e intelligenza artificiale*, ora in Id., *Letture di diritto costituzionale*, Giappichelli, Torino, 2020; A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligen-*

cratico. L'ambiente digitale nel quale la disinformazione si diffonde non costituisce un mero spazio neutrale di circolazione delle idee, ma una infrastruttura complessa, caratterizzata da logiche algoritmiche, modelli economici basati sull'attenzione e dinamiche di amplificazione che influenzano significativamente la formazione dell'opinione pubblica[3]. In tale contesto, la disinformazione assume una portata sistemica, tale da essere qualificata, in taluni casi e da alcuni ordinamenti giuridici[4], come una minaccia concreta alla stabilità delle democrazie pluralistiche. Parallelamente, il mutamento del contesto geopolitico ha contribuito a ridefinire ulteriormente la natura del fenomeno. Le campagne di disinformazione si inseriscono oggi in strategie più ampie di guerra ibrida, in cui strumenti informativi e tecnologici si affiancano a forme tradizionali di conflitto[5]. Come evidenziato di recente dalla dottrina[6], le società europee sono esposte a una pressione costante che si dispiega non solo nello spazio fisico, ma anche e soprattutto in quello cognitivo, attraverso una "guerra delle percezioni"[7]. In questo scenario, l'Unione europea in particolare si trova a dover affrontare una tensione strutturale: da un lato, la necessità di contrastare fenomeni di manipolazione informativa sempre più sofi-

za Artificiale, in A. D'ALOIA (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, FrancoAngeli, 2 ed., 2023.

[3] Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaello Cortina, 2017; S. ZUBOFF. *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, Luiss, 2019; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw J./Riv. BioDir.*, n. 1, 2019; G. GHIDINI, D. MANCA, A. MASSOLO, *La nuova civiltà digitale. L'anima doppia della tecnologia*, Milano 2020; V. CODELUPPI, *Mondo digitale*, Laterza, Roma-Bari, 2022. Sul modo attraverso cui questi aziende sono riuscite ad arrivare a un simile dominio e a costruire il loro potere v. da ultimo L. BALESTRIERI, *Big Tech. Il potere dei giganti della tecnologia*, Roma-Bari, Laterza, 2026.

[4] La School of Public Policy del Georgia Institute of Technology esprime forti critiche nei confronti di queste posizioni. A questo proposito, si veda in particolare M. MUELLER, «*Misinformation about Disinformation?*», in www.internetgovernace.org.

[5] A. BECCARIO, *Guerra e strategia nel XXI secolo*, Morcellina, Brescia, 2023, p. 27. Sulla guerra ibrida, recentemente, vi è stata una implosione di interesse. Per conseguenza difficile è una sua definizione stringente. È riconosciuto però che questo concetto è stato introdotto da J.N. MATTIS, F.G. HOFFMAN, nel loro articolo da titolo *Future Warfare: The Rise of Hybrid Wars*, in *US Naval Institute*, 132(11), 2005, pp. 1 ss.

[6] V. per tutti A. STERPA, *La difesa della democrazia dalle minacce ibride. Teorie della comunità, dell'autorità, del potere e migrazioni: elementi per un'analisi strategica della "guerra tiepida"*, Editoriale Scientifica, Napoli, 2025.

[7] Al riguardo v. l'ultimo rapporto NATO: J.M. BLATNY, S. SØNDERGAARD, *Cognitive Warfare*, 2025.

sticati; dall'altro, l'obbligo di preservare i diritti fondamentali, *in primis* la libertà di espressione[8]. Il presente contributo intende analizzare tale tensione, esaminando la configurazione giuridica della disinformazione in particolare nell'ordinamento europeo[9], le risposte normative adottate e i limiti che esse presentano alla luce delle trasformazioni in atto.

2. *La natura sistemica della disinformazione*

Per comprendere adeguatamente la disinformazione è necessario andare oltre al mero concetto di contenuto falso[10]. Il fenomeno *de quo* è fenomeno complesso e strutturato, e proprio per questo capace di incidere sull'equilibrio complessivo dello spazio pubblico. Nel contesto europeo, non a caso, essi viene definita come «la diffusione di informazioni false, inesatte o fuorvianti orientata a provocare un danno pubblico o a conseguire un vantaggio»[11], per porre in evidenza due dimensioni essenziali:

[8] Cfr. F. Nunez, *Disinformation Legislation and Freedom of Expression,* 10 *UC Irvine L. Rev.* 783*,* 2020*;* R.A. Jones, *Defamation, Disinformation, and the Press Function, 3 J. Free Speech L.* 103, 2023. V. anche la corposa introduzione di A. Clooney (*Introduction*, in A. Clooney, D. Neuberger (eds.), *Freedom of Speech in International Law*, Oxford, OUP, 2024) che confrontando diversi sistemi giuridici (internazionale e regionali, come europeo, americano e africano) rileva una sostanziale convergenza nella protezione della libertà di espressione, pur con alcune differenze, e mette in evidenza le principali sfide contemporanee cui è soggetta tale libertà, la cui tutela, secondo l'autore, non dipende da un solo strumento, ma da un sistema integrato fatto di norme vincolanti, limiti alle restrizioni, meccanismi di controllo e obblighi attivi degli Stati.

[9] Su alcuni dei differenti approcci nazionali alla lotta alla disinformazione cfr.: J. Charney, *Fake News under Siege: A Century of Regulation in Chile*; A. Park, *The Battle against Disinformation: Legislative Challenges in South Korea*; G. Bhatia, *Disinformation, Misinformation and Democracy: An Indian Constitutional Perspective*; And J. Botha, *Disinformation and Democracy in Africa and South Africa*, tutti in R.J. Krotoszynski, Jr., A. Koltay, C. Garden (eds.), *Disinformation, Misinformation and Democracy*, Cambridge, Cambridge University Press, 2024. V. anche: M. Milanovic, P. Webb, *False Speech,* in A. Clooney, D. Neuberger (eds.), *Freedom of Speech in International Law*, Oxford, OUP, 2024. Per comprendere la diversità delle politiche legislative adottate dai Paesi occidentali per affrontare la disinformazione v. Organization for Economic Co-operation and Development (OECD), *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, (Paris: OECD Publishing, 2024), available at: https://doi.org/10.1787/d909ff7a-en.

[10] Su tale concetto v. ampiamente e con un approccio comparato: M. Milanovic, P. Webb, *False Speech*, in A. Clooney, D. Neuberger (eds.), *Freedom of Speech in International Law*, OUP, Oxford, 2024.

[11] Definizione data nel 2018 da High-Level Expert Group on Fake News and On-

l'elemento soggettivo dell'intenzionalità e quello oggettivo del danno sistemico. Proprio questo inquadramento consente di distinguere la disinformazione dalla *misinformation*, ossia dalla circolazione inconsapevole di informazioni errate, evitando il rischio di una repressione generalizzata delle falsità e limitando l'intervento giuridico ai casi in cui sia concretamente compromesso il funzionamento dell'ordine democratico[12]. Al riguardo l'Unione europea ha più volte ribadito che la disinformazione, in quanto tale, non può essere considerata illegale, ma legale e dannosa[13]. Questo approccio riflette una concezione della libertà di espressione come diritto non assoluto, ma bilanciabile con altri interessi di rango costituzionale. In particolare la giurisprudenza europea ha chiarito che la tutela delle libertà di informazione non può estendersi alla diffusione deliberata di contenuti manifestamente falsi quando questi incidano in modo significativo su valori fondamentali quali la sicurezza pubblica o l'integrità dei processi decisionali[14].

In una simile prospettiva, la natura sistemica della disinformazione emerge sensibilmente nell'ecosistema digitale; un ambiente in cui, da un

line Disinformation, istituito dalla Commissione europea, cfr.: Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Tackling COVID-19 disinformation – Getting the facts right*, JOIN(2020)8 final, p. 4, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *On the European Democracy Action Plan*, COM/2020/790 final, p. 20.

[12] Tra i primi che misero l'accento su queste differenti disfunzioni nella informazione: C. WARDLE, H. DERAKHSHAN, *Information Disorder: Toward an interdisciplinary framework for reasearch and policy making*, Council of Europe report DGI(2017)09, 2017. Di recente v. B. TÖRÖK, *The Fight against Disinformation in the Council of Europe, and the Relevant Case Law of the European Court of Human Rights*, in JR. R.J KROTOSZYNSKI, A. KOLTAY, C. GARDEN (eds.), *Disinformation, Misinformation, and Democracy: Legal Approaches in Comparative Context*, Cambridge University Press, 2025.

[13] La Commissione europea afferma apertamente che l'approccio europeo alla lotta contro la disinformazione è caratterizzato dalla tutela della libertà di espressione e degli altri diritti garantiti dalla Carta dei diritti fondamentali dell'Unione europea e non dalla «criminalizzazione o dal divieto della disinformazione in quanto tale»: v. al riguardo: Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Commission Guidelines on strengthening the Code of Practice on Disinformation*, COM/2021/ 262 final, p. 1.

[14] Corte di Giustizia UE, sent. 8 dicembre 2022, *RE contro Google LLC*, C-460/20, p.to 65, che conferma le conclusioni dell'avvocato generale Pitruzzella del 7 aprile 2022, p.to 30. *Contra* il sistema americano: cfr. E. VOLOKH, *When Are Lies Constitutionally Protected?*, 22-10 Knight First Amend.Inst., in knightcolumbia.org, 19 ottobre 2022.

lato, le sovrane logiche algoritmiche delle piattaforme privilegiano contenuti polarizzanti, dall'altro, la velocità di propagazione delle informazioni supera i tempi della verifica e, infine, dove le strategie comunicative si fondano su una sofisticata ibridazione tra elementi veritieri e costruzioni manipolative. L'insieme di tutti questi fattori non solo amplificano la portata del fenomeno, ma incidono sulla qualità epistemica dello spazio pubblico, cioè sulla capacità dei cittadini di accedere a informazioni affidabili e, per conseguenza, di formare opinioni consapevoli. Ne deriva una concezione della disinformazione come pratica organizzata e strategica di manipolazione dell'informazione che non si esaurisce nel singolo contenuto, ma opera in modo diffuso e cumulativo, alterando le condizioni stesse del dibattito democratico e mettendo in discussione i presupposti conoscitivi su cui esso si fonda[15]. In ragione di tutto ciò, dunque, la rilevanza giuridica della disinformazione non può essere compresa appieno senza considerare il contesto tecnologico in cui essa si sviluppa. Le piattaforme digitali, lungi dall'essere semplici intermediari neutrali, svolgono un ruolo attivo nella selezione, gerarchizzazione e diffusione dei contenuti. In particolare, i sistemi algoritmici che regolano la visibilità delle informazioni tendono a privilegiare contenuti ad alta capacità di *engagement,* spesso coincidenti con quelli più polarizzanti o emotivamente rilevanti. A ciò si aggiunge l'impatto crescente dell'intelligenza artificiale, che consente la produzione automatizzata di contenuti sempre più sofisticati e difficilmente distinguibili da quelli autentici. Come evidenziato nel quadro normativo europeo, tali tecnologie sono in grado di incidere profondamente sulla percezione della realtà, rendendo sempre più labile il confine tra vero e falso. Ne deriva che la disinformazione non può essere affrontata esclusivamente sul piano dei contenuti, ma richiede un intervento sulle infrastrutture tecnologiche che ne rendono possibile la diffusione. È proprio questa consapevolezza che ha guidato l'evoluzione del modello normativo europeo.

3. Disinformazione e guerra ibrida

Negli ultimi anni, la disinformazione è stata progressivamente ricondotta, anche nel discorso giuridico, all'ambito della sicurezza, venendo qualificata come uno delle principali armi della guerra moderna, la *c.d.*

[15] Al riguardo v. S. Sassi, A. Sterpa (a cura di), *Minacce ibride alla sicurezza nazionale. Disinformazione e migrazioni*, Editoriale Scientifica, Napoli, 2025.

guerra ibrida. Quest'ultima si configura come una forma di conflitto che combina mezzi militari e non militari, collocandosi in una dimensione in cui lo spazio cognitivo assume un rilievo pari, se non superiore, a quello fisico. In tale prospettiva, le campagne di disinformazione condotte da attori statali e non statali mirano a sfruttare le vulnerabilità intrinseche delle democrazie liberali – fondate sull'apertura del dibattito pubblico e sulla libertà di espressione – al fine di erodere la fiducia nelle istituzioni, amplificare le divisioni sociali e politiche e influenzare processi elettorali e decisioni pubbliche[16].

Queste operazioni si distinguono per un elevato grado di coordinamento e per la capacità di integrare molteplici dimensioni – mediatica, digitale, economica e simbolica – dando luogo a strategie complesse e multilivello. Emblematiche, in tal senso, sono le operazioni attribuite alla Federazione Russa, che combinano l'uso di media tradizionali (quali RT), reti sociali, influencer e *bot,* insieme ad azioni fisiche come sabotaggi o provocazioni simboliche[17]. Particolarmente rilevante è la logica della sincronizzazione tra eventi materiali e narrazioni digitali: episodi di entità anche limitata, come intrusioni di droni, vengono rapidamente amplificati nello spazio informativo online, generando panico, disorientamento e sfiducia prima ancora che sia possibile una verifica dei fatti. In questo contesto, la disinformazione opera come un fattore di erosione interna e di destabilizzazione strategica, capace di incidere profondamente sulla percezione pubblica e sui processi decisionali. In questo senso il fenomeno *de quo* non può più essere considerato un mero problema comunicativo o informativo, ma come uno strumento di politica estera e di sicurezza, inserito a pieno titolo nelle dinamiche della competizione geopolitica contemporanea e nella più ampia riflessione sull'autonomia strategica dell'Unione europea.

4. Il modello normativo europeo e le sue criticità

Di fronte a tali sfide, l'Unione europea si distingue, rispetto ad altri

[16] V. S. SASSI, *Il ruolo della disinformazione nelle moderne strategie di guerra*, in E. IMPARATO, G. GIORGINI PIGNATIELLO (a cura di), *La libertà di espressione nel diritto comparato tra stato di diritto e stati di emergenza*, Giappichelli, Torino, 2024.

[17] Interessante il recente rapporto a cura di W. BROWN, J. KOBZOVA, N. POPESCU, J.I. TORREBLANCA, *From Shield to Sword: Europe's offensive Strategy for the Hybrid Age*, European Council on Foreign Relations, March 2026.

ordinamenti, per aver sviluppato un quadro normativo articolato[18], che trova i suoi pilastri principali nel Digital Services Act (DSA) e nell'AI Act[19].

Il DSA segna un passaggio significativo da un modello di autoregolamentazione a un sistema di responsabilità graduata per gli intermediari digitali. Esso introduce obblighi di due diligence volti a identificare, valutare e mitigare i rischi sistemici derivanti dall'uso delle piattaforme, tra cui la disinformazione[20].

Tuttavia, tale modello presenta una caratteristica peculiare: la gestione del rischio è in larga misura affidata agli stessi operatori privati, ai quali viene riconosciuta un'ampia discrezionalità nell'adozione delle misure necessarie. Se da un lato ciò consente una maggiore flessibilità, dall'altro solleva interrogativi significativi in termini di legittimazione democratica e tutela dei diritti fondamentali. Analoga logica si ritrova nell'AI Act, che affronta il problema della disinformazione sotto il profilo tecnologico, adottando un approccio basato sulla classificazione dei rischi[21]. Anche in

[18] In generale, sulle previsioni del pacchetto normativo digitale dell'Unione europea e sui suoi obiettivi, cfr. B. Casarotti, *La politica europea sul digitale: ancora molto rumore*, in *Riv. Trim. Dir.Pubbl.*, 4, 2022; G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. Trim. Dir. Pubbl.*, 4, 2022; L. Torchia, *Lo Stato digitale. Una introduzione*, il Mulino, Bologna, 2023; ID., *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. Trim. Dir. Pubbl.*, 4, 2022. Molti critici C. Novelli, L. Floridi, S. Larsson, M. Taddeo, S. L. Winter nel paper dal titolo: *The Artificial in "Artificial Intelligence": How Imagination Shapes AI Regulation*, pubblicato nel marzo 2026 dal Center for Digital Ethics.

[19] Su cui, v. il C. Camardi (a cura di), *La via europea per l'intelligenza artificiale*, Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche – Ca' Foscari Venezia, 25-26 novembre 2021, vol. 1, Wolters & Kluwers, Milano, 2022; T.E. Frosini, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. Inf.*, 2022 e D.U. Galetta, *Human-stupidy-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *federalismi.it*, 5, 2023.

[20] Sul DSA, tra i contributi più recenti, cfr. C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quad. cost.*, 3, 2023; E. Longo, *"Digital Services Act" – Libertà di informazione. Libertà di informazione e lotta alla disinformazione nel "Digital Services Act"*, in *Giorn. Dir. amm.*, 6, 2023; F. Casolari, *Il "Digital Services Act" e la costituzionalizzazione dello spazio digitale europeo*, in *Giur. it*, 2, 2024; M.C. Girardi, *Libertà e limiti della comunicazione nello spazio digitale*, in *federalismi.it*, 17, 2024; A. Iannotti, *Libertà di espressione e valori democratici alla prova dei social media: il DSA e un nuovo caso TikTok europeo*, in *federalismi.it*, 2, 2025.

[21] A livello generale: cfr. V. D'Antino, *L'approccio basato sul rischio nell'AI: un nuovo paradigma di regolazione dell'intelligenza artificiale*, in *federalismi.it*, 2025 e C. Rudschies, I. Schneider, *The Long and Widing Road to Bans for Artificial Intelligence: From Public Pressure and Regulatory Initiatives to the EU AI Act*, in *Digital Society*, 4, 2025.

questo caso, l'obiettivo non è quello di vietare in modo generalizzato determinate pratiche, ma di regolarne l'uso in funzione della loro capacità di incidere sui diritti fondamentali[22]. Nel loro complesso, tali strumenti delineano un modello di "costituzionalismo digitale"[23], in cui l'attenzione si sposta dai contenuti alle infrastrutture che ne condizionano la diffusione. Ciò rappresenta indubbiamente un'evoluzione significativa, ma non priva di criticità. Sicché, nonostante l'ambizione del quadro normativo delineato dall'ordinamento europeo, alcuni limiti strutturali ne mettono in discussione l'efficacia. In primo luogo, l'approccio europeo appare ancora fortemente orientato alla difesa, basato su strumenti quali il *fact-checking* e l'alfabetizzazione digitale. Sebbene tali misure siano necessarie, esse risultano spesso insufficienti di fronte a campagne di disinformazione altamente coordinate e sostenute da attori statali. In secondo luogo, la frammentazione istituzionale dell'Unione europea rende difficile una risposta tempestiva e coordinata. Le competenze sono distribuite tra diversi livelli di governo e tra una pluralità di attori, con il rischio di creare vuoti operativi. Infine, il ruolo centrale attribuito alle piattaforme digitali solleva questioni di natura costituzionale. La delega a soggetti privati del compito di bilanciare diritti fondamentali in uno spazio pubblico digitale comporta il rischio di fenomeni quali l'opacità decisionale, l'eccesso di rimozione dei contenuti e la compressione indiretta della libertà di espressione[24]. Alla luce delle criticità emerse, appare sempre più evidente la necessità di un'evoluzione del modello europeo. In particolare, si impone il superamento di una logica puramente reattiva, a favore di un approccio più proattivo e integrato. Ciò implica, da un lato, un rafforzamento delle capacità di coordinamento tra gli Stati membri e le istituzioni europee; dall'altro, lo sviluppo di strumenti in grado di incidere sulle dinamiche economiche e tecnologiche che alimentano la disinformazione.

[22] L'esempio più significativo dell'IA sulla disinformazione è il *deepfake*: su questo tema cfr.: M.R. SHOAIB, Z. WANG, M. TALEBY AHVANOOEY, J. ZHAO, *Deepfake, Misinformation, and Disinformation in the Era of Frontier AI, Generative AI, and Large AI Models*, in *International Conference on Computer Applications*, 2023; M.V. MALINCONI, *A War to Reality: deepfake e profili di sicurezza*, in S. SASSI, A. STERPA (a cura di), *op. cit*.; E. NURULLAH, B. SUHEYL*, Deepfake Disinformation,* 6 *Digital L. Rev.* 321, 2024.

[23] Sul costituzionalismo digitale v. per tutti: T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. Inf*., 2020,

[24] V. ZENO ZENCOVICH, *Big data e epistemologia giuridica*, e A. Stazi, *Legal big data: prospettive applicative in ottica comparatistica*, entrambi nel vol. a cura di S. FARO, T.E. FROSINI, G. PERUGINELLI, *Dati e algoritmi. Diritto e diritti nella società digitale*, il Mulino, Bologna, 2020.

Alcune proposte avanzate in ambito strategico suggeriscono la necessità di affiancare alle misure difensive anche forme di intervento più incisive, volte a disarticolare le reti di disinformazione e a contrastare attivamente le narrazioni ostili. Si tratta di un passaggio delicato, che richiede tuttavia una riflessione approfondita sulle implicazioni giuridiche e politiche di tali strumenti.

5. Alcune conclusioni

La disinformazione nell'ecosistema digitale europeo si configura come una sfida complessa e multidimensionale, che mette alla prova la capacità delle democrazie liberali di adattarsi a un contesto in rapido mutamento.[25]

L'approccio europeo, fondato sul bilanciamento tra libertà di espressione e tutela dell'ordine democratico, rappresenta un tentativo avanzato di governare tale fenomeno senza rinunciare ai valori fondamentali. Tuttavia, la crescente sofisticazione delle tecniche di disinformazione e la loro integrazione in strategie di guerra ibrida rendono evidente la necessità di un ulteriore sviluppo. La questione centrale non è più se intervenire, ma come farlo in modo coerente con i principi dello Stato di diritto. In questo senso, la sfida della disinformazione si rivela, in ultima analisi, una sfida per il costituzionalismo contemporaneo[26]: quella di garantire le condizioni di un dibattito pubblico libero e informato in un ambiente tecnologico che tende, strutturalmente, a comprometterle[27].

[25] Sullo stato di crisi che vive la democrazia, le principali difficoltà e le prospettive odierne, cfr. S. Cassese, *La democrazia e i suoi limiti*, Mondadori, Milano, 2017. Sull'impatto che le tecnologie riservano cfr. A. Simoncini, *Sovranità e potere nell'era digitale*, in T. E. Frosini, O. Pollicino, E. Apa, M. Bassini, (a cura di), *op. cit*.

[26] V. T.E. Frosini, *Il costituzionalismo nella società tecnologica*, cit. Per un abbinamento costituzionalismo e disinformazione cfr. S. Sassi, *Disinformazione contro Costituzionalismo*, cit.

[27] Interessanti al riguardo: H.A. Sale, *Monitoring Facebook*, in 12 *Harv. Bus. L. Rev.* 439, 2022 e L.G. Jacobs, *Misinformation, Social Media, and Opportunities for Content-Based Regulation within the Constraints of the United States Constitution's Free Speech Guarantee,* 55 *U. Pac. L. Rev.* 277, 2024.

PROSPETTIVE OPERATIVE

LA DIMENSIONE COGNITIVA DELLA GUERRA IBRIDA

Andrea Manciulli [*]

SOMMARIO: 1. La lunga durata della guerra cognitiva. – 2. Le democrazie liberali come spazi esposti. – 3. Russia, Sahel e Mediterraneo: una strategia multilivello. – 4. Il conflitto ucraino come punto di sintesi: dalla guerra ibrida alle sue evoluzioni. – 5. Italia ed Europa di fronte alla nuova realtà strategica.

1. *La lunga durata della guerra cognitiva*

Il rapporto tra comunicazione e uso della forza affonda le sue radici ben prima dell'epoca contemporanea e, osservato in una prospettiva di lunga durata, appare come una costante della storia militare. Ogni conflitto armato, infatti, non si esaurisce nella sola dimensione operativa o cinetica, ma include anche una componente simbolica e psicologica determinante.

La percezione dell'insicurezza, la reputazione del nemico e la costruzione della paura collettiva hanno inciso, in ogni epoca, sugli esiti delle campagne militari tanto quanto il potenziale bellico effettivamente dispiegato sul campo.

Già nelle guerre dell'età moderna la fama di determinati reparti precedeva il loro arrivo sul campo di battaglia. I Lanzichenecchi, ad esempio, erano circondati da una reputazione di brutalità che amplificava l'impatto della loro presenza ben oltre le capacità militari concretamente impiegate. L'avanzata di queste truppe alterava il morale delle popolazioni e degli eserciti avversari prima ancora dello scontro diretto e, in molti casi, bastava la notizia del loro arrivo per generare panico e disorganizzazione. Si trattava di una forma embrionale di pressione psicologica: sebbene limitata nello spazio e nella velocità di diffusione, era già in grado di condizionare profondamente il clima d'opinione entro il quale si svolgeva il conflitto.

La principale linea di discontinuità rispetto al presente riguarda la scala e la rapidità con cui operano questi meccanismi. L'evoluzione tecnologica – dalla stampa alla radio, dalla televisione fino alle piattaforme

[*] Direttore delle Relazioni istituzionali di Med-Or Italian Foundation.

digitali – ha ampliato progressivamente la portata delle narrazioni e delle percezioni collettive. L'ecosistema informativo contemporaneo permette di raggiungere simultaneamente milioni di individui, orientarne le sensazioni quasi in tempo reale e generare onde emotive in grado di influenzare il funzionamento di intere società.

La guerra cognitiva rappresenta dunque l'evoluzione sistemica di una componente sempre presente nella competizione tra grandi attori internazionali: il cosiddetto *storytelling*. Negli ultimi anni questa dimensione è stata analizzata con crescente attenzione nella letteratura strategica e nei documenti di pianificazione delle organizzazioni di sicurezza occidentali, che hanno iniziato a descriverla come una componente strutturale delle nuove forme di conflitto. Essa non sostituisce la dimensione militare tradizionale, ma la integra e ne amplifica gli effetti.

In questo nuovo paradigma, la forza di un Paese non si misura più soltanto in divisioni corazzate o sistemi missilistici, ma anche nell'influenza esercitata sul dibattito pubblico, nella possibilità di frammentare il consenso e di indebolire la fiducia nelle istituzioni.

Il terreno decisivo si sposta sul piano delle dinamiche collettive e sulla tenuta psicologica delle società. Quando il clima di insicurezza resta circoscritto, l'impatto degli eventi tende a restare limitato; quando invece si diffonde rapidamente attraverso le reti digitali, amplificato dalla logica algoritmica delle piattaforme, può produrre conseguenze sproporzionate rispetto all'evento originario. Un attacco a bassa intensità può generare paralisi urbane; un episodio isolato può trasformarsi in una crisi nazionale capace di influenzare decisioni politiche e orientamenti dell'opinione pubblica.

In questa prospettiva, la dinamica per cui Davide riesce a mettere sotto pressione Golia non appartiene più soltanto alla dimensione simbolica della storia, ma descrive una caratteristica concreta dei rapporti di potere contemporanei.

Lo *storytelling* bellico, pertanto, non opera solo sul piano rappresentativo, ma, permeando la realtà, interviene direttamente nella configurazione del conflitto e contribuisce a ridefinire gli equilibri tra attori asimmetrici. Questa dimensione richiama, in forma aggiornata, intuizioni già presenti nella riflessione strategica classica, secondo cui la guerra si gioca non solo sul piano materiale, ma anche sulla percezione, sulla volontà e sulla capacità di orientare il comportamento dell'avversario.

Diventa quindi essenziale interrogarsi su quali sistemi politici risultino più sensibili a queste forme di confronto.

2. *Le democrazie liberali come spazi esposti*

La competizione cognitiva non incide allo stesso modo su tutti i sistemi politici. Le democrazie liberali presentano una particolare esposizione strutturale che deriva dai principi stessi su cui si fondano: libertà di espressione, pluralismo informativo e apertura del confronto pubblico.

Nei sistemi autoritari, il controllo centralizzato della comunicazione consente allo Stato di modulare e contenere l'impatto di narrazioni destabilizzanti. In contesti in cui l'informazione è rigidamente filtrata e centralizzata, la diffusione incontrollata della paura o della disinformazione può essere limitata attraverso interventi diretti delle autorità politiche. Al contrario, nelle società aperte, la circolazione delle informazioni avviene in modo libero e decentralizzato. Sebbene tale caratteristica rappresenti una ricchezza democratica, essa genera spazi di vulnerabilità che attori ostili possono agevolmente sfruttare.

La questione centrale non riguarda la libertà in sé, ma l'asimmetria tra sistemi aperti e attori che operano senza vincoli equivalenti. Stati o reti transnazionali possono utilizzare le libertà garantite nelle società occidentali per diffondere disinformazione, alimentare la polarizzazione politica e minare la fiducia nelle istituzioni, senza essere esposti a pressioni analoghe nei propri contesti interni.

A questo elemento si aggiunge una trasformazione significativa dei tempi del dibattito pubblico. L'informazione digitale ha accelerato il ciclo dell'attenzione collettiva, producendo un flusso continuo di emergenze percepite. L'agenda pubblica tende, infatti, a essere dominata da eventi immediati e spesso episodici, mentre le questioni strutturali di lungo periodo faticano a trovare spazio nel confronto politico e mediatico.

Le operazioni ibride sfruttano in modo sistematico queste caratteristiche: moltiplicano i fronti di tensione, frammentano l'attenzione e producono una saturazione informativa che rende difficile distinguere i fenomeni di fondo dagli episodi contingenti. Le società democratiche finiscono così per trovarsi in una condizione di reattività permanente, mentre gli attori ostili riescono a pianificare le proprie iniziative seguendo una prospettiva di lungo periodo.

A questa dinamica si aggiunge oggi la sofisticazione tecnica delle modalità di manipolazione dell'informazione. L'uso di siti che simulano testate giornalistiche, tecniche di reindirizzamento per aggirare i controlli e reti coordinate di *account* automatizzati (*bot*) consente di amplificare artificialmente contenuti polarizzanti e di raggiungere pubblici differenziati con messaggi mirati, aumentando l'efficacia delle campagne di influenza.

Parallelamente, le scadenze elettorali rappresentano momenti di particolare vulnerabilità. Le campagne di disinformazione tendono a intensificarsi in prossimità delle consultazioni, con l'obiettivo di condizionare la percezione dei candidati e delegittimare il processo democratico.

Episodi recenti, peraltro, mostrano come tali campagne possano incidere sul dibattito pubblico anche in Europa, orientando la percezione di temi quali energia, sicurezza e gestione dei flussi migratori.

Le dinamiche osservate evidenziano una forte capacità adattiva degli attori ostili. Le misure di contrasto adottate dalle democrazie producono spesso effetti di breve periodo, ma vengono rapidamente aggirate attraverso la creazione di nuovi canali e piattaforme, evidenziando un divario tra la rigidità normativa dei sistemi democratici e la flessibilità operativa degli attori che li sfidano.

L'evoluzione delle tecnologie digitali, inclusi i sistemi di intelligenza artificiale generativa, è destinata a rendere questi fenomeni ancora più pervasivi, aumentando la capacità di produrre contenuti credibili e difficilmente distinguibili da fonti autentiche.

3. Russia, Sahel e Mediterraneo: una strategia multilivello

Un esempio particolarmente significativo di questa evoluzione può essere osservato nell'approccio adottato negli ultimi anni dalla Russia, che combina strumenti militari convenzionali, azioni indirette, pressione informativa, proiezione paramilitare e proiezione ideologica. Si tratta di un approccio che riflette una concezione del confronto tra potenze nella quale strumenti diversi vengono integrati all'interno di un disegno complessivo capace di operare simultaneamente su più piani.

L'aggressione all'Ucraina rappresenta la manifestazione più evidente di questa impostazione, ma non ne esaurisce la portata. Parallelamente al conflitto sul fronte europeo, Mosca ha rafforzato la propria presenza in diverse aree di instabilità che assumono un peso crescente negli equilibri geopolitici globali e nella sicurezza del continente europeo. La lezione degli ultimi decenni mostra, inoltre, che la superiorità tecnologica e la capacità di colpire a distanza non sono sufficienti a determinare l'esito politico di un conflitto. Le esperienze in Afghanistan, Iraq e Libia hanno dimostrato che senza controllo del territorio, comprensione del quadro sociale e capacità di stabilizzazione, l'uso della forza rischia di produrre vuoti di potere e instabilità prolungata.

Tra queste regioni, il Sahel occupa una posizione di particolare rilie-

vo. Negli ultimi anni Paesi come Mali, Burkina Faso e Niger sono stati attraversati da profonde crisi istituzionali culminate in colpi di Stato militari e in una ridefinizione delle relazioni con i partner occidentali. In questo contesto, la Russia ha consolidato la propria presenza attraverso strumenti indiretti, mediante strutture paramilitari già riconducibili all'esperienza del gruppo Wagner e alle reti che ne hanno assorbito il capitale operativo e relazionale.

Questa presenza non si limita alla dimensione militare, ma si intreccia con attività economiche informali, concessioni minerarie, sfruttamento di risorse naturali e reti di traffici illegali. Ne deriva un sistema di influenza che lega sicurezza, accesso alle risorse e penetrazione politica, rafforzando il posizionamento di Mosca in una delle aree più fragili del continente africano.

Ciò che rende particolarmente incisivo questo modello non è una superiorità intrinseca, ma la capacità di integrare strumenti diversi – militari, economici e informativi – all'interno di una strategia coerente nel tempo, sfruttando le vulnerabilità dei sistemi aperti, mentre le risposte europee restano spesso frammentate e reattive.

Il legame tra piano economico e operazioni informative appare evidente: le attività estrattive legate a oro, diamanti e uranio si accompagnano a campagne narrative che enfatizzano i temi dello sviluppo, della sovranità e della stabilità. La presenza militare o paramilitare viene così presentata come garanzia di sicurezza, mentre i benefici economici vengono utilizzati come elemento di legittimazione politica nei confronti delle popolazioni locali.

Il Sahel costituisce inoltre uno snodo cruciale di grande rilevanza per l'Europa. L'instabilità cronica della regione alimenta flussi migratori che attraversano il Nord Africa e raggiungono le coste del Mediterraneo, facendo sì che crisi apparentemente lontane dai confini dell'Unione europea producano effetti diretti sulla stabilità politica e sociale del continente.

Il Mediterraneo allargato si configura quindi come uno spazio di primaria rilevanza geopolitica, nel quale il fronte meridionale europeo non può essere separato dalle dinamiche che attraversano il fianco orientale e l'Artico. Pressione migratoria, presenza di gruppi jihadisti, fragilità istituzionale, traffici illeciti e rivalità tra potenze esterne contribuiscono a trasformare l'area in uno dei principali fronti della sicurezza europea.

In questa prospettiva, l'instabilità del Sahel non rappresenta un fenomeno periferico, ma una componente di un sistema di interdipendenze che collega Africa subsahariana, Nord Africa ed Europa. In tale contesto,

la dimensione informativa assume un ruolo centrale: narrazioni antioccidentali, campagne di disinformazione e operazioni di influenza mirano a rafforzare sentimenti di sfiducia nei confronti dell'Occidente, favorendo al tempo stesso la legittimazione di nuovi partner politici e militari.

Queste operazioni si appoggiano a un'architettura articolata che comprende piattaforme digitali, media locali e *influencer* capaci di radicare nel tempo specifiche narrazioni.

L'obiettivo non è necessariamente un'espansione territoriale diretta, ma un progressivo indebolimento della coesione europea.

Le operazioni di influenza si caratterizzano inoltre per una marcata differenziazione dei target: in Europa si concentrano su migrazioni e crisi economiche, mentre nel Sahel fanno leva su sovranità e anticolonialismo, aumentando così la loro efficacia. Alimentare divisioni interne e tensioni nel dibattito pubblico contribuisce, quindi, a indebolire la convergenza necessaria affinché l'Unione europea possa agire come attore politico unitario.

A queste trasformazioni si aggiunge il peso dell'Artico. Lo scioglimento dei ghiacci apre nuove rotte commerciali e nuove opportunità di sfruttamento energetico, trasformando la regione in uno spazio di crescente interesse strategico. In questo ambito, la Russia ha investito in modo significativo nel rafforzamento della propria presenza militare, consolidando infrastrutture, basi e capacità di controllo delle rotte marittime emergenti.

Queste evoluzioni riflettono una trasformazione più ampia delle modalità di confronto tra attori statali: la storia militare mostra come ogni epoca sia attraversata da momenti di rottura nei modelli operativi e nelle logiche dello scontro. In diverse fasi storiche l'innovazione tattica ha consentito ad attori più agili di mettere in difficoltà avversari apparentemente più potenti. Nella prima metà del Cinquecento, ad esempio, Giovanni delle Bande Nere seppe adattare strumenti e modalità operative a un contesto militare in rapido mutamento.

L'alleggerimento dell'equipaggiamento, la maggiore mobilità delle truppe e una conduzione della manovra più flessibile rispetto agli schemi tradizionali consentivano di sorprendere avversari ancora legati a modelli di combattimento più rigidi.

Il riferimento non riguarda naturalmente le tecniche militari in senso stretto, ma il principio che ne deriva: l'attitudine ad adattarsi rapidamente ai mutamenti dello scenario operativo.

Oggi tale trasformazione non riguarda soltanto le modalità tattiche del combattimento, ma l'intero spazio dello scontro tra potenze. Stru-

menti militari, leve di influenza, operazioni informative e azioni indirette vengono integrate all'interno di modelli di azione articolati, nei quali il campo di battaglia tende a sovrapporsi allo spazio politico, sociale e comunicativo delle società contemporanee.

In questa cornice, le aree di crisi non rappresentano teatri isolati, ma nodi di una rete di interdipendenze strategiche.

4. *Il conflitto ucraino come punto di sintesi: dalla guerra ibrida alle sue evoluzioni*

Il conflitto in Ucraina, nella fase apertasi con l'invasione su larga scala del febbraio 2022, può essere letto come un punto di sintesi e di accelerazione delle dinamiche proprie della guerra ibrida contemporanea, nel quale tendenze già emerse negli anni precedenti trovano una forma compiuta e sistemica. Non si tratta, tuttavia, di una rottura netta rispetto al passato: la campagna russa nei confronti dell'Ucraina aveva già assunto una configurazione ibrida a partire dal 2014, con l'annessione della Crimea e il sostegno alle formazioni separatiste nel Donbass.

Quella prima fase aveva, infatti, mostrato un insieme articolato di strumenti integrati – impiego di forze non dichiarate, pressione energetica come leva geopolitica, operazioni di influenza volte a indebolire la coesione delle risposte occidentali – prefigurando l'architettura del conflitto successivo. La *escalation* del 2022 ha aggiunto a questo repertorio una dimensione convenzionale di elevata intensità, integrando operazioni cinetiche, guerra elettronica, attacchi alle infrastrutture critiche e campagne informative su scala globale.

Ciò che rende il teatro ucraino un caso paradigmatico non è il ricorso simultaneo a strumenti diversi, elemento già presente in conflitti precedenti, quanto il livello di integrazione tra dominio fisico e dominio cognitivo e la rapidità con cui gli attori coinvolti hanno adattato le proprie modalità operative. La guerra si configura così come un sistema unitario nel quale dimensione militare, informativa e tecnologica risultano sempre più interdipendenti.

Sul piano cognitivo, il conflitto ucraino evidenzia un livello di integrazione e immediatezza senza precedenti nella relazione tra campo di battaglia e spazio informativo globale. La dimensione narrativa non si sviluppa più in una fase successiva agli eventi, ma accompagna in tempo reale lo svolgimento delle operazioni, diventando essa stessa parte integrante della dinamica del conflitto.

Ogni episodio bellico viene immediatamente trasformato in contenuto comunicativo, selezionato, interpretato e diffuso secondo logiche che rispondono a obiettivi strategici. La gestione della percezione assume così un valore operativo, incidendo sulla formazione del consenso interno, sulla tenuta delle alleanze e sulla legittimazione internazionale delle parti coinvolte.

La Russia ha impiegato in modo sistematico questa dimensione, articolando narrazioni differenziate in funzione dei pubblici di riferimento: all'interno, attraverso un sistema informativo fortemente controllato, costruendo una rappresentazione del conflitto funzionale alla mobilitazione del consenso; all'esterno, e in particolare nei confronti del Sud globale, promuovendo letture volte a relativizzare le responsabilità dell'aggressione e a spostare l'attenzione sugli effetti economici delle sanzioni occidentali.

L'Ucraina, parallelamente, ha sviluppato una capacità di comunicazione strategica di notevole efficacia. La *leadership* politica è stata trasformata in un vettore diretto di narrazione internazionale, con un uso continuo e mirato degli strumenti digitali per mantenere alta l'attenzione e consolidare il sostegno esterno. In questo senso, la resilienza cognitiva si configura come una risorsa strategica a tutti gli effetti, capace di incidere in modo significativo sulla tenuta complessiva dello sforzo bellico.

Il conflitto ha inoltre accelerato l'integrazione operativa di tecnologie già disponibili, ma finora impiegate in modo parziale o sperimentale. L'uso diffuso di droni commerciali adattati a fini militari, l'impiego di dati satellitari di origine privata, i sistemi di riconoscimento visivo e le operazioni di guerra elettronica su frequenze civili hanno contribuito ad abbassare la soglia di accesso a capacità avanzate.

Questa evoluzione riduce il vantaggio esclusivo delle grandi potenze e sposta progressivamente l'attenzione verso altri fattori: la velocità di adattamento, la qualità del processo decisionale e la capacità di integrare informazioni provenienti da fonti eterogenee. In questo contesto, la dimensione cognitiva non riguarda soltanto l'influenza esercitata sull'avversario, ma investe direttamente i meccanismi interni di elaborazione e gestione dell'informazione.

La capacità di selezionare, interpretare e tradurre in azione operativa un flusso continuo di dati rappresenta un elemento sempre più centrale della competizione strategica.

In questo quadro, l'evoluzione dei sistemi di intelligenza artificiale introduce un ulteriore fattore di trasformazione, consentendo di analizzare grandi volumi di dati in tempo reale, di generare contenuti sintetici

altamente credibili e di modulare le operazioni informative in funzione di pubblici specifici, ampliando così la portata e la precisione della dimensione cognitiva del conflitto.

L'osservazione del conflitto ucraino consente di individuare anche alcune tendenze destinate a condizionare l'evoluzione della guerra ibrida nei prossimi anni. La prima riguarda l'ampliamento del numero di attori in grado di condurre operazioni complesse. Tecnologie e strumenti un tempo riservati a un numero limitato di Stati sono oggi accessibili a una platea più ampia, che include attori non statali, reti transnazionali e soggetti privati.

Questa trasformazione produce un ambiente strategico più frammentato e meno prevedibile, nel quale i meccanismi tradizionali di deterrenza risultano più difficili da applicare. La possibilità di operare al di sotto della soglia del conflitto aperto, unita alla difficoltà di attribuzione, riduce l'efficacia delle risposte basate su schemi simmetrici.

Una seconda tendenza riguarda l'evoluzione dello spazio cognitivo verso forme di crescente personalizzazione delle operazioni di influenza. La possibilità di costruire campagne mirate non solo a gruppi sociali, ma a segmenti sempre più specifici della popolazione, fino al livello individuale, introduce un salto qualitativo rispetto alle forme tradizionali di propaganda e pone sfide significative ai sistemi di difesa delle democrazie.

Una terza traiettoria riguarda l'estensione del campo di competizione alle infrastrutture critiche delle società contemporanee. Sistemi energetici, reti di comunicazione, catene logistiche e infrastrutture finanziarie costituiscono ambiti nei quali operazioni ibride possono produrre effetti rilevanti senza superare formalmente la soglia del conflitto armato. Ne deriva una progressiva erosione della distinzione tra tempo di pace e tempo di guerra, sostituita da una condizione di competizione continua che si sviluppa su piani interconnessi.

In questo contesto, il conflitto ucraino evidenzia anche il ruolo centrale della coesione politica e della solidità delle alleanze. La tenuta del fronte occidentale, sostenuta da una capacità di coordinamento e da una continuità dell'impegno nel tempo, ha rappresentato un fattore determinante nel contenimento dell'evoluzione del conflitto.

Gli elementi emersi nel contesto ucraino trascendono il caso specifico e si proiettano direttamente sulle scelte strategiche che attendono l'Italia e l'Europa, chiamate a operare in un contesto in cui la competizione si sviluppa in modo permanente tra dimensione materiale e dimensione cognitiva del potere.

5. Italia ed Europa di fronte alla nuova realtà strategica

La crescente integrazione tra dimensioni militari, informative e tecnologiche rende evidente che la sicurezza non può più essere interpretata esclusivamente in termini territoriali. Le trasformazioni in atto nei diversi teatri di crisi – dal fianco orientale europeo al Mediterraneo allargato, dall'Artico al Sahel – producono effetti diretti sulle società europee, rendendo sempre più labile la distinzione tra spazio interno ed esterno, tra minaccia lontana e vulnerabilità prossima.

In questo contesto, difendere i principi della democrazia liberale non significa restringere gli spazi di libertà, ma rafforzare la capacità di tenuta delle società aperte.

La risposta alle operazioni ostili non può consistere nell'adozione di modelli autoritari: una simile scelta rischierebbe di compromettere la qualità delle istituzioni senza offrire un vantaggio strategico duraturo. Diritto, libertà e democrazia costituiscono il fondamento dell'identità europea, ma non possono essere disgiunti dalla capacità politica, industriale e militare di difenderli. In questo senso, la forza non rappresenta l'alternativa ai valori democratici, bensì la condizione della loro tutela.

Alla luce delle dinamiche emerse nei conflitti più recenti, e in particolare nel caso ucraino, la resilienza cognitiva assume un significato pienamente strategico. La capacità di orientarsi in un ambiente informativo complesso, di riconoscere le operazioni di manipolazione e di preservare la qualità dello spazio pubblico diventa un fattore essenziale per la stabilità delle democrazie. La competizione contemporanea si sviluppa, infatti, anche sulla tenuta dei sistemi decisionali e sulla fiducia collettiva che li sostiene.

In questo quadro, il coordinamento europeo nel contrasto alle minacce ibride appare imprescindibile. Le pressioni esercitate su un singolo Stato membro si propagano rapidamente a livello continentale attraverso reti digitali, flussi economici e processi sociali interconnessi. La frammentazione delle risposte nazionali tende a tradursi in un vantaggio per attori che operano secondo logiche di lungo periodo e con elevata flessibilità operativa.

Un ulteriore elemento riguarda la proiezione europea nel Mediterraneo allargato e nel Sahel. In assenza di una presenza strutturata e continuativa, altri attori consolidano progressivamente non solo una presenza militare ed economica, ma anche una capacità di influenza capace di incidere sugli equilibri politici nel medio periodo. Lasciare spazi privi di iniziativa strategica significa, in questo senso, favorire la formazione di assetti destinati a riflettersi direttamente sulla sicurezza del continente.

Per l'Italia, la dimensione mediterranea rappresenta una priorità naturale. La posizione geografica e la profondità storica delle relazioni con la sponda sud rendono il Mediterraneo uno spazio nel quale stabilità, sviluppo e sicurezza risultano strettamente interconnessi. Un approccio efficace richiede dunque politiche capaci di integrare sicurezza, sviluppo sostenibile e partenariato economico, all'interno di una cornice europea coerente. In questa prospettiva, la questione centrale non è scegliere tra autonomia europea e legame transatlantico, ma costruire una capacità effettiva di azione.

La fase attuale può essere interpretata come un momento di transizione tra paradigmi strategici. I modelli tradizionali di risposta mostrano limiti crescenti, mentre le nuove forme di competizione – ibride, tecnologiche e cognitive – non hanno ancora trovato un assetto pienamente consolidato. È in questa fase intermedia che si concentrano le maggiori vulnerabilità, ma anche le opportunità di adattamento.

Nei prossimi decenni, la competizione si svilupperà sempre più su terreni immateriali, nei quali la capacità di integrazione tra dimensione tecnologica, informativa e politica risulterà determinante quanto la forza materiale. In questo scenario, la principale risorsa delle democrazie liberali risiede nella solidità delle istituzioni, nella capacità di mantenere un ecosistema informativo pluralistico e affidabile e nella possibilità di rinnovarsi senza rinunciare ai propri principi.

Trasformare la consapevolezza delle vulnerabilità in un processo di rafforzamento strategico rappresenta una condizione essenziale per affrontare un contesto internazionale sempre più complesso. Mantenere coesione interna, sviluppare una visione di lungo periodo e rafforzare la cooperazione tra alleati diventa quindi decisivo affinché l'Italia e l'Europa possano non solo resistere alle pressioni esterne, ma continuare a contribuire attivamente alla definizione degli equilibri globali futuri.

Y-TRUST: PROGETTARE UN'ARCHITETTURA SOCIO-TECNICA CONTRO IL DISORDINE INFORMATIVO. *INFLUENCER*, *FACT-CHECKING* E MODELLI LINGUISTICI APERTI TRA *GDPR*, *DIGITAL SERVICES ACT* E *AI ACT*

Michele Empler[*]

1. *Premessa*

Ritengo che il primo passo per ragionare seriamente di disinformazione consista nell'abbandonare l'idea, ancora largamente diffusa, che essa rappresenti una patologia individuale del lettore o un vizio morale dell'autore di un singolo contenuto. La ricerca consolidata degli ultimi otto anni indica con sufficiente chiarezza che il fenomeno è un effetto di sistema: dipende da un'infrastruttura informativa, fatta di algoritmi di raccomandazione, di economia dell'attenzione, di asimmetria di velocità fra produzione e verifica, che premia ciò che cattura prima di ciò che documenta[1]. Se questa lettura è corretta, ne discende un corollario operativo non scontato: le contromisure efficaci non possono essere puntuali. Devono essere, a loro volta, architettoniche.

La nostra ipotesi di lavoro è che il progetto «Y-TRUST», un portale che si propone di intermediare la circolazione di notizie verificate

[*] Dottorando di ricerca in "Società in mutamento: politiche, diritti e sicurezza" nell'Università degli Studi della Tuscia.

[1] Cfr. S. VOSOUGHI, D. ROY, S. ARAL, *The Spread of True and False News Online*, in Science, 2018, pp. 1146-1151, in cui gli autori dimostrano, su un *dataset* di circa centoventiseimila storie diffuse su Twitter tra il 2006 e il 2017, che il falso si propaga «*farther, faster, deeper, and more broadly than the truth*» in tutte le categorie tematiche analizzate, con scarti particolarmente pronunciati nelle notizie politiche.

fra un *pool* di *fact-checker*, una rete profilata di *influencer* e un modello linguistico di grandi dimensioni *open-source* ospitato in locale, possa essere assunto come *case-study* utile a problematizzare proprio questa dimensione architettonica. Y-TRUST non è soltanto un progetto: è, ai fini della nostra indagine, un dispositivo socio-tecnico, ossia un assemblaggio eterogeneo di attori umani, componenti tecnologiche, regole giuridiche e norme deontologiche, la cui *funzionalità complessiva* non si lascia ricondurre a nessuna delle sue parti.

Su questa premessa, l'articolo si sviluppa in nove paragrafi che procedono per cerchi concentrici. I primi tre delineano la grammatica concettuale entro cui si situa l'oggetto: la tipologia delle forme del falso (*infra*, §2), lo stato delle contromisure psicologiche e redazionali (*infra*, §3). I tre paragrafi successivi descrivono Y-TRUST nella sua materialità (*infra*, §4), nella scelta tecnica di un modello linguistico aperto e *on-premise* (*infra*, §5) e nella mediazione, insieme strategica e fragile, degli *influencer* (*infra*, §6). Il settimo paragrafo (*infra*, §7) sviluppa l'aspetto a mio giudizio caratterizzante del caso: la convergenza, sullo stesso dispositivo, di tre regimi normativi europei (*GDPR*, *Digital Services Act*, *AI Act*) che non si elidono ma si stratificano. Chiudono il lavoro un paragrafo sui limiti del dispositivo e sulle direzioni di validazione empirica (*infra*, §8) e una sintesi conclusiva (*infra*, §9).

2. *Il quadro concettuale:* mis-*,* dis- *e* mal-information

La prima conseguenza concreta dell'assunzione del disordine informativo come fenomeno di sistema è terminologica. Confondere, come pure accade nella pubblicistica corrente, falso involontario, falso intenzionale e vero strumentalizzato significa progettare contromisure cieche, poiché ciascuna delle tre forme richiede risposte distinte. Il *framework* proposto nel 2017 da Wardle e Derakhshan per il Consiglio d'Europa rimane, a otto anni di distanza, lo strumento più persuasivo per articolare la distinzione e ne assumiamo qui il vocabolario[2].

Sintetizziamo. Per *misinformation* si intende l'informazione falsa diffusa senza intento di danneggiare: la condivisione di una notizia errata

[2] C. WARDLE, H. DERAKHSHAN (a cura di), *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*, Council of Europe, 2017, pp. 20-25. Una sintesi divulgativa aggiornata in C. WARDLE, *Understanding Information Disorder*, First Draft, New York, 2019, pp. 5-12.

che si ritiene in buona fede attendibile è il caso paradigmatico. Per *disinformation* si intende l'informazione falsa o deliberatamente fuorviante diffusa con l'intenzione di danneggiare un individuo, un gruppo, un'organizzazione, un Paese. Per *malinformation* si intende, infine, l'informazione vera diffusa con intento di danneggiare: il *doxing*, la diffusione selettiva di dati personali corretti per pregiudicare la reputazione di una persona, alcune forme di *outing* politico ne sono esempi puntuali.

A questa tripartizione, Wardle aveva già nel 2017 affiancato una tipologia delle forme concrete in cui il contenuto disinformativo si manifesta: satira o parodia, contenuto fuorviante, contesto improprio, contenuto impostore, contenuto manipolato, contenuto fabbricato, connessione falsa. Sette voci che non esauriscono il fenomeno ma che, prese insieme, mettono in evidenza la natura *composita* del problema. Una falsa connessione fra titolo e corpo dell'articolo, per esempio, non è tecnicamente «fabbricazione» di contenuto inesistente, ma ne riproduce la funzione persuasoria con costi marginali quasi nulli per il produttore.

Sul piano della letteratura accademica, la tipologia di Tandoc, Lim e Ling[3] ci permette di apprezzare quanto il concetto stesso di «*fake news*» sia stato oggetto di una decina di definizioni operative concorrenti, dalle quali derivano scelte metodologiche di campionamento e di misura che condizionano radicalmente i risultati di un'indagine. Il *takeaway* analitico è che il vocabolario non è neutro: una piattaforma che si proponga di contrastare il «falso» deve, prima di tutto, decidere quale falso vuole contrastare. Y-TRUST opera, come vedremo, in uno spazio assai più mirato di quello dell'intera famiglia *fake news*: il suo obiettivo dichiarato è l'amplificazione del *verificato*, non la *neutralizzazione* del falso, e la differenza non è semantica.

Su un secondo piano, di tipo strutturale, l'asimmetria fra propagazione del vero e del falso è stata stabilita con accuratezza empirica nello studio di Vosoughi, Roy e Aral[4]. Su un *dataset* di circa centoventiseimila storie verificate o falsificate da sei organizzazioni indipendenti di *fact-checking*, gli autori dimostrano che il falso raggiunge le prime mille per-

[3] E.C. Tandoc Jr., Z.w. Lim, R. Ling, *Defining «Fake News»: A Typology of Scholarly Definitions*, in *Digital Journalism,* 2018, pp. 137-153. Gli autori ricostruiscono trentaquattro contributi pubblicati fra il 2003 e il 2017 e li riconducono a sei tipi: satira, parodia, fabbricazione, manipolazione, pubblicità travestita, propaganda.

[4] S. Vosoughi, D. Roy, S. Aral, *op. cit.*, pp. 1148-1150. Il *dataset* riguarda Twitter tra il 2006 e il 2017 ed è oggi uno dei *benchmark* di riferimento per la letteratura sulla diffusione dell'informazione *online*.

sone fra le sei e le venti volte più velocemente del vero; che la profondità della cascata di condivisione è significativamente maggiore; e che, punto controintuitivo, questa asimmetria non dipende prioritariamente dai *bot*, ma dalla scelta umana di condividere contenuti emotivamente più «sorprendenti», che il falso, libero dal vincolo della realtà, è in grado di confezionare meglio del vero.

Il contesto strutturale è ulteriormente illuminato da due contributi che vanno tenuti in conto. Da un lato l'analisi di Allcott e Gentzkow sulle elezioni statunitensi del 2016, che ha quantificato per la prima volta in modo accurato l'esposizione media degli adulti statunitensi a *fake news* nei tre mesi precedenti il voto[5]: dati che hanno tradotto in metriche il sospetto, sino ad allora qualitativo, che la disinformazione *online* fosse un fattore quantitativamente significativo nella formazione dell'opinione pubblica. Dall'altro la riflessione di Sunstein sulla deriva polarizzante delle piattaforme[6], che pone in continuità il *filter bubble* con tendenze più antiche della comunicazione politica e indica, già nel 2017, la necessità di «cyber-incontri non programmati» con punti di vista diversi dai propri, esattamente ciò che il modello di Y-TRUST tenta di realizzare per via mediata.

Una postilla terminologica è dovuta sull'uso che faremo del concetto di «disinformazione». Nelle pagine che seguono lo impieghiamo, ove non altrimenti specificato, nell'accezione restrittiva del *framework* del Consiglio d'Europa: informazione falsa diffusa con intenzione di danneggiare. Le altre due forme, *misinformation* e *malinformation*, saranno indicate, quando ricorrano, con i loro nomi inglesi e in corsivo. La scelta non è puramente lessicale: assumere il termine «disinformazione» nella sua sola accezione intenzionale impedisce di confondere il problema dell'errore in buona fede, che è prevalentemente un problema di alfabetizzazione informativa, con il problema dell'inganno deliberato, che è prevalentemente un problema di tutela dell'ordine informativo pubblico. Y-TRUST si propone come dispositivo contro la *disinformation* in senso stretto, non come dispositivo di *media literacy*: la distinzione condiziona, come vedremo, la valutazione dei suoi limiti (cfr. *infra*, §8).

Tracciato il vocabolario, possiamo passare alle contromisure.

[5] H. ALLCOTT, M. GENTZKOW, *Social Media and Fake News in the 2016 Election*, in *Journal of Economic Perspectives*, 2017, pp. 211-236. Secondo gli autori, gli adulti statunitensi hanno visto in media una o più fake news nei mesi precedenti il voto e poco più della metà di chi se ne è ricordata vi ha prestato fede.

[6] C.R. SUNSTEIN, *#Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton, 2017, pp. 31-50 e 233-263.

3. *Lo stato del contrasto:* debunking*,* prebunking*,* fact-checking

Le contromisure documentate in letteratura si distribuiscono lungo un asse temporale che ne chiarisce la complementarità e i limiti: a valle l'azione di smentita successiva alla diffusione (*debunking*); a monte la preparazione cognitiva del lettore (*prebunking*, o *inoculation theory*); in tempo reale la verifica condotta nei *feed* dalle piattaforme e dai *fact-checker* terzi. Ciascuna delle tre famiglie ha generato un corpo di evidenza robusto e ciascuna, presa singolarmente, è insufficiente.

Sul versante del *debunking*, la letteratura più aggiornata ha in larga parte ridimensionato, pur senza azzerarlo, il timore di un *backfire effect*, ossia di un effetto di consolidamento del falso indotto dalla sua smentita esplicita; allo stesso tempo ha confermato la persistenza del *continued influence effect*, ossia la capacità di un'informazione errata di continuare a orientare il giudizio anche dopo essere stata esplicitamente ritrattata. *The Debunking Handbook 2020*, redatto da Lewandowsky e da altri ventidue ricercatori, sintetizza il consenso disciplinare in una serie di raccomandazioni operative: presentare la verità prima del falso, ripeterla, ancorarla a un meccanismo alternativo che spieghi *perché* il falso fosse plausibile, e accompagnarla a un'avvertenza esplicita sulla manipolazione subita[7].

Le raccomandazioni del *Debunking Handbook* meritano di essere richiamate con qualche dettaglio in più, perché informano direttamente le scelte operative di Y-TRUST in fase di adattamento del contenuto. La struttura raccomandata della smentita è triplice: enunciazione del fatto verificato in forma positiva e ripetibile, esposizione del *myth* da contrastare con un'avvertenza esplicita che lo segnali come tale, spiegazione causale alternativa che renda intelligibile *perché* il *myth* fosse plausibile e *perché* non sia, ciononostante, corretto[8]. La distanza temporale fra esposizione al falso e *debunking* riduce significativamente l'efficacia della contromisura, e questa è una delle ragioni per cui Y-TRUST opera, programmaticamente, sull'amplificazione del vero più che sulla smentita del falso: l'amplificazione, a differenza della smentita, non richiede che il falso sia già stato incontrato dal pubblico per produrre un effetto utile.

Sul versante del *prebunking*, l'inoculazione psicologica è il filone me-

[7] S. Lewandowsky, J. Cook, U.K.H. Ecker et al., *The Debunking Handbook 2020*, 2020, DOI 10.17910/b7.1182, pp. 8-15.

[8] Ivi, pp. 12-15. Sulla rilevanza delle plausibili alternative nel contrastare il *continued influence effect*, cfr. anche ivi, pp. 17-19.

todologicamente più promettente. Mutuato dalla teoria dell'immunizzazione cognitiva di McGuire degli anni Sessanta, esso consiste nell'esporre preventivamente il lettore a una versione attenuata e riconosciuta come tale della tecnica manipolatoria che potrebbe incontrare, in modo da rafforzarne la capacità di riconoscerla nei contesti reali. Una rassegna recente firmata da Traberg, Roozenbeek e van der Linden documenta la replicabilità dell'effetto inoculante su tecniche manipolative quali la falsa dicotomia, il *fearmongering*, l'attacco *ad hominem*, le incoerenze argomentative[9]. Roozenbeek e van der Linden hanno proposto applicazioni mirate al dominio sanitario[10] e hanno mostrato che l'inoculazione tecnica risulta efficace anche di fronte a disinformazione del mondo reale e non solo *in vitro*[11].

Il punto di svolta, quello che ci interessa qui maggiormente, è la dimostrazione, ottenuta da Roozenbeek, van der Linden e altri ricercatori nel 2022 mediante un esperimento di campo su YouTube su un campione complessivo di circa ventiduemila utenti, che l'inoculazione psicologica può essere distribuita su scala industriale attraverso brevi video pre-*roll* (di circa novanta secondi ciascuno) e produrre un miglioramento misurabile della capacità del pubblico di riconoscere tecniche manipolative comuni[12]. È il primo studio, a nostra conoscenza, che dimostra la fattibilità di un *prebunking* nativamente integrato nell'ambiente di piattaforma, e ne riprenderemo le implicazioni in §6 e §8.

Una sintesi divulgativa ma rigorosa di questo filone è stata recentemente offerta dallo stesso van der Linden in *Foolproof*[13], a cui rimando per una panoramica accessibile dell'intera agenda di ricerca.

[9] C.S. TRABERG, J. ROOZENBEEK, S. VAN DERLINDEN, *Psychological Inoculation against Misinformation: Current Evidence and Future Directions*, in *The Annals of the American Academy of Political and Social Science*, 2022, pp. 136-151.

[10] J. ROOZENBEEK, S. VAN DER LINDEN, *How to Combat Health Misinformation: A Psychological Approach*, in *American Journal of Health Promotion*, 2022, pp. 569-575.

[11] J. ROOZENBEEK, C.S. TRABERG, S. VAN DER LINDEN, *Technique-based Inoculation against Real-world Misinformation*, in *Royal Society Open Science*, 2022, art. 211719.

[12] J. ROOZENBEEK, S. VAN DER LINDEN, B. GOLDBERG, S. RATHJE, S. LEWANDOWSKY, *Psychological Inoculation Improves Resilience against Misinformation on Social Media*, in Science Advances, 2022, art. eabo6254. Lo studio integra sei esperimenti pre-registrati randomizzati (n = 6.464) con un esperimento di campo su YouTube (n = 22.632) e dimostra che l'esposizione preventiva ai video di inoculazione migliora la capacità degli utenti di riconoscere manipolazione emotiva, incoerenza, false dicotomie, *scapegoating* e attacchi *ad hominem.*

[13] S. VAN DER LINDEN, *Foolproof: Why Misinformation Infects Our Minds and How to Build Immunity*, W. W. Norton & Company, New York, 2023, pp. 165-220.

Sul versante della psicologia individuale, il contributo recente di Pennycook e Rand[14] ha riarticolato la disputa fra «conto cognitivo» (*classical reasoning account*) e «conto motivazionale» (*motivated reasoning account*) della credenza nelle *fake news*, sostenendo che gran parte della suscettibilità è attribuibile a deficit di ragionamento analitico e a *scorciatoie euristiche*, familiarità della fonte, ripetizione del messaggio, più che a polarizzazione politica intenzionale. La conclusione non assolve l'utente dalla responsabilità di valutare, ma sposta l'accento sui meccanismi non deliberativi della condivisione: una persona che condivide un titolo *clickbait* non sempre ne crede il contenuto, ma frequentemente non gli ha dedicato neppure il tempo necessario a valutarlo.

Il *fact-checking* tradizionale, infine, ha conseguito risultati documentati nella riduzione della credenza in singoli *claim* falsi, ma soffre di tre limiti strutturali ben noti: latenza, il tempo necessario per la verifica supera spesso quello della massima diffusione virale del contenuto; copertura selettiva, i *fact-checker* possono verificare solo una piccola percentuale del volume informativo; *last-mile problem*, la verifica raggiunge raramente lo stesso pubblico esposto al falso. È in questo spazio operativo, sospeso fra le tre famiglie di contromisure, che si colloca la proposta di Y-TRUST: la sua promessa è di affrontare il *last-mile problem*, non con un altro *fact-checker* indipendente, ma con un meccanismo di amplificazione fiduciaria del verificato, fondato sulla mediazione degli *influencer*.

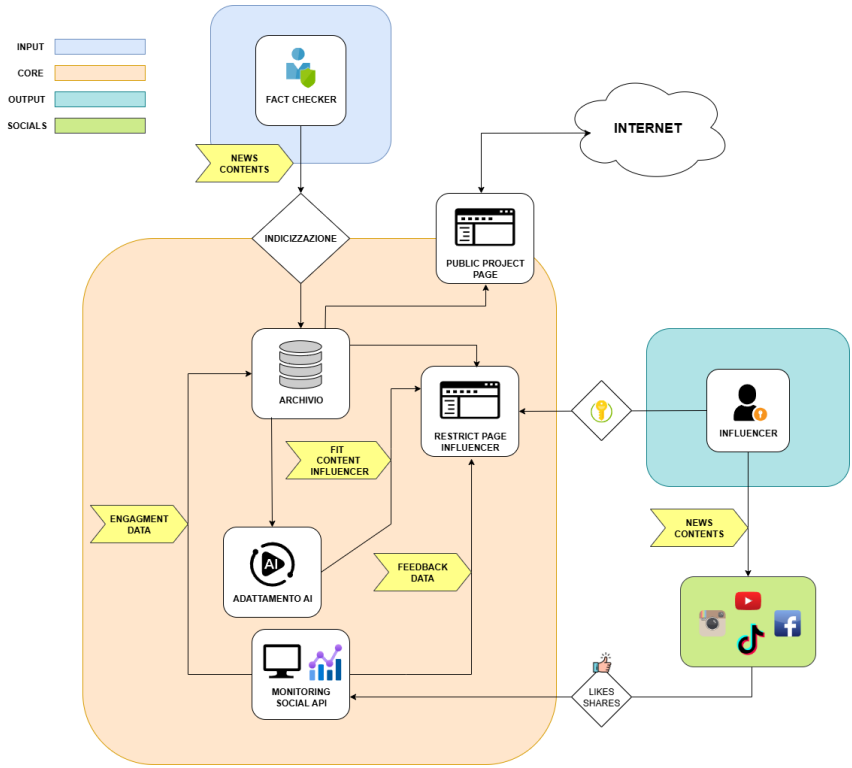
4. Y-TRUST come dispositivo socio-tecnico

Definiamo Y-TRUST come un dispositivo socio-tecnico orientato all'amplificazione controllata del verificato. La definizione richiede due chiose. La prima: non si tratta di una piattaforma di pubblicazione, il contenuto non vi viene pubblicato per essere consumato, vi entra per essere ridistribuito altrove. La seconda: non si tratta di un *fact-checker*, la verifica del contenuto è a monte, condotta da soggetti terzi qualificati il cui prodotto Y-TRUST riceve, conserva, indicizza. Il dispositivo è dunque, in senso tecnico, un *intermediario*; e, come ogni intermediario, il suo valore non risiede in ciò che produce, ma nelle relazioni che istituisce fra gli attori che mette in collegamento.

L'architettura funzionale del portale si suddivide in due aree prin-

[14] G. Pennycook, D.G. Rand, *The Psychology of Fake News*, in *Trends in Cognitive Sciences*, 2021, pp. 388-402.

cipali, una Sezione Pubblica, accessibile a chiunque, e un'Area Riservata *Influencer*, accessibile solo previa registrazione e *vetting*, sorrette da un *back-end* amministrativo destinato a *fact-checker* e amministratori del progetto. La logica del sistema è restituita dal diagramma di flusso riprodotto qui sotto.



Il diagramma articola il dispositivo in quattro blocchi cromaticamente distinti: un *Input* azzurro che ospita il *Fact-Checker*, un *Core* arancione che contiene Archivio, Adattamento AI, *Restricted Page Influencer, Monitoring Social API* e *Public Project Page*, un *Output* turchese che ospita l'*Influencer* e un *Socials* verde che raccoglie Instagram, YouTube, TikTok e Facebook. Le frecce nere identificano flussi di dati: *News Contents* in ingresso, *Fit Content Influencer* e *Feedback Data* interni al *Core*, *News Contents* in uscita verso i *Socials*, *Engagment Data* ed *Likes Shares* di ritorno verso il *Monitoring*. Il sistema chiude su sé stesso un ciclo: verificato, archivio, adattamento, *restricted page*, *social*, metriche, archivio.

Letto come dispositivo, Y-TRUST realizza tre operazioni che sicuramente è utile distinguere analiticamente. La prima è una operazione di archiviazione: il contenuto verificato dai *fact-checker* viene indicizzato, dotato di metadati (categoria, *tag*, fonti, data di verifica) e reso ricercabile, costituendo nel tempo un archivio strutturato che ha valore proprio anche al di là della sua amplificazione. La seconda è una operazione di adattamento: lo stesso contenuto, prima di essere distribuito, viene riformulato dal modulo di intelligenza artificiale linguistica in modo da risultare coerente con lo stile dell'influencer selezionato e con il formato del social di destinazione, un punto al quale è dedicato il prossimo paragrafo. La terza è una operazione di amplificazione: il contenuto adattato viene messo a disposizione dell'*influencer*, che lo pubblica sui propri canali e ne segnala al sistema gli *Uniform Resource Locator*, alimentando il modulo di *monitoring* che chiude il *loop*.

La cifra del dispositivo non sta in alcuna di queste tre operazioni in isolamento, esistono archivi documentali, esistono strumenti di *content adaptation* basati su modelli linguistici, esistono *dashboard* di *social listening*, ma nella loro composizione coordinata su un'unica filiera fiduciaria. La filiera attribuisce a ciascun nodo una funzione differente: il *fact-checker* è il garante epistemico del contenuto; il modulo di adattamento è il mediatore stilistico, vincolato al principio di non-distorsione dei fatti; l'*influencer* è il vettore fiduciario presso il pubblico; il *monitoring* è il sensore che alimenta il *feedback loop* metrico.

La distribuzione delle funzioni produce due effetti che riteniamo di rilievo teorico. Il primo è una decentralizzazione del rischio editoriale: nessun singolo nodo concentra la responsabilità integrale del contenuto pubblicato; ciascuno risponde, nei termini propri della sua funzione, di una porzione definita. Il secondo è la visibilità della filiera: a differenza di una piattaforma generalista, dove l'utente vede il contenuto ma non i meccanismi che lo hanno selezionato, Y-TRUST può, e a nostro avviso deve, rendere esplicito che il contenuto pubblicato dall'*influencer* è il prodotto di un processo di verifica e di adattamento, esibendo la propria origine come marchio di affidabilità.

Questa scelta architettonica solleva, tuttavia, una questione di trasparenza algoritmica che non possiamo eludere. Ananny e Crawford hanno mostrato, in un saggio diventato un riferimento canonico nel campo dell'*algorithmic accountability*, che l'ideale di trasparenza incontra dieci limiti strutturali, fra cui il fatto che la sola esibizione del codice o degli output di un sistema non equivale alla comprensione del suo funzionamento, e che la trasparenza «verso» l'utente generico è spesso indistin-

guibile dalla sua opacità sostanziale[15]. La filiera Y-TRUST, anche quando esplicitata, resterà in larga parte opaca rispetto al criterio di selezione delle notizie, alla taratura del modulo di adattamento, alla calibrazione dei *tier* premianti. Questo non è, di per sé, un vizio del dispositivo: è un effetto della sua natura ibrida. È però una ragione in più per accompagnarne il dispiegamento con strumenti istituzionali, audit indipendenti, accesso strutturato ai *log* da parte di ricercatori, su cui torneremo in §8.

L'architettura di Y-TRUST è la nostra prima risposta alla domanda posta in apertura: come si costruisce, materialmente, una contromisura al disordine informativo che non sia un'altra forma di censura, né una semplice ripetizione del verificato in un nuovo canale. La risposta che il dispositivo propone è: ibridando funzioni che normalmente stanno separate (verifica, mediazione, amplificazione) sotto un vincolo metodologico esplicito di *fact preservation*. È sul cuore tecnico di questo vincolo (il modulo di adattamento linguistico) che ora occorre soffermarsi.

5. *L'adattamento del contenuto tramite* Large Language Models *aperti e ospitati* on-premise

Affermare che un dispositivo socio-tecnico contro il disordine informativo impieghi, per il proprio modulo di adattamento, «un modello linguistico di grandi dimensioni *open-source* ospitato in locale» è una indicazione di indirizzo, non una scelta di progetto. Riteniamo che, in assenza della specificazione delle famiglie di modelli effettivamente caricate in produzione, del motore di inferenza, dell'infrastruttura *hardware* di esecuzione e della politica di provenienza e di etichettatura degli *output*, gli obblighi che il *Regolamento generale sulla protezione dei dati* (di seguito *GDPR*), il *Digital Services Act* e, soprattutto, il *Regolamento europeo sull'intelligenza artificiale* (di seguito *AI Act*) impongono al titolare del trattamento e al *deployer* del sistema di intelligenza artificiale restano enunciati astratti e non documentabili dinanzi all'autorità di vigilanza. La legittimità di un'infrastruttura come Y-TRUST si gioca, per la nostra analisi, esattamente nel passaggio dall'enunciazione di principio all'adozione di una *AI stack* compiuta, dichiarata, esponibile *ex ante* tanto al *Comitato europeo per la protezione dei dati* quanto, dal 2 agosto 2026, al nuovo *AI Office* della Commissione

[15] M. ANANNY, K. CRAWFORD, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, in *New Media & Society*, 2018, pp. 973-989.

europea[16]. Su questo punto la versione operativa del progetto ha effettuato scelte che meritano un'esposizione analitica e che vale la pena ricostruire nei loro tre strati: il modello, il motore di inferenza, la provenienza.

Lo strato del modello adotta, in regime di produzione, una *dual-model architecture* che combina due famiglie di modelli aperti complementari per finalità e per regime di trasparenza dei dati di addestramento. Il primo è *Mixtral 8x22B Instruct*, rilasciato da Mistral AI nell'aprile 2024 con licenza *Apache 2.0*, fra i pochi modelli *frontier* di origine europea a coniugare un'architettura *Mixture-of-Experts* (centoquarantuno miliardi di parametri totali, trentanove attivi per *token*) con una licenza pienamente permissiva, e a dimostrare sui *benchmark* multilingui *HellaSwag*, *Arc Challenge* e *MMLU* prestazioni superiori a *LLaMA 2 70B* nelle lingue europee, italiano incluso[17]. Il secondo è *Minerva-7B-instruct-v1.0*, sviluppato dal *Sapienza NLP Group* dell'Università di Roma «La Sapienza» in collaborazione con il programma *Future Artificial Intelligence Research* e con il consorzio *CINECA*, rilasciato anch'esso con licenza *Apache 2.0*[18]. La peculiarità di *Minerva* è di essere, alla data di questa trattazione, l'unica famiglia di modelli *truly open* (sia il modello sia i dati di *training*) addestrata *from scratch* su un *corpus* documentato di circa duemilacinquecento miliardi di *token*, di cui circa millecentoquaranta in italiano. La scelta della *dual-model* non è ridondanza progettuale: *Mixtral* assicura la qualità generativa richiesta dall'adattamento stilistico al profilo dell'*in-*

[16] Per il riferimento normativo primario, cfr. Regolamento (UE) n. 679 del 2016, in particolare artt. 25 e 32. Sull'interpretazione operativa dell'obbligo di documentazione *ex ante* in capo al titolare del trattamento, cfr. European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, *version 2.0*, adottate il 20 ottobre 2020, §§ 17-31. Sul calendario di applicazione degli obblighi di trasparenza dell'*AI Act*, di competenza dell'*AI Office* istituito dalla Commissione europea, e sulle relative sanzioni (fino a quindici milioni di euro o al 3% del fatturato annuo mondiale), cfr. Commissione Europea, *Consultation on the Draft Guidelines on Transparency Obligations under the AI Act*, 2026, in www.digital-strategy.ec.europa.eu.

[17] Mistral AI, *Cheaper, Better, Faster, Stronger*, 17 aprile 2024, in www.mistral.ai. Sul confronto delle prestazioni multilingui rispetto alla famiglia *LLaMA 2*, *ivi*, sezione «*Multilingual benchmarks*»: gli autori riportano un margine di accuratezza significativo a favore di *Mixtral 8x22B* su *HellaSwag*, *Arc Challenge* e *MMLU* nelle versioni francese, tedesca, spagnola e italiana.

[18] Sapienza NLP Group, *Minerva LLMs: The First Family of Large Language Models Trained from Scratch on Italian Texts*, 2024, *passim*. La *model card* ufficiale di *Minerva-7B-instruct-v1.0* è pubblicata in www.minerva-llm.org. Sulla genesi del progetto, sull'architettura e sui criteri di selezione del *corpus*, cfr. il comunicato dell'Università di Roma «La Sapienza», in www.uniroma1.it.

fluencer; *Minerva* svolge la funzione di validazione semantica intermedia e di *fallback* nei contesti in cui la verificabilità integrale del *corpus* di *training* costituisce, come argomenteremo *infra*, un *enabler* decisivo della *due diligence* prevista dall'art. 53 dell'*AI Act*.

Lo strato del motore di inferenza è affidato a *vLLM*, libreria *open-source* rilasciata con licenza *Apache 2.0* dal *Sky Computing Lab* della *University of California at Berkeley* e oggi considerata lo *standard de facto* dell'inferenza ad alte prestazioni in ambienti *enterprise*, grazie a una architettura *PagedAttention* che restituisce, a parità di carico, un *throughput* di un ordine di grandezza superiore rispetto alle librerie *transformers* convenzionali e che è alla base delle *pipeline* di produzione di Meta, Mistral AI, IBM e Red Hat[19]. La rilevanza giuridica della scelta eccede il piano tecnico. L'esecuzione di *vLLM* su infrastruttura europea sovrana, *poniamo* un *cluster* di unità *NVIDIA H100* gestite direttamente dal titolare o presso un *partner* nazionale come la rete *CINECA Leonardo*, restituisce al titolare del trattamento il controllo integrale dei *log* di inferenza, della politica di ritenzione e dei punti di applicazione delle misure tecniche di sicurezza richieste dall'art. 32 del *GDPR*. Nessun *prompt*, nessuna porzione di testo verificato, nessun *embedding* intermedio lascia l'infrastruttura del titolare; nessun trasferimento internazionale di dati personali ai sensi del Capo V del *GDPR*; nessuna necessità di clausole contrattuali tipo né di una *Transfer Impact Assessment* ai sensi degli artt. 44-46 del medesimo Regolamento. La scelta *on-premise*, in questo modo, non si limita a semplificare la *compliance*: la rende verificabile, perché ogni passaggio è auditabile entro un perimetro tecnico unitario.

Lo strato della provenienza è il più recente nella sua maturazione regolatoria e il più decisivo per la legittimazione pubblica del dispositivo. L'art. 50 del Regolamento (UE) n. 1689 del 2024 entra in piena applicazione il 2 agosto 2026 e impone, per i contenuti generati o manipolati con assistenza di intelligenza artificiale, una marcatura in formato leggibile da macchina e, per i *deep fake* e per i contenuti destinati a informare il pubblico su questioni di interesse pubblico, una etichettatura visibile e tempestiva[20]. Il *Code of Practice on the Marking and Labelling of*

[19] VLLM PROJECT, *vLLM: Easy, Fast, and Cheap LLM Serving for Everyone*, *repository* ufficiale, *passim*, in github.com/vllm-project/vllm. Sull'adozione di *vLLM* nelle *pipeline* di produzione *enterprise* e sulla sua qualificazione come *standard de facto* dell'inferenza *open-source*, cfr. RED HAT, *What is vLLM?*, 2026, in www.redhat.com

[20] Art. 50, Regolamento (UE) n. 1689 del 2024, in *Gazzetta Ufficiale dell'Unione Europea*, L serie, 12 luglio 2024.

AI-Generated Content della Commissione europea, di cui è disponibile la seconda bozza del marzo 2026 e la cui versione definitiva è attesa per il giugno 2026, raccomanda esplicitamente l'adozione del *framework* tecnico *C2PA Content Credentials*, giunto nel febbraio 2026 alla versione 2.3, come *layer* di marcatura crittograficamente firmata, da integrare con un secondo *layer* di *watermarking* impercettibile e con un terzo *layer* di *fingerprinting* per il recupero della provenienza qualora i metadati vengano rimossi nel transito attraverso le piattaforme di destinazione[21]. Y-TRUST adotta, in regime di produzione, l'intera tripletta: ogni adattamento prodotto dalla *pipeline Mixtral-vLLM* è incapsulato in un *manifest C2PA* firmato con chiave privata del titolare, marcato con *watermark* impercettibile a livello di sequenza generativa e indicizzato a *fingerprint* nel *repository* del progetto. La scelta eccede il *minimum standard* fissato dall'art. 50 e si motiva, per ammissione esplicita, soltanto a partire dall'assunzione che l'adempimento dell'*AI Act* non sia un *check* formale ma un dovere sostanziale rispetto al pubblico finale, in particolare rispetto a quella frazione di pubblico raggiunta dall'*influencer* per via mediata e dunque meno in grado di ricostruire autonomamente l'origine del contenuto.

Una considerazione di sintesi va condotta sulla coerenza fra questi tre strati e il principio di *data protection by design and by default* sancito dall'art. 25 del *GDPR* e declinato in *enabling controls* operativi nelle *Guidelines* dell'EDPB[22]. L'esecuzione *on-premise* della *pipeline Mixtral-Minerva* su *vLLM* assolve, *by design*, agli obiettivi di *Confidentiality* (i testi verificati, le preferenze stilistiche dell'*influencer*, gli esempi di stile e i *prompt* di sistema non escono dall'infrastruttura del titolare) e di *Storage limitation* (la politica di ritenzione dei *log* di inferenza è interamente determinata dal titolare e può essere fissata a zero per i dati di *prompt* che contengano elementi personali). Il rilascio degli *output* con manifesto *C2PA* firmato assolve all'obiettivo di *Transparency*. La pubblicazione, nella documentazione di progetto, della *model card* di *Mixtral 8x22B* e del

[21] Commissione Europea, *Code of Practice on the Marking and Labelling of AI-Generated Content*, seconda bozza, marzo 2026, *passim*. La specifica tecnica di riferimento è Coalition For Content Provenance and Authenticity, *Content Credentials Specification*, versione 2.3, febbraio 2026, in spec.c2pa.org. Sulla persistenza dei *manifest* nel transito attraverso le principali piattaforme social e sulla conseguente necessità di un *layer* aggiuntivo di *fingerprinting*, cfr. la nota tecnica dello stesso *Code of Practice*, sezione «*Durable Content Credentials*».

[22] European Data Protection Board, *Guidelines 4/2019*, *cit.*, §§ 17-31 e allegato. Sulla genesi storica del principio, A. Cavoukian, *Privacy by Design: The 7 Foundational Principles*, 2009 (II ed. 2011), *passim*.

training data report di *Minerva 7B* assolve all'obiettivo di *Accountability*. Nessuno di questi adempimenti, preso singolarmente, è straordinario; tutti insieme costituiscono ciò che riteniamo essere la dimostrazione documentabile che la *due diligence* del *deployer* sia stata esercitata *ex ante* sull'intera *AI stack* e non rimandata a una rivendicazione *ex post* di buona fede. Su questo terreno, peraltro, la *dual-model* aperta si rivela strategica anche rispetto a una seconda dimensione dell'*AI Act*: l'art. 53, che disciplina gli obblighi dei fornitori di *General-Purpose AI Models*, impone documentazione tecnica, informazione ai *deployer* e sintesi pubblica del *corpus* di addestramento. La combinazione di *Mixtral 8x22B* (fornitore Mistral AI, *model card* e documentazione tecnica integralmente pubbliche, *training data* parzialmente documentato) e di *Minerva 7B* (fornitore *Sapienza NLP Group*, *training data* integralmente documentato e accessibile) consente a Y-TRUST, nella veste di *deployer*, di esercitare gli obblighi *downstream* che gli competono, in particolare la documentazione della catena di provenienza dei modelli, la verifica delle dichiarazioni rese dai fornitori a monte, l'ispezione, ove tecnicamente necessaria, della composizione del *corpus*. Veale e Zuiderveen Borgesius, nell'analisi della struttura di responsabilità multilivello tracciata dall'*AI Act*, hanno mostrato come ciascun anello della *AI value chain* sia tenuto a contribuzioni specifiche di trasparenza e di documentazione[23]: la *dual-model* aperta consente a Y-TRUST di adempiere alle proprie senza trovarsi sprovvisto di prova affermativa in caso di contestazione, condizione che, in regime di modelli chiusi accessibili via *Application Programming Interface* di fornitori extra-europei, si tradurrebbe in una mera fiducia in dichiarazioni unilaterali non ispezionabili.

Resta da affrontare il tema, sostanziale e non procedurale, del rischio di *allucinazione*. Anche un modello aperto, ben addestrato e ospitato in ambiente controllato può inserire, nell'adattamento di una notizia verificata, dettagli inventati che la rete neurale «riempie» per produrre un testo plausibile. La risposta strutturale adottata dal dispositivo è multilivello. In primo luogo, il contenuto verificato dal *fact-checker* viene

[23] M. VEALE, F. ZUIDERVEEN BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act*, in *Computer Law Review International*, 2021, pp. 97-112. Pur riferendosi alla versione di proposta del 2021, l'analisi della struttura di responsabilità multilivello è confermata, nella sua impostazione, dal testo finale del 2024. Sul piano dell'etica applicata, l'orizzonte di riferimento entro cui collochiamo l'intera *stack* è quello del quadro *AI4People* di L. FLORIDI *et al.*, *AI4People: An Ethical Framework for a Good AI Society*, in *Minds and Machines*, 2018, pp. 689-707, articolato sui cinque principi di *beneficence*, *non-maleficence*, *autonomy*, *justice* ed *explicability*.

iniettato come *system prompt* immutabile durante l'inferenza, in modo che la fonte autorevole costituisca il vincolo informativo che il modello non può eludere. In secondo luogo, una *pipeline* automatica di confronto fra l'*output* generato e l'*input* originario è eseguita su un insieme limitato di entità nominate (numeri, percentuali, date, nomi propri, citazioni testuali) prima che l'adattamento venga reso disponibile all'*influencer*: ogni divergenza superi una soglia preimpostata viene segnalata al *fact-checker* per validazione manuale. In terzo luogo, *Minerva 7B* è impiegata come *second-pass validator* per la verifica di coerenza in italiano, esercizio nel quale la sua natura di modello *Italian-native* offre, sulla base della letteratura disponibile, un vantaggio non trascurabile rispetto a modelli multilingue di provenienza non europea. In quarto luogo, la revisione umana dell'*influencer* resta indispensabile e contribuisce, a valle, al principio di *fact preservation* assunto come «inderogabile» dal progetto. La piena risoluzione del rischio resta, beninteso, un orizzonte e non un esito; ma la concorrenza di quattro *guardrail* indipendenti riduce, in modo verificabile, lo spazio in cui un *output* allucinato possa attraversare la *pipeline* senza essere intercettato.

L'adattamento, in sintesi, non è un dettaglio tecnico. È il punto in cui un dispositivo come Y-TRUST si misura contemporaneamente con tre regimi normativi europei, con un imperativo etico di non-distorsione del verificato e con i limiti epistemici propri dei modelli generativi. La scelta di una *dual-model* aperta, eseguita *on-premise* con *vLLM* su infrastruttura europea sovrana e tracciata in provenienza secondo *C2PA*, è la traduzione, sul piano dell'ingegneria di sistema, della tesi che attraversa l'intero articolo: la legittimità di un'infrastruttura informativa europea non è una proprietà a sé stante che si possa rivendicare in dichiarazioni di principio, ma una proprietà emergente di scelte tecniche documentabili, ispezionabili e verificabili sino al singolo *commit* della libreria di inferenza.

6. *La mediazione degli* influencer*: profilazione, sistema premiante,* guardrail

L'*influencer*, nel disegno di Y-TRUST, è il nodo che permette al verificato di raggiungere il pubblico che il *fact-checker* tradizionale non raggiunge. È anche, riteniamo, il nodo che presenta la maggiore concentrazione di rischio dell'intero dispositivo: rischio etico, giuridico e reputazionale. Le due osservazioni vanno tenute insieme: senza l'*influencer*, Y-TRUST non amplifica nulla; con l'*influencer*, Y-TRUST si espone a

una serie di vulnerabilità che la sola architettura tecnica non può risolvere e che devono essere governate da scelte di *design* contrattuali, deontologiche e regolatorie.

Una prima osservazione di scenario. Il rapporto UNESCO del 2024 *Behind the Screens*, basato su una *survey* condotta presso cinquecento *digital content creator* in quarantacinque Paesi, restituisce la fotografia di una categoria professionale ancora largamente sotto-regolata, in cui la pratica del *fact-checking* sistematico è eccezione e non regola, e in cui la percezione del proprio ruolo informativo è spesso oggettivamente sproporzionata rispetto agli strumenti deontologici disponibili[24]. Un secondo segnale, di segno congruente, viene dal lavoro di Mulcahy e altri, che ha documentato in uno studio empirico recente come gli *influencer* siano vettori del verificato e, con effetto misurabile, anche di *misinformation*[25]. Il rischio, in altri termini, è simmetrico al beneficio: la rete di distribuzione che si vuole arruolare per la causa del vero è la stessa che, in altre condizioni, propaga il falso.

Su questo sfondo, il progetto propone un sistema premiante a tre *tier* (*Ambassador Base*, *Ambassador Avanzato*, *Ambassador Elite*) declinato in due alternative: una simbolico-reputazionale (Alternativa A) e una con incentivi monetari (Alternativa B), oltre a un possibile sistema misto. L'analisi del *trade-off* fra le due alternative ci sembra centrale.

L'Alternativa A, riconoscimenti simbolici, *badge*, attestati digitali, visibilità sul portale pubblico, fa leva su motivazioni intrinseche e ha il vantaggio strutturale di non aprire un fronte di conflitto di interessi: l'*influencer* non riceve denaro per condividere il contenuto, riceve *status*. Il vantaggio si paga in termini di scalabilità: una motivazione esclusivamente reputazionale è efficace su un numero limitato di partecipanti particolarmente motivati e poco selettiva su un pubblico ampio.

L'Alternativa B, incentivi monetari, *bonus* per *tier*, compensi *performance-based*, risolve il problema di scalabilità ma introduce il rischio di cattura. Un *influencer* retribuito per ogni notizia condivisa è, *per definizione*, parte di una catena commerciale; la sua indipendenza dichiarativa

[24] UNESCO, *Behind the Screens: Insights from Digital Content Creators*, 2024, *passim*. Lo studio è il primo del suo genere a coprire un campione internazionale di questa estensione.

[25] R. MULCAHY, R. BARNES, R. DE VILLIERS SCHEEPERS, S. KAY, E. LIST, *Going Viral: Sharing of Misinformation by Social Media Influencers*, in *Australasian Marketing Journal*, 2025. Cfr. anche, per un inquadramento teorico della figura dell'*influencer* come *micro-celebrity*, C. ABIDIN, *Internet Celebrity: Understanding Fame Online*, 2018, *passim*.

rispetto al contenuto deve essere costantemente difesa da meccanismi contrattuali, da soglie di qualità, da audit indipendenti. Su questo terreno, il terreno della trasparenza dei contenuti commerciali, interviene direttamente la delibera AGCOM n. 197/25/CONS del 2025, che ha approvato le *Linee guida e codice di condotta in materia di contenuti diffusi dagli influencer sulle piattaforme online*[26]. La delibera fissa soglie quantitative (numero di *follower*, indicatori di *engagement*) per individuare gli *influencer* «rilevanti» ai sensi del *Testo Unico dei servizi di media audiovisivi* e impone obblighi di trasparenza, in particolare per i contenuti commerciali, le partnership monetizzate, le promozioni. L'applicabilità della delibera all'ipotesi B di Y-TRUST è, a nostro avviso, diretta: una collaborazione retribuita per la diffusione di contenuti, anche se di interesse pubblico, ricade nella nozione di *partnership* monetizzata e deve essere segnalata come tale al pubblico.

L'apparato AGCOM si combina, dal nostro punto di vista, in modo significativo con la regolazione DSA-derivata. Mentre l'AGCOM disciplina la condotta del singolo *influencer* sul singolo contenuto, il *Digital Services Act*, quando applicabile alle piattaforme di destinazione su cui l'*influencer* pubblica, disciplina la condotta della piattaforma rispetto alla pubblicità e ai *recommender systems*. La condotta dell'*influencer* Y-TRUST si trova così esposta, simultaneamente, a due regimi che non si sovrappongono perfettamente ma che ne stringono le condizioni di legittimità: deve essere trasparente *come influencer* (regime AGCOM), e il contenuto che pubblica deve essere trattato secondo regole di trasparenza dalla piattaforma sulla quale viene pubblicato (regime DSA, se applicabile). Y-TRUST può presidiare il primo regime contrattualmente; sul secondo non ha leva diretta, ma può fornire all'*influencer*, come parte del *kit* di pubblicazione, *meta-tag* e *disclaimer* standardizzati che ne facilitino la corretta categorizzazione algoritmica.

Esiste, tuttavia, un secondo livello del problema che non è risolto neppure dall'osservanza della delibera AGCOM. Il *Digital Services Act* impone, al suo art. 26, obblighi di trasparenza sulla pubblicità mostrata sulle piattaforme online ai *recipients* del servizio, e il Codice di Condotta UE rafforzato sulla disinformazione del 2022, integrato come *Code of Conduct* nel *Digital Services Act* il 13 febbraio 2025, disciplina, all'impegno IV, l'integrità del servizio rispetto a *bot* e comportamenti inautentici

[26] La delibera articola gli obblighi di trasparenza per gli *influencer rilevanti*, individuati sulla base di soglie quantitative di pubblico e di engagement, e fornisce un *test* operativo per distinguere il contenuto editoriale dal contenuto promozionale.

coordinati[27]. La nozione di «comportamento inautentico coordinato» è ampia e, letta in connessione con la disciplina AGCOM sugli *influencer*, può estendersi a forme strutturate di amplificazione di contenuti incentivata da soggetti terzi. Y-TRUST non rientra evidentemente nella fattispecie classica della *coordinated inauthentic behavior*, il contenuto è verificato, la mediazione è dichiarata, ma il fatto che esista una rete strutturata, profilata, premiata per diffondere lo stesso *pool* di contenuti su più canali è una circostanza che, in assenza di adeguate misure di trasparenza, potrebbe essere assimilata, sul piano fattuale, a una forma di *astroturfing* edificante. La distinzione fra le due figure non è giuridica ma deontologica e va attivamente difesa.

A queste considerazioni ne aggiungiamo una sul piano della profilazione. Il modulo di profilazione di Y-TRUST raccoglie, oltre ai dati anagrafici di base, informazioni sui canali social dell'*influencer*, sul numero di *follower*, sulla demografia del pubblico, sulle categorie di interesse, sullo stile comunicativo. Tale insieme di dati configura una *attività di profilazione* ai sensi dell'art. 4 n. 4 del *GDPR* e, quando combinata con la successiva produzione di contenuti adattati allo stile dichiarato, costituisce, riteniamo, un trattamento per il quale è opportuno valutare la conduzione di una *Data Protection Impact Assessment* ai sensi dell'art. 35 del medesimo Regolamento. Non perché il trattamento integri necessariamente i criteri del *high risk*, ma perché la combinazione di profilazione sistematica, finalità innovativa e impatto potenziale sull'autenticità della comunicazione politica e sociale è sufficiente a giustificare, in via cautelare, l'esercizio della DPIA come strumento di documentazione e di *accountability*[28].

Quanto ai *guardrail* operativi, riteniamo che il dispositivo, per essere difendibile, debba prevedere almeno quattro misure ulteriori rispetto a quanto già esposto. Primo, un *opt-in* esplicito dell'*influencer* alla profilazione stilistica, con possibilità di revoca *runtime* e cancellazione degli esempi utilizzati per il *prompting*. Secondo, un *audit qualitativo* preventivo prima dell'attribuzione di un *tier* premiante, condotto su un campione casuale dei post pubblicati. Terzo, una clausola contrattuale di non-di-

[27] Sull'integrazione del Codice nel DSA come *Code of Conduct* ai sensi dell'art. 45 DSA, cfr. il comunicato della Commissione del 13 febbraio 2025, in www.digital-strategy.ec.europa.eu.

[28] Regolamento (UE) n. 679 del 2016, art. 35, *cit.* Cfr. anche le *Guidelines on Data Protection Impact Assessment* del Gruppo dell'Articolo 29, WP 248, rev. 01, adottate il 4 ottobre 2017 e successivamente fatte proprie dall'EDPB.

storsione dei fatti che sopravviva alla cessazione del rapporto, con clausole di *clawback* del *bonus* monetario in caso di documentata violazione. Quarto, un meccanismo di trasparenza esplicita verso il pubblico finale, non un'etichetta in piccolo, ma una segnalazione visibile che il contenuto deriva da una notizia verificata adattata in collaborazione con il progetto Y-TRUST. Queste misure non risolvono il rischio di cattura: lo gestiscono. È il massimo che, in questa fase, sembra essere ragionevole chiedere a un dispositivo della complessità che Y-TRUST si propone di realizzare.

7. *Conformità* by design*:* GDPR*,* Digital Services Act *e* AI Act *nella stessa piattaforma*

Riteniamo che il progetto sia un caso di studio esemplare per una ragione che lo trascende: lo stesso dispositivo è insieme un trattamento di dati personali ai sensi del GDPR, un servizio digitale con tratti DSA-compatibili, un sistema che impiega, in più moduli, intelligenza artificiale e quindi rientra nel perimetro dell'AI Act. I tre regimi non sono alternativi e non si elidono. Si stratificano sull'unico oggetto: la stessa funzionalità, l'adattamento AI di una notizia verificata da parte di un *influencer* profilato, è simultaneamente un trattamento *ex* GDPR, una pratica di moderazione/intermediazione su cui sovraintende lo spirito del DSA, una pipeline AI generativa *ex* AI Act. Progettare *by design*, in questo contesto, significa progettare per la *convergenza* dei tre piani, non per la loro somma sequenziale.

Il punto di ingresso metodologico è ovvio: i sette principi di *Privacy by Design* enunciati da Cavoukian nel 2009 e rivisti nel 2011, *proactive not reactive*; *privacy as the default*; *privacy embedded into design*; *full functionality*; *end-to-end security*; *visibility and transparency*; *respect for user privacy*[29], costituiscono un metodo di progettazione, non uno slogan. Il loro recepimento nell'art. 25 del GDPR e la successiva declinazione operativa nelle *Guidelines* EDPB 4/2019[30] hanno trasformato il *frame* di Cavoukian in un obbligo giuridico nella misura in cui il titolare deve, in modo verificabile, mostrare di aver implementato misure tecniche e organizzative adeguate fin dalla progettazione del trattamento.

Applicato a Y-TRUST, il metodo *by design* impone scelte concrete.

[29] A. Cavoukian, *Privacy by Design: The 7 Foundational Principles*, 2009 (II ed. 2011), pp. 2-5.

[30] Cfr. altresì in merito all'articolazione del principio in *enabling controls* operativi.

La scelta del modello *on-premise*, già discussa *supra* (§5), è una di queste. La scelta di una *Sezione Pubblica* deliberatamente *povera* di trattamenti, informativa, non profilante, è una seconda. La distinzione netta fra l'area riservata, accessibile solo previo *vetting* e consenso esplicito, e il *back-end* amministrativo, accessibile solo ai gestori del progetto con profili di accesso segregati, è una terza. Il principio di *data minimisation*, solo i dati strettamente necessari, niente dati relativi a minorenni se non in forma anonimizzata e aggregata, niente memorizzazione di date di nascita precise quando basta il *flag* di maggiore età, è la quarta. La politica di *data retention* esplicita, con anonimizzazione o cancellazione automatica oltre un orizzonte temporale definito, è la quinta. Nessuna di queste scelte, presa singolarmente, è straordinaria; tutte insieme, e dichiarate *ex ante* in una *Data Protection Impact Assessment* allegata alla progettazione, costituiscono ciò che riteniamo essere il *minimum standard* di *Privacy by Design* per un dispositivo di questa natura.

Sul piano del *Digital Services Act*, Y-TRUST presenta un profilo giuridico non immediato. Il portale non offre, *stricto sensu*, un servizio di *hosting* ai sensi dell'art. 6 del Regolamento (i contenuti non sono caricati da utenti: sono inseriti da *fact-checker* accreditati e gestiti dagli amministratori) né di *intermediation* nel senso che il DSA assegna alle piattaforme *online*. La sua dimensione, prevedibilmente, non lo qualifica come *Very Large Online Platform* (VLOP) ai sensi dell'art. 33[31]. Ciononostante, l'orizzonte regolatorio del DSA è metodologicamente rilevante per il dispositivo, sotto due profili. Il primo: la disciplina dei termini e condizioni di servizio, in particolare l'art. 14, fornisce un modello di chiarezza contrattuale verso utenti *business* (gli *influencer*) che è opportuno adottare anche al di fuori dell'obbligo. Il secondo: la disciplina dell'attenuazione dei rischi sistemici di cui agli artt. 34-35, pur indirizzata alle VLOPs, indica una metodologia di analisi del rischio (identificazione, valutazione, mitigazione, documentazione) trasferibile a qualsiasi dispositivo che intervenga sulla circolazione di informazione pubblica. Y-TRUST può, e a nostro avviso dovrebbe, autoassumere volontariamente questa metodologia di *risk assessment* e di *risk mitigation*, pur non essendovi tenuto.

Per quanto riguarda l'AI Act, il primo problema di qualificazione concerne il livello di rischio del sistema. La lettura sistematica del Regolamento e dell'allegato III induce a escludere che il modulo di adattamento di Y-TRUST integri la definizione di *high-risk AI system*: la generazione di un testo *social* a partire da una notizia verificata non rientra in alcuna

[31] Art. 33, Reg. (UE) 2065/2022.

delle otto aree: biometria, infrastrutture critiche, istruzione, accesso al lavoro, accesso a servizi pubblici, *law enforcement*, migrazione, amministrazione della giustizia. Restano applicabili, tuttavia, gli obblighi di trasparenza dell'art. 50, già discussi *supra* (§5), e, sul piano della *value chain*, la pretesa di tracciabilità verso i fornitori del modello di cui all'art. 53.

Un punto che riteniamo meriti un'attenzione specifica concerne l'art. 22 del GDPR, sulle decisioni esclusivamente automatizzate. La selezione delle notizie raccomandate all'*influencer* è il prodotto di un algoritmo di *matching* fra categorie dichiarate, stile preferito e *pool* delle notizie verificate; l'*output* è una *raccomandazione*, non una decisione automatizzata che produca effetti giuridici o significativamente analoghi sull'interessato. Il caso non integra, dunque, la fattispecie dell'art. 22; ma il rischio di scivolamento, se la raccomandazione diventasse, nei fatti, una imposizione, o se la non-presa in carico ripetuta di notizie comportasse penalizzazioni nel sistema premiante senza intervento umano, andrebbe presidiato con un punto di *human in the loop* esplicito, documentato e auditabile.

Sul piano di *soft law*, infine, il Codice di Condotta UE rafforzato sulla disinformazione del 2022 e la sua successiva integrazione come *Code of Conduct* nel DSA il 13 febbraio 2025 forniscono, più che obblighi cogenti per dispositivi della scala di Y-TRUST, un vocabolario condiviso e un insieme di pratiche di riferimento. L'adesione volontaria a singoli impegni del Codice (in particolare gli impegni II *Scrutiny of Ad*

Placement, IV *Integrity of Services*, V *Empowering Users*) è uno strumento di posizionamento e di *accountability* che il progetto non dovrebbe trascurare[32].

Il *tableau* normativo che emerge è esigente ma navigabile. Y-TRUST non è penalizzato dalla pluralità di regimi che lo investono, ne è, al contrario, qualificato. Un dispositivo che si proponga di lavorare sull'informazione pubblica europea in modo affidabile e duraturo non può sottrarsi alla stratificazione normativa che è propria dell'ordine giuridico-digitale europeo: deve, anzi, assumerla come propria condizione di legittimità.

8. Limiti del dispositivo e prospettive di ricerca empirica

A questo punto della trattazione possiamo, e dobbiamo, mostrare i limiti del dispositivo. Riteniamo che almeno tre questioni rimangano irrisolte anche nell'ipotesi di una sua esecuzione tecnicamente impeccabile.

[32] Sull'integrazione del Codice nel DSA, *supra*, nota 28.

La prima è ciò che la letteratura nordamericana, a partire dal contributo di Chesney e Citron sui *deep fakes*, ha chiamato *liar's dividend*[33]. Quando l'esistenza pubblica di una rete di amplificazione del verificato si afferma, parallelamente si afferma la possibilità per chi è chiamato a rispondere di una propria dichiarazione documentata di sostenere che il contenuto fattuale che lo accusa sia falso, manipolato, generato artificialmente. Il dispositivo del vero, in altri termini, produce inavvertitamente uno spazio per chi voglia delegittimare il vero accusandolo di falsità. Y-TRUST non risolve questo paradosso: vi si trova esposto come ogni altra infrastruttura del verificato, ed è dunque necessario che il dispositivo si accompagni a strumenti di provenienza e di firma crittografica del contenuto, *content credentials*, *digital provenance*, che permettano al pubblico di verificare l'autenticità della fonte e non semplicemente di credere alla sua dichiarazione.

La seconda questione concerne la *cattura* dell'*influencer* da parte di interessi commerciali esterni al progetto. La discussione del paragrafo precedente sui *guardrail* contrattuali e deontologici riduce, ma non azzera, questo rischio. Un *influencer* che operi in più reti contemporaneamente, Y-TRUST e una agenzia commerciale, poniamo, può subire pressioni discordanti sulla scelta dei contenuti, sui tempi di pubblicazione, sul tono. La sola difesa strutturale è la trasparenza: ogni partecipante deve dichiarare le proprie altre collaborazioni; ogni collaborazione esterna che ecceda una soglia minima deve essere oggetto di valutazione di compatibilità; il *pool* dei contenuti del progetto deve essere diversificato in modo da non concentrare l'amplificazione su pochi *influencer* sovraesposti.

La terza questione è la *scalabilità linguistica*. Y-TRUST, nella sua versione iniziale, è progettato per il contesto italiano, con apertura programmatica al multilinguismo via traduzione automatica dell'LLM. La traduzione, però, non risolve il problema della *verifica* nelle lingue di destinazione: una notizia verificata in italiano, tradotta in albanese da un modello, non è una notizia verificata in albanese, è una traduzione, accurata o meno, di una verifica condotta in altra lingua e in altro ecosistema informativo. La scalabilità autentica richiederebbe *partnership* con reti di *fact-checker* federate, che operino con metodologia compatibile e che riconoscano reciprocamente il proprio prodotto. La direzione di sviluppo è qui implicita.

[33] R. CHESNEY, D.K. CITRON, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, in *California Law Review*, 2019, pp. 1758-1788 (per la formulazione originaria della nozione di *liar's dividend*).

Sulle prospettive di ricerca empirica, indichiamo tre linee che a nostro avviso possono trasformare il dispositivo da progetto a oggetto di studio rigoroso. La prima è uno *studio quasi-sperimentale comparativo* fra *post* di *influencer* Y-TRUST e un gruppo di controllo di post non mediati dal progetto, in cui si misurino, a parità di tema, di canale, di pubblico, *fact preservation*, *engagement* e percezione di credibilità del messaggio. La seconda è un *audit sociolinguistico* dell'adattamento AI: estratto un campione casuale di adattamenti generati, si misuri quantitativamente la *fact preservation* su un insieme limitato di entità nominate e qualitativamente la coerenza stilistica con il profilo dichiarato dell'*influencer*. La terza è una *survey longitudinale* sul pubblico esposto, condotta in più *waves*, per valutare se il messaggio mediato sia percepito come più credibile, equivalente o meno credibile rispetto alla notizia originale. Sulla prima linea, lo studio quasi-sperimentale, riteniamo opportuno suggerire alcuni accorgimenti di disegno. L'assegnazione casuale dei contenuti agli *influencer* del *pool* sperimentale rispetto a quelli del *pool* di controllo deve essere stratificata per categoria tematica, per piattaforma di pubblicazione e per fascia di pubblico dell'*influencer*, per evitare confondimenti che vanificherebbero la misura. La *baseline* deve essere costituita da contenuti di analoga lunghezza e densità informativa prodotti dagli stessi *influencer* in assenza della mediazione del modulo AI. La misurazione della *fact preservation* deve essere condotta in cieco da valutatori indipendenti rispetto al gruppo di assegnazione, su una *checklist* di entità nominate predefinita prima dell'apertura del *dataset*. La misurazione dell'*engagement* deve coprire un orizzonte temporale sufficiente a osservare anche la *long tail* della propagazione, che spesso costituisce, come la letteratura sulla diffusione ha mostrato, una frazione significativa dell'impatto totale[34]. Infine, la pre-registrazione delle ipotesi e del piano analitico in un *repository* pubblico costituisce, oggi, il *minimum standard* metodologico per studi di questo tipo.

Per ciascuna delle tre linee, una nozione metodologicamente utile è quella di *algorithmic accountability* nella formulazione di *Diakopoulos*[35]: l'auditing del dispositivo deve essere condotto da terze parti, con accesso strutturato ai *log*, con metodologia replicabile, con risultati pubblici.

Una nota istituzionale chiude il paragrafo. L'art. 40 del DSA prevede,

[34] Sulla rilevanza della *long tail* nella diffusione online, cfr. S. Vosoughi, D. Roy, S. Aral, *op. cit*., pp. 1149-1150, *passim*.

[35] N. Diakopoulos, *Algorithmic Accountability: Journalistic Investigation of Computational Power Structures*, in *Digital Journalism*, 2015, pp. 398-415.

per le VLOPs, un canale strutturato di accesso ai dati da parte di ricercatori accreditati[36]. Y-TRUST non è una VLOP, e dunque non vi è tenuto. Ma il principio, la separazione fra il soggetto che gestisce il dispositivo e il soggetto che lo studia, e la conseguente necessità di un canale formale di accesso al dato, è metodologicamente trasferibile, e la sua adozione volontaria sarebbe, per il progetto, un'ulteriore evidenza di postura *accountable*.

9. Conclusioni

Il valore di Y-TRUST (questo, almeno, è il nostro giudizio dopo la trattazione) sta meno nella sua capacità di amplificare il verificato che nella sua capacità di rendere visibile la stratificazione normativa che oggi grava su qualsiasi infrastruttura informativa europea. Costruire un dispositivo socio-tecnico contro il disordine informativo è possibile; ma richiede di assumere (non di nascondere) la complessità giuridica, etica e tecnica del costruirlo. La promessa, che riteniamo seria e non retorica, è quella di un'amplificazione fiduciaria del verificato che resista al *last-mile problem* del *fact-checking* tradizionale. Il prezzo è la disponibilità a navigare contemporaneamente GDPR, *Digital Services Act* e *AI Act*, senza scorciatoie.

Tre tesi portanti emergono dalla nostra analisi. La prima: l'architettura del dispositivo distribuisce le funzioni di verifica, mediazione, amplificazione e monitoraggio in modo che nessun singolo nodo concentri il rischio editoriale, e questa distribuzione è essa stessa una contromisura alla concentrazione del potere informativo (cfr. *supra*, §4). La seconda: la mediazione degli *influencer* è insieme la condizione di possibilità e la fragilità del dispositivo; la sua *governance* richiede *guardrail* contrattuali, deontologici e regolatori, di cui abbiamo proposto un primo abbozzo, e una vigilanza che non può essere delegata alla sola buona fede dei partecipanti (cfr. *supra*, §6). La terza: la conformità *by design* a un sistema normativo tripolare è il livello minimo, non massimo, di ambizione che un dispositivo come Y-TRUST può permettersi se vuole sopravvivere oltre la fase pilota (cfr. *supra*, §7).

Resta aperta una questione che il caso-studio non chiude e che ci sembra costituisca l'agenda più ampia entro cui collocare il lavoro futuro. Y-TRUST è un dispositivo *di parte*: dichiaratamente schierato dalla

[36] Art. 40, Reg. (UE) 2065/2022.

parte del verificato. La sua scalabilità geografica, linguistica, tematica, dipende dalla capacità di replicare l'infrastruttura fiduciaria in contesti istituzionali diversi, anche in contesti dove il *fact-checking* indipendente è osteggiato, dove gli *influencer* operano sotto pressione politica, dove l'infrastruttura tecnica non è disponibile o non è di proprietà pubblica. La risposta a queste sfide eccede l'oggetto del presente articolo, ma ne costituisce l'orizzonte. Su quell'orizzonte si misurerà, in ultima istanza, la portata di ciò che oggi si presenta come un caso italiano di amplificazione fiduciaria del verificato, e che intende invece, siamo persuasi, proporsi come un modello replicabile di architettura informativa europea.

Una riflessione conclusiva, infine, sulla collocazione disciplinare del lavoro. Questa trattazione si è mossa nello spazio di intersezione fra il diritto pubblico europeo del digitale, gli studi sulla disinformazione di matrice sociopsicologica e l'analisi socio-tecnica delle infrastrutture informative. Riteniamo che la rilevanza scientifica del caso Y-TRUST non risieda nella sua compiutezza (il dispositivo, alla data di questa trattazione, è ancora un progetto e non un esperimento concluso) ma nella sua capacità di rendere visibili le tensioni tipiche di un'intera generazione di iniziative *anti-disinformation* che, nel quinquennio successivo all'entrata in vigore del *Digital Services Act* e all'approvazione dell'*AI Act*, dovranno necessariamente disegnarsi entro lo stesso reticolo di vincoli giuridici e di scelte tecniche.

LA MENTE QUALE OBIETTIVO STRATEGICO: LA DIFESA DELLA DIMENSIONE COGNITIVA ATTRAVERSO LO SVILUPPO DEL PENSIERO CRITICO

Massimo Panizzi[*]

1. Premessa

Il mutamento della natura del conflitto rappresenta uno dei tratti distintivi dell'attuale fase storica. Se nel XX secolo la competizione strategica si è sviluppata prevalentemente nel dominio militare-industriale, il XXI secolo è caratterizzato da una progressiva estensione del confronto nella sfera cognitiva e percettiva. La pressione strategica non si esercita più soltanto attraverso la forza o la deterrenza, ma mediante l'influenza sui processi di interpretazione della realtà.

In tale contesto, la mente umana assume una centralità inedita. Essa non è più soltanto il luogo in cui il conflitto viene compreso o giudicato, ma diventa essa stessa oggetto e strumento del confronto strategico. Opinioni pubbliche, sistemi informativi e piattaforme digitali costituiscono oggi spazi di competizione permanente, nei quali l'obiettivo principale non è la conquista territoriale, bensì l'orientamento delle percezioni, delle emozioni e delle categorie interpretative.

Il presente lavoro si colloca in questa prospettiva e intende analizzare la guerra cognitiva come fenomeno strutturale delle democrazie contemporanee. L'assunto di fondo è che la risposta a tali dinamiche non possa essere esclusivamente tecnica o normativa. È necessario un approccio

[*] Generale di Corpo d'Armata (ris.) dell'Esercito Italiano.

culturale e strategico, fondato sul rafforzamento del pensiero critico, della consapevolezza cognitiva e dell'intelligenza culturale come fattori di sicurezza democratica.

2. *La trasformazione del conflitto e la centralità della mente*

Nel corso della storia, la guerra ha sempre riflesso la struttura profonda delle società che la combattevano. L'attuale fase storica è segnata da una trasformazione significativa: il conflitto non si manifesta più esclusivamente attraverso lo scontro armato, ma si sviluppa in modo continuo e diffuso all'interno delle architetture cognitive delle comunità politiche.

La mente umana non rappresenta più soltanto il luogo della comprensione del conflitto, ma diventa essa stessa oggetto di pressione strategica. Opinioni pubbliche, comunità digitali e individui iperconnessi sono al tempo stesso bersaglio e vettore di influenza. In tale contesto, la distinzione tra tempo di pace e tempo di guerra risulta sempre più sfumata, sostituita da una condizione di competizione cognitiva permanente[3].

Le piattaforme tecnologiche svolgono un ruolo centrale in questo processo. Esse non si limitano a veicolare informazioni, ma strutturano l'accesso alla realtà attraverso meccanismi di selezione, amplificazione e gerarchizzazione dei contenuti. La realtà non è negata, bensì filtrata. Ciò che appare nei flussi informativi assume rilevanza e legittimità, mentre ciò che resta invisibile perde progressivamente cittadinanza nel discorso pubblico.

La guerra cognitiva, al riguardo, non mira a imporre una verità alternativa, ma a compromettere la possibilità stessa di costruire una verità condivisa. Il suo obiettivo non è convincere, ma disorientare; non creare consenso, ma frammentarlo. Quando viene meno un orizzonte epistemico comune, la democrazia perde la propria capacità deliberativa e si trasforma in uno spazio dominato da reazioni emotive e polarizzazione[1].

In questo quadro, la sicurezza non può più essere concepita esclusivamente in termini militari o tecnologici. Difendere la sicurezza oggi significa anche difendere la capacità delle società di interpretare, comprendere e decidere in modo consapevole. La cultura e la formazione cognitiva diventano, pertanto, elementi strutturali della strategia.

[1] Cfr. M. CASTELLS, *Communication Power*, Oxford University Press, Oxford, 2009.

3. Dal dominio informativo al dominio cognitivo

Per gran parte della seconda metà del Novecento, la competizione strategica nel dominio informativo è stata concepita come una lotta per il controllo dei messaggi e dei canali di comunicazione. La guerra dell'informazione si fondava sull'assunto che l'influenza fosse esercitata principalmente attraverso la persuasione, la propaganda e la gestione delle narrazioni pubbliche.

Nel contesto contemporaneo, questo paradigma risulta superato. La guerra cognitiva rappresenta un'evoluzione qualitativa, poiché non agisce prevalentemente sui contenuti, ma sui processi mentali che regolano attenzione, interpretazione e giudizio[2]. L'obiettivo non è sostituire una convinzione con un'altra, bensì intervenire sulle condizioni stesse del pensiero.

L'ambiente informativo digitale contribuisce in modo determinante a questa trasformazione. La combinazione di sovraccarico informativo, l'accelerazione dei flussi comunicativi e la stimolazione emotiva continua producono una compressione del tempo cognitivo. In un contesto caratterizzato da urgenza permanente, la riflessione viene progressivamente marginalizzata, mentre la reazione immediata diventa la modalità dominante di risposta.

Gli algoritmi di selezione e raccomandazione svolgono un ruolo centrale in tale dinamica. Essi determinano quali contenuti siano visibili, rilevanti o prioritari, influenzando implicitamente l'agenda cognitiva degli individui. L'influenza assume così una forma indiretta e sistemica: non è necessario imporre un messaggio specifico, è sufficiente orientare l'attenzione[3].

La guerra cognitiva prospera in questo spazio, in cui la manipolazione non si presenta come atto ostile esplicito, ma coincide con il funzionamento ordinario dell'ecosistema informativo. Le società democratiche, fondate sull'apertura e sul pluralismo, risultano particolarmente esposte a tale pressione, poiché la libertà di espressione e la circolazione delle informazioni costituiscono al tempo stesso una risorsa e una vulnerabilità.

In questo quadro, la sicurezza cognitiva non può essere ridotta a un problema di contenuti falsi o ingannevoli. Essa riguarda la capacità delle

[2] Cfr. N. Bolt, E. Lange-Ionatamishvili, *The Next Generation Information Environment*, NATO Strategic Communications Centre of Excellence, Riga, 2026.

[3] Cfr. C. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton, 2017.

società di mantenere condizioni cognitive che consentano il giudizio critico, la deliberazione e la responsabilità individuale. La transizione dal dominio informativo al dominio cognitivo impone dunque un ripensamento profondo delle strategie di difesa democratica.

4. Il campo di battaglia algoritmico

Nel contesto della guerra cognitiva, il campo di battaglia non è più esclusivamente umano. I sistemi algoritmici non si limitano a supportare la comunicazione, ma intervengono attivamente nei processi di selezione, classificazione e prioritizzazione delle informazioni, esercitando un'influenza strutturale sull'esperienza della realtà.

L'automazione dei processi informativi introduce una trasformazione cruciale: l'influenza diventa sempre più *machine-driven*. Le competizioni cognitive si svolgono a livello di modelli, dati e sistemi di raccomandazione, spesso prima che l'essere umano entri consapevolmente nel processo decisionale[4]. Gli individui ne sperimentano gli effetti a valle, sotto forma di percezioni già strutturate.

Questo spostamento produce una progressiva delega dell'autorità cognitiva a sistemi tecnologici opachi. Ciò che è reso visibile nei flussi informativi appare legittimo e rilevante; ciò che resta invisibile perde progressivamente peso nel discorso pubblico. La realtà non viene negata, ma mediata secondo logiche non trasparenti e non sottoposte a controllo democratico diretto.

Una delle conseguenze principali di questo processo è la frammentazione dell'esperienza collettiva. Ogni individuo riceve una rappresentazione personalizzata del mondo, calibrata su comportamenti, preferenze ed emozioni. In assenza di un terreno epistemico comune, il confronto democratico s'indebolisce e lascia spazio a polarizzazioni emotive e identitarie[5].

Dal punto di vista strategico, il campo di battaglia algoritmico rappresenta una sfida che va oltre la dimensione tecnologica. La questione centrale non è soltanto come regolare i sistemi automatici, ma come preservare il controllo umano sui processi di senso. Senza una consapevolezza diffusa dei meccanismi di mediazione algoritmica, le società rischiano

[4] Cfr. N. BOLT, E. LANGE-IONATAMISHVILI, *The Next Generation Information Environment*, cit.

[5] Cfr. E. PARISER, *The Filter Bubble*, Penguin Press, New York, 2011.

di perdere la capacità di interpretare criticamente la realtà che esse stesse producono.

5. La frammentazione della realtà e la dissoluzione dello spazio pubblico

Uno degli effetti più rilevanti della trasformazione dell'ambiente informativo contemporaneo è la progressiva frammentazione della realtà condivisa. Le democrazie moderne si sono storicamente fondate sull'esistenza di uno spazio pubblico nel quale fatti e informazioni, pur interpretati in modo diverso, erano riconosciuti come base comune del confronto politico. Tale presupposto risulta oggi sempre più fragile.

La personalizzazione algoritmica dei contenuti informativi produce ambienti percettivi differenziati, nei quali ogni individuo accede a una selezione della realtà coerente con le proprie preferenze, convinzioni ed emozioni[6]. Questo processo non genera pluralismo, ma isolamento cognitivo. La moltiplicazione delle cosiddette *echo chambers* riduce l'esposizione alla complessità e rafforza meccanismi di conferma identitaria.

Nel contesto della guerra cognitiva, la frammentazione della realtà non è un effetto collaterale, ma una condizione strategicamente vantaggiosa. Non è necessario imporre una narrazione dominante; è sufficiente impedire la costruzione di un terreno epistemico comune. Quando viene meno la possibilità di riconoscere fatti condivisi, il confronto democratico si trasforma in una competizione permanente di percezioni.

La dissoluzione dello spazio pubblico produce un indebolimento strutturale della fiducia: nelle istituzioni, nei media, nella competenza e, più in generale, nella possibilità stessa di una conoscenza affidabile. In assenza di fiducia, la deliberazione democratica perde efficacia e si riduce a una sequenza di reazioni emotive polarizzate[7].

Difendere lo spazio pubblico oggi significa, quindi, difendere la possibilità di una realtà condivisa, pur nella legittima diversità delle interpretazioni. Si tratta di una sfida eminentemente culturale, che richiede strumenti di consapevolezza cognitiva più che soluzioni meramente tecniche.

[6] Cfr. *ibidem*.

[7] Cfr. C. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, cit.

6. *La crisi dell'autorità della conoscenza*

La frammentazione della realtà condivisa conduce a una crisi più profonda e strutturale: la crisi dell'autorità della conoscenza. In un ambiente informativo saturo e "disintermediato", diventa sempre più difficile stabilire chi sia legittimato a definire ciò che è vero, rilevante o affidabile.

Le istituzioni tradizionalmente deputate alla produzione e alla validazione del sapere – scuola, università, stampa, comunità scientifica – vedono progressivamente erosa la loro autorevolezza. Tale fenomeno non deriva necessariamente da una perdita di competenza, ma dalla trasformazione dell'ecosistema informativo, nel quale l'autorità è percepita come sospetta e l'intermediazione come una forma di controllo[8].

In questo vuoto si inseriscono i sistemi tecnologici. Motori di ricerca, piattaforme digitali e sistemi di intelligenza artificiale assumono un ruolo crescente nella selezione e nell'organizzazione delle informazioni. Essi non dichiarano cosa sia vero, ma determinano cosa sia visibile. In un contesto cognitivo, la visibilità equivale spesso alla legittimità.

Si assiste così a un cambio di regime epistemico: il dibattito pubblico non verte più sulla solidità delle evidenze, ma sulla fiducia nel sistema che le ordina e le presenta. La domanda fondamentale non è più «è vero?», bensì «chi lo rende credibile?»[9]. La guerra cognitiva opera precisamente su questa faglia, contaminando l'ecosistema della conoscenza piuttosto che sostituirlo.

La delega dell'autorità epistemica a sistemi automatizzati comporta un rischio strutturale per le democrazie. Laddove il potere di definire il senso non è più ancorato a responsabilità umane e a processi trasparenti, la legittimità democratica si indebolisce.

Difendere la conoscenza significa dunque preservare la capacità umana di giudicare, distinguere e assumersi la responsabilità del discernimento.

7. *Emozioni, neuroscienze e manipolazione della* pietas

La guerra cognitiva non opera principalmente sul piano della razionalità, ma su quello delle emozioni. Le neuroscienze hanno dimostrato che le risposte emotive precedono e orientano l'elaborazione cognitiva, influenzando in modo significativo il processo decisionale.

[8] Cfr. T. NICHOLS, *The Death of Expertise*, Oxford University Press, Oxford, 2017.
[9] Cfr. L. FLORIDI, *The Fourth Revolution*, Oxford University Press, Oxford, 2014.

Le strategie cognitive contemporanee sfruttano questa architettura neurobiologica. I messaggi più efficaci non sono necessariamente quelli più accurati, ma quelli emotivamente più attivanti. In questo senso, la guerra cognitiva non mira a convincere, bensì a innescare reazioni. Paura, indignazione e compassione diventano leve strategiche.

Tra queste emozioni, la *pietas* occupa una posizione centrale. Intesa come riconoscimento della vulnerabilità dell'altro e responsabilità morale verso la sofferenza, essa rappresenta un valore fondamentale delle società democratiche. Proprio per questo, è particolarmente esposta alla strumentalizzazione.

La selezione delle vittime degne di empatia, la decontestualizzazione del dolore e la narrazione emotiva asimmetrica possono orientare giudizi morali e posizioni politiche senza passare attraverso la comprensione razionale[10]. Il problema non è l'emozione in sé, ma la sua separazione dal contesto cognitivo e culturale.

Quando la *pietas* non è accompagnata dal pensiero critico, si trasforma in reazione automatica. La guerra cognitiva non distrugge l'etica, ma la utilizza. Recuperare la *pietas* nella sua autenticità significa reintegrarla in un quadro interpretativo che ne impedisca l'uso manipolatorio e la renda compatibile con il discernimento.

8. Il pensiero critico come infrastruttura strategica

Nel dibattito pubblico contemporaneo, il pensiero critico è spesso trattato come una competenza individuale o come un obiettivo educativo di carattere generale. Tale impostazione ne riduce la portata strategica. Nell'ambito della guerra cognitiva, il pensiero critico deve essere invece considerato una infrastruttura immateriale essenziale per la sicurezza e la resilienza delle democrazie.

Il pensiero critico non coincide con lo scetticismo sistematico né con il relativismo epistemologico. Esso presuppone l'esistenza di criteri di verità e di affidabilità, pur riconoscendo la complessità dei fenomeni e la fallibilità dei processi conoscitivi. In termini operativi, consiste nella capacità di distinguere tra fatti, interpretazioni e opinioni, di valutare le fonti, di riconoscere *bias* cognitivi e di collocare le informazioni nel loro contesto[11].

[10] Cfr. G. Le Bon, *La psychologie des foules* (1895), Hogwords, Torino, 2022.
[11] Cfr. D. Kahneman, *Thinking, Fast and Slow*, Farrar, Straus & Giroux, New York, 2011.

Dal punto di vista strategico, il pensiero critico introduce un elemento di attrito cognitivo all'interno dell'ecosistema informativo. Esso rallenta la risposta immediata agli stimoli emotivi, interrompe l'automatismo della reazione e restituisce spazio alla deliberazione. Proprio per questo motivo, il pensiero critico rappresenta uno degli obiettivi indiretti della guerra cognitiva, la quale tende a renderlo impraticabile attraverso saturazione informativa e accelerazione comunicativa.

Una società in cui il pensiero critico è diffuso e strutturalmente sostenuto risulta meno vulnerabile alla manipolazione. Ciò non elimina il conflitto, ma lo rende governabile all'interno di procedure democratiche. Al contrario, l'assenza di attrito cognitivo favorisce polarizzazione, radicalizzazione e delega emotiva delle decisioni.

Considerare il pensiero critico come infrastruttura implica riconoscere che esso non può essere lasciato alla sola iniziativa individuale. Esso deve essere coltivato sistemicamente, attraverso politiche educative, culturali e comunicative coerenti. La sua erosione non produce soltanto disinformazione, ma una vera e propria insicurezza cognitiva, con ricadute dirette e pesanti sulla legittimità democratica.

9. Intelligenza culturale e consapevolezza cognitiva

Se il pensiero critico fornisce gli strumenti analitici per valutare informazioni e argomentazioni, l'intelligenza culturale rappresenta la capacità di interpretare i messaggi nel loro contesto simbolico, storico e antropologico. Nel caso della guerra cognitiva, tale competenza assume una rilevanza strategica.

Le narrazioni non operano mai in modo astratto. Esse parlano alle identità, alle memorie collettive, ai codici culturali e ai sistemi di valori. Senza la capacità di riconoscere questi livelli, l'individuo resta esposto a una doppia vulnerabilità: reagisce emotivamente e interpreta in modo decontestualizzato ciò che osserva[12].

L'intelligenza culturale consente di distinguere tra valori universalistici e rappresentazioni culturali specifiche, evitando letture letterali o semplificate di messaggi costruiti per produrre reazioni emotive immediate. In questo senso, essa costituisce una forma di difesa cognitiva preventiva, che agisce prima della polarizzazione.

[12] Cfr. S. ANG, L. VAN DYNE, *Handbook of Cultural Intelligence*, Routledge, Londra, 2008.

La consapevolezza cognitiva nasce dall'integrazione tra pensiero critico e intelligenza culturale. Quest'ultima può essere definita come la capacità di riconoscere non solo il contenuto di un messaggio, ma anche il contesto che lo rende efficace. Significa comprendere quando una determinata reazione emotiva viene sollecitata strategicamente, quali *bias* vengono attivati e quali interessi ne traggono beneficio.

Dal punto di vista strategico, la consapevolezza cognitiva trasforma l'individuo da bersaglio passivo a soggetto interpretante. Non elimina il conflitto, ma ne limita la capacità di colonizzare la mente. In assenza di tale consapevolezza, la guerra cognitiva opera in modo silenzioso e pervasivo, sfruttando vulnerabilità culturali più che informative.

10. Educazione, leadership *e resilienza democratica*

La difesa cognitiva delle democrazie non può essere affidata esclusivamente alla responsabilità individuale. Essa richiede una strategia educativa e culturale di lungo periodo, capace di rafforzare in modo sistemico le capacità di discernimento e interpretazione dei cittadini.

L'educazione alla consapevolezza cognitiva non coincide con la semplice alfabetizzazione digitale o informativa. Essa implica l'apprendimento del pensiero critico, la comprensione dei meccanismi emotivi e la capacità di riconoscere le dinamiche culturali che rendono efficaci le narrazioni. In questo senso, scuola e università non sono soltanto luoghi di trasmissione del sapere, ma spazi di formazione del giudizio[13].

Accanto all'educazione, la *leadership* svolge un ruolo determinante. I leader politici, istituzionali e culturali non sono soltanto decisori, ma modelli cognitivi. Il modo in cui interpretano la realtà, comunicano le crisi e gestiscono l'emotività collettiva, incide direttamente sulla resilienza o sulla fragilità delle società democratiche.

Una *leadership* che semplifica e polarizza accelera la degradazione cognitiva dello spazio pubblico. Al contrario, una *leadership* che spiega, contestualizza e riconosce la complessità contribuisce a rafforzare la fiducia e la capacità deliberativa. In questo quadro, la resilienza democratica non è il risultato di un singolo intervento, ma di una cultura condivisa del discernimento.

Investire in educazione e *leadership* responsabile significa investire nella capacità delle democrazie di resistere alla pressione cognitiva senza rinunciare ai propri principi fondamentali.

[13] Cfr. J. Dewey, *Democracy and Education* (1916), Simon & Brown, Londra, 2011.

11. Conclusioni: difendere la democrazia significa difendere la capacità di pensare

L'analisi svolta nei capitoli precedenti mostra come il conflitto contemporaneo abbia progressivamente oltrepassato i confini tradizionali della dimensione militare e informativa per insediarsi in modo strutturale nella sfera cognitiva. La guerra cognitiva non rappresenta una tecnica accessoria delle minacce ibride, ma una trasformazione profonda del modo in cui il potere è esercitato e contestato[14].

In questo nuovo contesto strategico, la mente umana diventa il principale terreno di competizione. Non attraverso forme evidenti di coercizione, ma mediante la frammentazione della realtà, la saturazione emotiva e l'erosione dell'autorità della conoscenza. Il risultato non è l'adesione a una narrazione alternativa, bensì la perdita delle condizioni cognitive che rendono possibile una deliberazione democratica condivisa[15].

Le democrazie risultano particolarmente esposte a questa forma di pressione. Fondate sull'apertura, sul pluralismo e sulla libertà di espressione, esse presuppongono cittadini capaci di discernere, confrontare e giudicare. Quando tali capacità risultano indebolite, la democrazia non collassa improvvisamente, ma si svuota dall'interno: le istituzioni restano formalmente in piedi, mentre la fiducia che le sostiene si dissolve[16].

L'elemento più critico che emerge dall'analisi è la crisi dell'autorità della conoscenza. In un ambiente informativo mediato da sistemi algoritmici opachi, la distinzione tra vero e falso tende a essere sostituita dalla distinzione tra visibile e invisibile. La delega dell'autorità epistemica a sistemi automatici, percepiti come neutrali ma non responsabili, rappresenta una deriva incompatibile con i principi democratici[17].

Di fronte a questa sfida, le risposte puramente tecniche – regolamentazione delle piattaforme, contrasto alla disinformazione, *fact-checking* – risultano necessarie ma insufficienti. Esse intervengono sugli effetti, non sulle cause. La vera posta in gioco è la capacità delle società di preservare il controllo umano sui processi di senso.

In tale prospettiva, il pensiero critico emerge come una vera e propria infrastruttura strategica. Esso introduce attrito cognitivo, rallenta la

[14] Cfr. N. BOLT, E. LANGE-IONATAMISHVILI, *The Next Generation Information Environment*, cit.

[15] Cfr. C. SUNSTEIN, *#Republic: Divided Democracy in the Age of Social Media*, cit.

[16] Cfr. L. FREEDMAN, *The Future of War*, cit.

[17] Cfr. L. FLORIDI, *The Fourth Revolution*, cit.

reazione immediata e restituisce spazio alla deliberazione. Senza pensiero critico diffuso, la libertà d'informazione si trasforma in vulnerabilità strutturale[18].

Accanto al pensiero critico, l'intelligenza culturale e la consapevolezza cognitiva svolgono un ruolo decisivo. Le narrazioni agiscono sempre all'interno di contesti simbolici e identitari. La capacità di riconoscere tali contesti consente di sottrarsi alla manipolazione empatica e alla strumentalizzazione di emozioni fondamentali come la *pietas*, restituendo all'etica una dimensione riflessiva e responsabile.

Educazione e *leadership* rappresentano, in questo quadro, i pilastri della resilienza democratica. Educare non significa soltanto trasmettere informazioni, ma formare il giudizio. Guidare non significa soltanto decidere, ma offrire modelli cognitivi responsabili. Una *leadership* che semplifica e polarizza accelera la fragilità cognitiva; una *leadership* che spiega, contestualizza e riconosce la complessità rafforza la fiducia e la coesione.

Difendere la democrazia oggi significa quindi proteggere la capacità di pensare in modo libero, consapevole e responsabile. Non si tratta di orientare ciò che le persone devono pensare, ma di preservare le condizioni che rendono possibile il pensiero stesso. In un'epoca di automazione crescente, la tutela dell'autorità umana sul giudizio non è un ostacolo al progresso, ma una condizione essenziale della libertà.

[18] Cfr. T. Nichols, *The Death of Expertise*, cit.

CONFLITTI E CONFINI IMMATERIALI. VIOLENZA IBRIDA, PROPAGANDA E GOVERNO DEL CAOS

Vincenzo D'Anna[*]

1. *Introduzione*

Le forme attuali di competizione internazionale si sviluppano sempre più spesso in spazi ambigui, nei quali diventa difficile distinguere tra pace e conflitto, informazione e manipolazione, confronto politico legittimo e azione ostile intenzionale. Non siamo più soltanto davanti a minacce che occupano territori o distruggono infrastrutture, ma a dinamiche che agiscono progressivamente sulle percezioni, sulle emozioni, sulla fiducia e sulla capacità di giudizio delle collettività.

Questa condizione è particolarmente evidente quando l'obiettivo riguarda gli elementi fondanti delle democrazie liberali. In questi sistemi, aperti per natura al pluralismo, alla libertà di espressione e alla competizione delle idee, l'attacco può assumere forme indirette e difficili da attribuire. Non sempre punta a imporre una verità alternativa; spesso mira piuttosto a indebolire la possibilità stessa di riconoscere un terreno comune di realtà, di fiducia e di decisione. Il conflitto cognitivo si sviluppa precisamente in questo spazio fluido, dove gli strumenti tradizionali della sicurezza si intrecciano con dimensioni simboliche, percettive e narrative, e dove l'obiettivo non è necessariamente la distruzione fisica dell'avversario, ma la alterazione delle condizioni entro cui individui e collettività percepiscono, interpretano e decidono.

In tale prospettiva, la tecnologia non va intesa come causa originaria di queste dinamiche, bensì come potente fattore di accelerazione,

[*] Co-fondatore di DYNAMES e Consigliere della Federazione Relazioni Pubbliche Italiana (FERPI) del Lazio.

amplificazione e diffusione di processi relazionali, psicologici e politici più profondi. Il centro di gravità del conflitto resta l'uomo, non soltanto come individuo, ma come parte di una collettività esposta a flussi informativi continui, a stimoli emotivi concorrenti e a meccanismi di influenza sempre più difficili da attribuire e da contenere. La guerra cognitiva si colloca dunque all'incrocio tra dimensione politica, sfera pubblica e struttura comunicativa delle società contemporanee, ponendo interrogativi che investono direttamente la tenuta del consenso democratico, la qualità della deliberazione e la stabilità dell'ordine liberale.

Il presente contributo non ambisce a fornire una lettura totalizzante del fenomeno, ma propone una chiave di analisi orientata ad individuare alcune logiche profonde della minaccia ibrida nei confronti delle democrazie contemporanee. In primo luogo, il lavoro ricostruisce il progressivo slittamento dalla centralità della coercizione fisica verso forme indirette di influenza cognitiva. In secondo luogo, esamina la propaganda come componente strutturale delle società di massa, mostrando come il suo ruolo si sia progressivamente trasformato dall'orientamento del consenso alla frammentazione sistemica della volontà collettiva. Infine, dedica particolare attenzione al passaggio dalla vulnerabilità del singolo alla dinamica emergente del comportamento collettivo, evidenziando come, in ambienti caratterizzati da volatilità, polarizzazione, non linearità e saturazione informativa, il caos possa essere analizzato non soltanto come effetto della complessità, ma come possibile strumento di vantaggio strategico.

Da questa prospettiva, la difesa delle democrazie liberali non può essere ridotta alla protezione di infrastrutture o alla smentita di singoli contenuti falsi. Essa richiede piuttosto una riflessione più ampia sulle condizioni cognitive, culturali e istituzionali che rendono possibile l'esercizio consapevole della libertà politica. È su questo terreno, immateriale ma decisivo, che si colloca oggi una parte crescente della competizione strategica.

2. *Il concetto di violenza e il superamento della coercizione fisica*

Nel dibattito strategico e politologico contemporaneo, il concetto di violenza richiede una ridefinizione che tenga conto delle profonde trasformazioni intervenute nei rapporti tra potere, società e conflitto. Lungi dal poter essere interpretata esclusivamente come deviazione patologica dell'ordine politico, la violenza costituisce una costante strutturale del-

la convivenza umana e dell'organizzazione del potere. Come mostrato dalla tradizione del pensiero politico moderno, essa non rappresenta un accidente eliminabile, bensì un elemento fisiologico in continua trasformazione.

Già in Hobbes la violenza emerge come sfondo permanente della condizione umana: l'ordine politico – e si intenda anche quello internazionale – nasce precisamente dall'esigenza di contenere e regolare una conflittualità originaria che, se lasciata priva di argini, renderebbe impossibile qualsiasi forma stabile di cooperazione sociale[1]. In questa prospettiva, lo Stato – e in diverse forme e tentativi le organizzazioni regionali e internazionali – si configura come detentore del monopolio della forza, non per negare la violenza, ma per sottrarla alla dispersione e ricondurla a una forma centralizzata e prevedibile. Max Weber, riprendendo e modernizzando tale intuizione, definirà lo Stato come l'istituzione che rivendica il monopolio della violenza legittima, collocando l'uso della forza all'interno di un quadro di responsabilità politica e di razionalità strumentale[2].

Questa impostazione consente di cogliere un primo elemento decisivo: la violenza non scompare con la modernità, ma viene progressivamente normata, amministrata e giustificata in funzione della stabilità dell'ordine politico. Ciò che muta, nel tempo, non è la sua presenza, bensì la sua efficacia relativa come strumento di governo e di competizione tra attori. È su questo punto che si innesta la riflessione di Hannah Arendt, la quale distingue con nettezza la relazione tra potere e violenza, mostrando come il ricorso crescente a quest'ultima segnali, paradossalmente, una crisi del primo[3]. Nelle società complesse e altamente organizzate, l'uso sistematico della violenza fisica tende a produrre costi politici, simbolici e di legittimazione sempre più elevati, riducendone l'efficacia strategica complessiva. È il caso della bomba atomica, che segna il picco storico dell'uso della violenza dopo il quale ogni simile azione può rivelarsi addirittura controproducente e sposta l'essenza della sua efficacia dal piano dell'effettivo uso alla mera rappresentazione simbolica come elemento di deterrenza.

In questo quadro, la violenza tende a spostarsi dal piano visibile della coercizione fisica a quello meno tangibile, ma non meno incisivo, dell'in-

[1] Cfr. T. Hobbes, *Leviatano*, (1651), Bur, Milano, 2011, Cap. XIII.

[2] M. Weber, *La scienza come professione. La politica come professione*, (1919), Einaudi, Torino, 2004, pp. 66-67.

[3] Cfr. H. Arendt, *Sulla violenza*, (1969), Guanda, Milano, 2023, parte III.

fluenza cognitiva. L'obiettivo non è più primariamente la distruzione delle capacità materiali dell'avversario, bensì la modifica del suo orizzonte percettivo e decisionale. Tale slittamento è stato descritto, in chiave prevalentemente analitica e non come dottrina univoca, nelle riflessioni sulla cosiddetta *Fifth Generation Warfare* (5GW), che individua forme di conflitto caratterizzate dall'assenza di dichiarazioni formali di guerra, dalla difficoltà di attribuzione delle responsabilità e dalla prevalenza di azioni "sottosoglia", volte a incidere sulla volontà politica e sulla coesione sociale più che sul confronto armato diretto[4]. In questa prospettiva, la violenza non viene negata, ma ricondotta a modalità indirette, diffuse e continuative.

Le riflessioni di Thomas C. Schelling e di Alexander L. George consentono di tradurre questa dinamica in termini strategici. In *Arms and Influence*, Schelling mostra come la violenza, o anche solo la sua minaccia, operi principalmente come forma di comunicazione, volta a manipolare aspettative, percezioni del rischio e calcoli di convenienza[5]. George, elaborando il concetto di *coercive diplomacy*[6], evidenzia come la pressione politica possa essere esercitata efficacemente attraverso una combinazione calibrata di segnali, ambiguità e credibilità, riducendo il ricorso al confronto armato diretto. Nel contesto contemporaneo, tale pressione tende inoltre a intrecciarsi con forme di *public diplomacy* e *media diplomacy*[7], cioè con modalità di influenza rivolte direttamente ai pubblici di Stati terzi senza la mediazione esclusiva dei canali diplomatici tradizionali. In entrambi i casi, la dimensione cognitiva si rivela centrale: il successo non dipende dalla quantità di forza impiegata, ma dalla capacità di incidere sui processi decisionali dell'altro.

La considerazione di Serge Tchakhotine sulla propaganda come "violenza psichica"[8] consente infine di cogliere con particolare lucidità la natura di questo slittamento. Analizzando i meccanismi di mobilitazione di massa del primo Novecento, il sociologo tedesco evidenziava come

[4] A.D. ABBOTT, *The Handbook of 5GW: A Fifth Generation of War?*, Nimble, Oakham, 2010, pp. 15-17.

[5] Cfr. T.C. SCHELLING, *Arms and Influence*, (1966), Yale University Press, New Haven, 2020, pp. 21-22.

[6] A.L. GEORGE, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*, United States Institute of Peace, 1992, p. 25.

[7] G. ANZERA, A. MASSA, *Media diplomacy e narrazioni strategiche. Autorappresentazione dello Stato e attuazione della politica estera in rete*, Bonanno, Acireale, 2017, p. 53.

[8] Cfr. S. TCHAKHOTINE, *Le des foules par la propagande politique*, (1952), Gallimard, Parigi, 2015, pp. 13-17.

l'azione politica moderna potesse fare a meno della coercizione fisica sistematica, facendo invece leva su stimoli simbolici ed emotivi capaci di produrre comportamenti prevedibili e conformi. In questa stessa direzione si colloca, in forma ancora embrionale ma sorprendentemente lucida, l'analisi di Arthur Ponsonby sui meccanismi ricorrenti della propaganda bellica. Già all'indomani della Prima guerra mondiale, Ponsonby mostrava come essa operasse attraverso schemi ricorrenti volti a costruire consenso, ridurre la complessità e neutralizzare preventivamente il dissenso, anticipando così l'idea di una manipolazione sistematica delle percezioni come alternativa alla forza. Tali schemi sono stati successivamente sistematizzati da Anne Morelli nei suoi «Principi elementari della propaganda di guerra». I "dieci principi" non costituiscono singoli messaggi, ma vere e proprie matrici operative sul campo cognitivo, tuttora richiamate nella riflessione sulla comunicazione politica[9].

Infine, tali intuizioni trovano un'eco significativa nelle analisi contemporanee di Byung-Chul Han, secondo cui le forme attuali di potere tendono a operare non attraverso l'imposizione esterna, ma mediante processi di interiorizzazione e auto-sfruttamento cognitivo[10]. Nel contesto dei sistemi democratici liberali, il superamento della centralità esclusiva della violenza fisica non coincide dunque con una sua scomparsa, ma con la sua trasfigurazione e con la sua integrazione in forme più sottili e pervasive. La violenza cognitiva si configura come integrazione necessaria della violenza tradizionale, più compatibile con società complesse, interdipendenti e sensibili ai costi politici della coercizione diretta. Essa agisce sui presupposti cognitivi e simbolici della convivenza democratica, ponendo interrogativi ineludibili sulla tenuta dei processi deliberativi e sulle condizioni di possibilità del consenso.

3. L'essenza della propaganda nelle democrazie liberali

La propaganda rappresenta uno degli elementi più controversi e, al tempo stesso, più strutturali della vita politica nelle democrazie contemporanee. Lungi dall'essere un'anomalia o una deviazione patologica del processo democratico, essa si configura, come ha mostrato in modo par-

[9] A. Morelli, *Principi elementari della propaganda di guerra. Utilizzabili in caso di guerra fredda, calda o tiepida*, Futura Editrice, Roma, 2005.

[10] B.-C. Han, *Psicopolitica. Il neoliberismo e le nuove tecniche del potere*, Nottetempo, Milano, 2016, pp. 8-9.

ticolarmente netto Jacques Ellul, come una componente fisiologica delle società di massa fondate sul consenso. In sistemi politici in cui il potere non può essere esercitato stabilmente attraverso la coercizione, la convergenza delle volontà individuali verso una direzione comune diventa una necessità funzionale. La propaganda risponde precisamente a questa esigenza: orientare, stabilizzare e rendere durabile il consenso all'interno di comunità politiche complesse[11].

In una democrazia liberale, infatti, la decisione politica non è mai l'espressione di una volontà unitaria preesistente, ma il risultato di un processo di mediazione tra interessi, valori e aspettative differenti. La politica democratica è, per sua natura, un'operazione di sintesi e di compromesso, nella quale la pluralità delle volontà individuali viene ricondotta a una linea d'azione condivisa. In tale contesto, Bernays prima e successivamente Ellul, hanno ragione nel sostenere che la propaganda non costituisca un corpo estraneo alla democrazia, bensì uno strumento attraverso cui essa riesce a funzionare e a mantenere un minimo di coesione interna. Essa opera come meccanismo di integrazione, rafforzando l'adesione ai presupposti del patto democratico e consolidando lo *status quo* di coloro che occupano una posizione di forza nel sistema politico[12].

Questa dinamica si manifesta su almeno due piani distinti. Sul piano interno, la propaganda contribuisce a stabilizzare la maggioranza intesa non solo come dato numerico, ma come insieme di cittadini che riconoscono e accettano le regole del gioco democratico. Sul piano esterno, essa diviene uno strumento di posizionamento strategico, attraverso il quale gli Stati proiettano la propria influenza su attori terzi, senza ricorrere necessariamente alla coercizione militare. Le esperienze storiche di esercizio dello *smart power* mostrano come la capacità di orientare percezioni e preferenze possa risultare decisiva quanto il controllo delle risorse materiali[13].

È tuttavia proprio questa natura strutturale della propaganda a renderla un potenziale fattore di vulnerabilità per le democrazie liberali. Come ha osservato Tzvetan Todorov, tali sistemi politici sono minacciati non tanto da nemici esterni, quanto dalle loro stesse predisposizioni interne. I principi che fondano la democrazia – libertà, sovranità popolare,

[11] J. ELLUL, *Propaganda: The Formation of Men's Attitudes*, Vintage, New York, 1973, pp. 3-7.

[12] Cfr. E.L. BERNAYS, *Propaganda* (1928), ShaKe, Milano, 2020, p. 9.

[13] Cfr. J.S. NYE, *Soft Power. The Means to Success in World Politics*, Public Affairs, New York, 2004.

pluralismo – possono trasformarsi, se assolutizzati e sganciati dai necessari equilibri istituzionali e normativi, in strumenti di erosione dall'interno. La propaganda "nera"[14] si inserisce in questa tensione, sfruttando le aperture del sistema democratico per amplificarne le contraddizioni[15].

Il voto universale rappresenta, in questo senso, la massima espressione della libertà politica e dell'equilibrio tra volontà individuali e, proprio per questo, costituisce anche un punto di particolare esposizione. Processi decisionali concentrati in singoli eventi – come referendum o consultazioni plebiscitarie – offrono occasioni privilegiate per interventi di influenza intenzionale, volti a orientare l'esito complessivo agendo selettivamente su segmenti dell'elettorato. In tali contesti, la cittadinanza tende a trasformarsi in un pubblico permanentemente esposto e reattivo, che può essere profilato, "targettizzato" e polarizzato in modo sistematico, non tanto attraverso l'imposizione di specifici contenuti, quanto mediante lo sfruttamento congiunto del sovraccarico informativo e delle predisposizioni cognitive ed emotive preesistenti. Come evidenzia Di Gregorio, l'erosione dei processi deliberativi e la centralità dell'attivazione emotiva favoriscono una forma di consenso immediato e volatile, rendendo la partecipazione politica dei cittadini più vulnerabile a dinamiche di semplificazione, polarizzazione e manipolazione cognitiva[16].

Ci si sofferma ora sulla dimensione individuale e sul ruolo del singolo che compone il complesso sociale: il cittadino, oggi "*net citizen*" o "*netizen*"[17]. Immerso in un flusso informativo continuo, ipertrofico e ridondante, l'individuo dispone di un accesso potenzialmente illimitato alle informazioni a fronte di risorse cognitive limitate per elaborarle cri-

[14] La distinzione tra propaganda bianca e propaganda nera costituisce un elemento classico della dottrina della guerra psicologica. Come evidenziato da Linebarger, la propaganda bianca è caratterizzata da una fonte dichiarata e riconoscibile, generalmente istituzionale, mentre la propaganda nera si fonda sulla dissimulazione della fonte reale e sull'attribuzione fittizia del messaggio. La letteratura successiva ha ulteriormente sviluppato questa distinzione introducendo la categoria intermedia della propaganda grigia, riferita a forme di comunicazione caratterizzate da attribuzione ambigua o parziale; cfr. P.M.A. Linebarger, *Psychological Warfare,* (1948), Martino, 2020, pp. 30-50.

[15] T. Todorov, *I nemici intimi della democrazia*, Garzanti, Milano, 2012, pp. 13, 17, 202.

[16] L. Di Gregorio, *Demopatìa. Sintomi, diagnosi e terapie del malessere democratico*, Rubbettino, Soveria Mannelli, 2019, pp. 9-10.

[17] Per gli aspetti qui trattati, meritano citazione i concetti di "*citizen journalist*" e "*citizen diplomats*" per indicare cittadini della rete che si dedicano in modo non professionale o addirittura improvvisato al giornalismo e alla trattazione di tematiche diplomatiche; cfr. A. Valeriani, *Twitter factor*, Laterza, Bari-Roma, 2011, p. 4.

ticamente. Ne deriva una crescente dipendenza da schemi interpretativi semplificati, coerenti con i propri *bias* cognitivi e rafforzati da ambienti informativi omofili. In tale contesto, la propaganda contemporanea non impone più una narrazione unitaria, ma frammenta lo spazio del senso, combinando macro-narrazioni rivolte all'infosfera generale e micro-narrazioni adattate a pubblici specifici. Questa trasformazione si riflette empiricamente, non in termini deterministici ma come tendenza strutturale osservata, nella discrepanza tra l'elevata esposizione a contenuti politici sui social media e la persistente o crescente disaffezione verso la partecipazione elettorale tradizionale. Studi comparativi mostrano come l'intensa attività politica online favorisca forme di partecipazione espressiva e identitaria, senza tradursi in un aumento sistematico dell'affluenza alle urne[18]. In alcuni casi, la dipendenza dai social come fonte primaria di informazione politica risulta addirittura associata a una minore propensione al voto.

Il passaggio da una propaganda intesa come gestione dei flussi del consenso a una logica di frammentazione cognitiva produce così un indebolimento strutturale dell'immaginario democratico condiviso. La moltiplicazione dei *frame* e delle narrazioni non rafforza il legame tra informazione, decisione e azione collettiva, ma lo dissolve, contribuendo a una sfiducia sistemica nelle istituzioni e nella capacità del voto di produrre cambiamento politico significativo[19]. Seppur formulata in un contesto storico e culturale radicalmente diverso, questo concetto è rintracciabile nello Stratagemma XX della tradizione strategica cinese, noto come «intorbidire l'acqua per catturare i pesci»[20]. Il principio sotteso, che sarà successivamente approfondito, non consiste nell'annientamento frontale dell'avversario, bensì nella creazione deliberata di confusione e disordine, tali da compromettere la sua capacità di discernimento e di reazione coerente.

Non solo. Altri contributi recenti aiutano a rendere più leggibile la natura concreta della minaccia. Byung-Chul Han ha mostrato come le forme contemporanee di potere tendano a operare meno attraverso la coercizione esplicita e più mediante meccanismi di auto-sfruttamento cognitivo: l'individuo non è costretto dall'esterno, ma è indotto a esporsi

[18] S. BOULIANNE, *Social Media Use and Participation*, in *Information, Communication & Society*, 18(5), 2015.

[19] L. DI GREGORIO, *Demopatìa. Sintomi, diagnosi e terapie del malessere democratico,* cit.

[20] G. MAGI, *I 36 Stratagemmi*, Il Punto d'Incontro, Vicenza, 2014, p. 203.

volontariamente, a produrre contenuti, a reagire continuamente a stimoli informativi e a prendere posizione su questioni sempre nuove. La partecipazione costante al dibattito pubblico digitale, l'obbligo implicito di "esserci" e di esprimere un'opinione, trasformano così l'attenzione in una risorsa continuamente consumata, spesso senza che vi sia il tempo o lo spazio per una reale elaborazione critica[21]. Su un piano complementare, Bernard Stiegler ha posto l'accento sul ruolo dell'attenzione e del tempo come risorse strategiche. Nel contesto attuale, la competizione cognitiva non si gioca tanto sulla falsità o veridicità dei singoli contenuti, quanto sulla saturazione dell'ambiente informativo: l'accelerazione dei flussi, la moltiplicazione dei canali e la sovrapposizione di temi politici, emotivi e identitari riducono la capacità dei cittadini di distinguere ciò che è rilevante da ciò che è contingente. In questa prospettiva, la propaganda non agisce più soltanto convincendo, ma modellando l'ecosistema cognitivo nel quale le decisioni prendono forma, rendendo strutturale la reazione immediata e intermittente[22]. La conseguenza è una dinamica politica sempre più orientata al breve termine. Governi e attori politici si trovano a rispondere a crisi comunicative continue, a oscillazioni dell'opinione pubblica misurate in tempo reale e a campagne di influenza che sfruttano l'emotività del momento. In tale contesto, la programmazione strategica di lungo periodo diventa difficile da sostenere, mentre prevalgono logiche di *marketing* politico e di competizione elettorale permanente, nelle quali la gestione dell'attenzione conta spesso più della costruzione di decisioni stabili e condivise[23].

4. Il caos: analisi e sfruttamento per il vantaggio

L'esposizione continua a flussi informativi accelerati, la frammentazione dell'attenzione e la reattività immediata non restano confinate alla sfera del singolo cittadino, ma si riflettono e si moltiplicano nell'interazione tra individui, contribuendo alla formazione di *pattern* sociali complessi e instabili.

[21] B.-C. Han, *Psicopolitica. Il neoliberismo e le nuove tecniche del potere*, cit., pp. 17-18.

[22] B. Stiegler, *Taking Care of Youth and the Generations*, Stanford University Press, 2010, pp. 95, 103-104.

[23] L. Di Gregorio, *Demopatìa. Sintomi, diagnosi e terapie del malessere democratico*, cit.

In questo senso, appare necessario compiere un ulteriore passaggio analitico, spostando il focus dalla dimensione individuale a quella collettiva, al fine di comprendere come tali dinamiche si traducano in trend emergenti dell'intero sistema sociale. Il comportamento collettivo non può infatti essere interpretato come semplice somma lineare di decisioni individuali, ma deve essere compreso come il risultato crescente di interazioni distribuite tra una molteplicità di attori interconnessi. In questa prospettiva, il concetto di "*netizen*" trova una sua più compiuta rappresentazione se letto attraverso la metafora dello sciame o della mormorazione: un sistema dinamico in cui il comportamento globale non è determinato da un centro decisionale, ma emerge dall'adattamento continuo di ciascun elemento alle azioni dei soggetti più prossimi.

Come nello stormo di uccelli, ogni individuo regola il proprio movimento sulla base di informazioni locali, limitate e parziali, reagendo a variazioni immediate del contesto piuttosto che a una visione complessiva del sistema. Il risultato è la formazione di *pattern* collettivi altamente complessi, caratterizzati da apparente coerenza ma privi di una direzione unitaria stabilmente identificabile. Tale dinamica, traslata nello spazio cognitivo delle società contemporanee, implica che le opinioni, le percezioni e i comportamenti politici non si diffondano secondo logiche gerarchiche o verticali, ma attraverso processi reticolari, nei quali ogni nodo agisce al tempo stesso come ricevente, interprete e vettore di informazione.

L'ambiente entro cui questo "sciame cognitivo" si muove è tuttavia profondamente instabile. A differenza delle società tradizionali, in cui i flussi informativi erano relativamente lenti e filtrati, l'ecosistema digitale contemporaneo è attraversato da una molteplicità di correnti – mediatiche, algoritmiche, emotive e politiche – che modificano continuamente le condizioni di percezione e di decisione. In questo contesto, il paradigma VUCA (*volatility, uncertainty, complexity, ambiguity*), elaborato in ambito dottrinale presso l'U.S. *Army War College* e successivamente ripreso da Bob Johansen[24] per descrivere gli scenari strategici contemporanei, continua a offrire una chiave interpretativa utile, ma non più pienamente sufficiente a cogliere la natura delle dinamiche attuali. Alla volatilità dei flussi informativi si affianca infatti una loro crescente accelerazione; all'incertezza si sovrappone una difficoltà strutturale nell'attribuzione delle responsabilità e delle cause; alla complessità si accompagna

[24] B. JOHANSEN, *Leaders Make the Future: Ten New Leadership Skills for an Uncertain World*, Berrett-Koehler, San Francisco, 2009, pp. 5-6.

una non linearità sempre più marcata nei rapporti tra causa ed effetto; all'ambiguità si aggiunge, infine, una progressiva perdita di intelligibilità del contesto.

In questa prospettiva, alcuni sviluppi recenti propongono di estendere il modello introducendo una dimensione ulteriore, talvolta identificata come *paradox*[25] e talvolta come *polarized* (VUCAP). Nel primo caso, l'accento è posto sulla coesistenza di dinamiche tra loro apparentemente contraddittorie ma simultaneamente operative, che rendono instabili i criteri di interpretazione e di decisione. Nel secondo, emerge invece la tendenza alla frammentazione dello spazio cognitivo in comunità sempre più chiuse e contrapposte, nelle quali le informazioni non circolano più secondo logiche condivise ma si rafforzano all'interno di circuiti autoreferenziali. L'integrazione di queste dimensioni consente di cogliere come l'ambiente informativo contemporaneo non sia soltanto instabile e complesso, ma anche strutturalmente sensibile a contraddizioni interne e processi di polarizzazione, che ne amplificano l'imprevedibilità e ne riducono ulteriormente la governabilità.

In tale scenario, il comportamento collettivo tende a svilupparsi attraverso variazioni repentine e difficilmente prevedibili. Come uno stormo esposto a correnti d'aria improvvise, anche la società iperconnessa reagisce a stimoli locali – una notizia, un'immagine, un contenuto virale – generando spostamenti rapidi dell'attenzione e dell'opinione pubblica e delle relative azioni nella vita democratica e sociale in lettura globale. Questi movimenti non seguono necessariamente una logica razionale o deliberativa, ma risultano dall'interazione tra fattori cognitivi, emotivi e relazionali che operano su scale temporali sempre più ridotte. Il tempo della riflessione viene così compresso a favore di una reattività immediata, nella quale la capacità di orientare il flusso dell'attenzione diventa più rilevante della solidità dei contenuti.

È in questo spazio che il caos assume una funzione strategica. Lungi dall'essere un semplice effetto collaterale della complessità, esso può essere prodotto, amplificato e sfruttato come leva di influenza. In un sistema sensibile e istericamente adattivo come quello descritto, non è necessario controllare direttamente i singoli nodi; è sufficiente intervenire sulle condizioni ambientali – saturando i canali informativi, moltiplicando le narrazioni concorrenti, accelerando i tempi di circolazione – per indurre il sistema a comportamenti instabili o incoerenti. Il caos, in questa

[25] A.A. Gümüsay, *Embracing religions in moral theories of leadership*, in *Academy of Management Perspectives*, 33(3), 2019, pp. 304-305.

prospettiva, non distrugge l'ordine esistente, ma ne altera i meccanismi di formazione, rendendo più difficile la convergenza verso decisioni collettive stabili e razionali. Questo passaggio rappresenta un'evoluzione significativa rispetto alle forme tradizionali di propaganda. Se quest'ultima era orientata prevalentemente a indirizzare la volontà collettiva verso una determinata direzione, le strategie contemporanee di influenza operano sempre più spesso in senso opposto, frammentando il campo cognitivo e moltiplicando i punti di attrito. L'obiettivo non è tanto convincere, quanto disarticolare; non tanto costruire consenso, quanto impedire la formazione di un consenso coerente e duraturo. Quel principio strategico dello «intorbidire l'acqua per catturare i pesci» trova una declinazione pienamente attuale: non si tratta di prevalere in un confronto diretto, ma di rendere il contesto talmente instabile da compromettere la capacità decisionale dell'avversario[26].

Le riflessioni sulla complessità e sull'incertezza radicale consentono di comprendere ulteriormente questa dinamica. Come evidenziato da Taleb, i sistemi complessi non rispondono in modo proporzionale agli stimoli, ma possono produrre effetti amplificati e imprevedibili a partire da perturbazioni apparentemente marginali[27]. Applicato allo spazio cognitivo, ciò significa che interventi limitati ma mirati possono generare effetti sistemici rilevanti, soprattutto in presenza di un ambiente già caratterizzato da elevata interconnessione e bassa resilienza deliberativa.

In questo quadro, il passaggio dal paradigma VUCA a quello BANI (*brittle, anxious, nonlinear, incomprehensible*) rappresenta un ulteriore avanzamento interpretativo. Se VUCA descrive soprattutto le caratteristiche strutturali di un ambiente instabile e complesso, BANI consente di cogliere come tale ambiente venga percepito, interiorizzato e vissuto dai soggetti che vi sono immersi[28]. La fragilità indica la tendenza dei sistemi apparentemente solidi a collassare improvvisamente; l'ansia riflette la difficoltà degli individui nel gestire l'incertezza; la non linearità segnala la sproporzione tra cause ed effetti; l'incomprensibilità evidenzia la perdita di senso che accompagna la "bulimia informativa". In questo senso, BANI risulta particolarmente utile per l'analisi della guerra cognitiva, poiché sposta l'attenzione dalla sola instabilità del contesto agli effetti cognitivi e comportamentali che tale instabilità produce sugli individui

[26] Cfr. G. MAGI, *I 36 Stratagemmi*, cit.

[27] N.N. TALEB, *Il Cigno nero. Come l'improbabile governa la nostra vita*, Il Saggiatore, Milano, 2008, pp. 5-7; N.N. TALEB, *Antifragile*, Il Saggiatore, Milano, 2012, pp. 18-19

[28] Cfr. J. CASCIO, *Facing the Age of Chaos*, in *Medium*, 2020.

e sulle collettività, incidendo direttamente sulla qualità dell'orientamento, del giudizio e della decisione. Questa trasformazione ha implicazioni dirette per la sicurezza delle democrazie liberali. In un ambiente BANI, la vulnerabilità non risiede soltanto nella possibilità di essere esposti a informazioni false, ma nella difficoltà strutturale di costruire interpretazioni condivise e orientamenti stabili. Il caos cognitivo diventa così il terreno privilegiato della competizione ibrida: uno spazio in cui l'influenza si esercita non attraverso il controllo diretto, ma mediante la modulazione delle condizioni sistemiche entro cui si formano percezioni e decisioni.

Da questa prospettiva, il problema strategico non è semplicemente quello di contrastare singoli atti di disinformazione, ma di comprendere e governare le dinamiche emergenti di sistemi complessi e adattivi. Il passaggio dal VUCA al BANI non rappresenta dunque soltanto un aggiornamento terminologico, ma segnala la necessità di ripensare gli strumenti di analisi e di intervento. Come verrà approfondito nel paragrafo successivo, ciò implica lo sviluppo di strategie capaci di agire non solo sui contenuti, ma sulle condizioni strutturali della comunicazione e della formazione del giudizio, con l'obiettivo di rafforzare la resilienza cognitiva e preservare la possibilità stessa di una deliberazione democratica consapevole.

5. Confini cognitivi e possibili strategie di risposta

A differenza delle dimensioni fisiche e virtuali tradizionali del conflitto – che inglobano i domini terrestre, marittimo, aereo e, più recentemente, cibernetico – quella cognitiva si caratterizza per una natura radicalmente immateriale[29]. Pur potendo essere mediata da infrastrutture tecnologiche e piattaforme digitali, essa non coincide con le stesse, né può essere ricondotta a parametri esclusivamente tecnici. La dimensione cognitiva – o, secondo alcune dottrine, dominio cognitivo, tema altamente meritevole di approfondimento – non presenta confini fisici chiaramente delimitabili, né consente una misurazione immediata degli effetti prodotti nel medio e lungo periodo. Tale indeterminatezza costituisce al tempo stesso la sua forza strategica e la principale difficoltà per l'elaborazione di risposte efficaci.

Se il cyberspazio, pur nella sua complessità, resta ancorato a reti, nodi

[29] *Cognitive Warfare. La competizione nella dimensione cognitiva*, in www.difesa.it, 2023.

e infrastrutture critiche materiali, la dimensione cognitiva investe direttamente il piano delle rappresentazioni, delle percezioni e dei processi decisionali individuali e collettivi. È in questo spazio che può essere collocato ciò che qui viene definito come "*limes* cognitivo", ovvero l'insieme dei confini immateriali entro cui si rendono possibili tali processi. Ne consegue che la difesa non può fondarsi su logiche puramente reattive o su strumenti esclusivamente tecnologici. Essa richiede, piuttosto, una riflessione preventiva sui confini immateriali che una comunità democratica intende riconoscere e tutelare, confini che non possono che essere tracciati a partire dagli elementi fondanti della democrazia stessa, ossia dal rapporto tra individuo, società e potere politico.

A questo proposito, il concetto di *limes* cognitivo rimanda all'insieme delle condizioni che rendono possibile un esercizio consapevole della libertà politica. Difendere la dimensione (e/o dominio) cognitiva non significa proteggere specifici contenuti informativi, bensì salvaguardare i processi attraverso cui i cittadini formano giudizi, orientano le proprie preferenze e partecipano alla deliberazione pubblica.

Come evidenziato, ad esempio, dal rapporto del Parlamento britannico su *Disinformation and 'Fake News'*, la minaccia principale non risiede nella circolazione di singole informazioni false, ma nella progressiva erosione di un terreno cognitivo condiviso, in cui la distinzione tra informazione, opinione e manipolazione tende a sfumare, compromettendo la capacità dei cittadini di valutare criticamente le scelte politiche. In tal senso, il *limes* cognitivo può essere inteso come una soglia dinamica: all'interno di essa, l'influenza politica opera attraverso la persuasione e il confronto; al di là, diventa coercizione indiretta, poiché altera aspettative, percezioni e criteri decisionali degli individui, secondo una logica che Thomas C. Schelling ha già descritto come centrale nei processi di influenza e coercizione strategica[30]. Ciò implica un approccio olistico alla difesa del dominio cognitivo, orientato non al controllo dei messaggi, ma alla tutela delle condizioni cognitive e istituzionali che rendono possibile una deliberazione pubblica libera, informata e responsabile[31].

Un possibile livello di intervento riguarda la cosiddetta "logistica dell'informazione", intesa come l'insieme delle infrastrutture, delle pratiche e dei processi che regolano la raccolta, la circolazione e l'elaborazione dell'informazione, producendo capacità operative, orientamenti

[30] T.C. SCHELLING, *Arms and Influence*, cit.
[31] Cfr. J. HABERMAS, *Fatti e norme*, Laterza, Bari-Roma, 1996.

cognitivi e condizioni di possibilità dell'azione politica e strategica[32]. Tali flussi possono essere analizzati e, in parte, governati adattando schemi concettuali noti agli studi sulla comunicazione, tenendo conto della complessità dei rapporti tra "*one*" e "*many*" che caratterizzano l'ecosistema digitale contemporaneo. Come osserva Giorgino, la comunicazione politica odierna si sviluppa attraverso una pluralità di modelli di flusso – *one-to-one*, *one-to-many* e *many-to-many* – che coesistono e interagiscono, producendo differenti asimmetrie informative e specifici effetti sulla formazione dell'opinione pubblica e sull'esercizio del potere[33].

In termini analitici, è possibile osservare tre piani di azione interdipendenti: gli emittenti, intesi non più soltanto come attori istituzionali o mediatici tradizionali, ma anche come soggetti diffusi e piattaforme; i riceventi, sempre più attivi, segmentati e cognitivamente sollecitati; e i canali, che non svolgono una funzione neutrale di trasmissione, ma incidono sulla visibilità, sulla circolazione e sull'interpretazione dei contenuti. Tale impostazione si colloca nel solco degli studi classici sulla comunicazione e sulla sfera pubblica, aggiornati alla logica reticolare e digitale[34].

Il primo piano concerne il ruolo degli emittenti. In una sfera pubblica fortemente interconnessa, la distinzione tra produttori e consumatori di informazione tende a sfumare, attribuendo a ciascun soggetto una responsabilità potenziale nella diffusione di contenuti capaci di rafforzare o indebolire la coesione sociale. Un approccio socio-politologico dovrebbe mirare a rafforzare tale consapevolezza civica, senza scivolare in forme di controllo preventivo incompatibili con i principi democratici[35].

Il secondo piano, probabilmente il più delicato, riguarda i riceventi. Qui la questione non è tanto la verifica puntuale delle informazioni, quanto la promozione di una più ampia educazione alla resistenza cognitiva. La difesa dell'attenzione emerge come un autentico bene pubblico, in quanto prerequisito per qualsiasi forma di deliberazione razionale. In questa direzione, il concetto di "militanza cognitiva", come elaborato da

[32] M. Mezza, *Net-war. Ucraina: come il giornalismo sta cambiando la guerra*, Donzelli, Roma, 2022, pp. 19-21, 132, 210-211.

[33] F. Giorgino, *Alto volume. Politica, comunicazione e potere*, Luiss University Press, Roma, 2019.

[34] Cfr. H.D. Lasswell, *The Structure and Function of Communication in Society, in The Communication of Ideas*, Harper and Row, New York, 1948; cfr. M. Castells, *Communication Power*, Oxford University Press, Oxford, 2009; cfr. Y. Benkler, *The Wealth of Networks*, Yale University Press, New Haven, 2006.

[35] Cfr. J. Habermas, *Storia e critica dell'opinione pubblica*, Laterza, Bari-Roma, 2006.

Sterpa, indica non un'adesione ideologica, ma un allenamento alla complessità, al confronto argomentativo e alla sospensione del giudizio[36].

Il terzo piano riguarda i canali, oggi rappresentati prevalentemente dalle piattaforme digitali e dai sistemi di intelligenza artificiale. La loro centralità come infrastrutture cognitive impone una riflessione sul piano giuridico e di *governance*, che includa forme di regolazione proporzionate, meccanismi di trasparenza algoritmica "auditabile" e una più netta separazione funzionale tra informazione, intrattenimento e persuasione strategica[37].

A completare questo quadro, le riflessioni di Hartmut Rosa sull'accelerazione sociale offrono una chiave interpretativa decisiva. L'intensificazione e la compressione dei tempi della comunicazione amplificano la vulnerabilità cognitiva delle società contemporanee, riducendo gli spazi di elaborazione critica e favorendo risposte emotive e reattive. In tale prospettiva, rallentare i flussi informativi e ricostruire un rapporto più consapevole, dialogico e fiduciario tra individui, istituzioni e discorso pubblico non rappresenta una regressione, ma una scelta strategica orientata alla resilienza democratica[38].

Nel loro insieme, queste linee di intervento mostrano come la difesa del dominio cognitivo non possa essere affidata a soluzioni unidimensionali. La tecnologia agisce come potente acceleratore di dinamiche antropologiche e sociali preesistenti, ma non ne costituisce l'origine. Per questo, una strategia efficace di contrasto alla guerra cognitiva deve riconoscere il primato delle dimensioni umanistiche e istituzionali, integrando gli strumenti tecnici in una più ampia visione culturale e politica della sicurezza democratica[39].

6. Conclusioni

La riflessione sulla guerra cognitiva e sulle sue implicazioni per le democrazie liberali conduce a un livello di analisi che trascende la dimen-

[36] A. STERPA, *La difesa della democrazia dalle minacce ibride. Teorie della comunità, dell'autorità, del potere e migrazioni: elementi per un'analisi strategica della "guerra tiepida"*, Editoriale Scientifica, Napoli, 2022, pp. 65-86.

[37] Cfr. S. ZUBOFF, *Il capitalismo della sorveglianza*, Luiss University Press, Roma, 2019.

[38] H. ROSA, *Accelerazione e alienazione*, Einaudi, Torino, 2015.

[39] Cfr. L. FERRAJOLI, *Poteri selvaggi. La crisi della democrazia italiana*, Laterza, Bari-Roma, 2011.

sione tecnico-operativa e si colloca sul piano filosofico e culturale. È su questo orizzonte di senso che si gioca la resilienza dei sistemi democratici: senza un'idea di verità non assoluta ma orientativa, senza un'antropologia che non riduca l'individuo a semplice utente o *target* comunicativo e senza una cultura del limite, ogni tentativo di governance rischia di essere percepito come censura.

Come aveva lucidamente compreso Jacques Ellul, la propaganda diviene realmente efficace quando l'uomo non è più in grado di riconoscere le ragioni della propria resistenza. In tale condizione, la perdita non riguarda singole opinioni, ma investe la capacità stessa di attribuire senso all'agire pubblico. La guerra cognitiva opera precisamente su questo piano: non mira a sostituire una verità con un'altra, bensì a erodere le condizioni che rendono possibile la deliberazione razionale e il confronto democratico.

Da questa prospettiva, il contrasto alla guerra cognitiva non può essere affidato esclusivamente a strumenti tattici quali il *fact-checking* o l'elaborazione di principi etici per l'intelligenza artificiale. Pur necessari, tali strumenti intervengono a valle di processi già in atto. La dimensione strategica della risposta risiede, invece, nella capacità delle istituzioni di proteggere le condizioni del pensiero, dei sistemi educativi di formare soggetti capaci di attrito cognitivo e della riflessione filosofica di restituire legittimità al dubbio, alla lentezza e alla complessità.

In questo senso, la difesa della democrazia nel XXI secolo non coincide con la mera salvaguardia delle sue procedure formali, ma con la cura degli spazi cognitivi e simbolici che ne rendono possibile il funzionamento. Affrontare la guerra cognitiva significa, in ultima analisi, riconoscere nel limite e nella responsabilità non un freno all'azione politica, ma la sua condizione di possibilità.

DALLA DISINFORMAZIONE AL SABOTAGGIO NELL'ERA DIGITALE: GUERRA COGNITIVA, IA AGENTE E SOVRANITÀ DEL DATO

Pierguido Iezzi[*]

1. *Introduzione*

Nell'era digitale in cui l'informazione regna e il dato è sovrano, il contesto geopolitico internazionale sta conoscendo una torsione senza precedenti dovuta a uno sviluppo prima inimmaginabile della guerra ibrida, così come teorizzata dal Capo di Stato Maggiore dell'Armata Rossa, Vassily Vasilevich Gerasimov, alla vigilia dell'invasione russa dell'Ucraina, ormai 4 anni fa.

La "*gibridnaya voyna*" differisce sostanzialmente dall'interpretazione che si dà normalmente in Occidente a questo stato di belligeranza, focalizzandosi maggiormente sulla disgregazione interna del tessuto socioculturale nemico attraverso una strategia che fonde mezzi militari convenzionali con tattiche irregolari, cyberattacchi, disinformazione – di cui la Russia è maestra sin dai tempi del Comintern di cui il comunista tedesco Willi Münzenberg[1] animò la propaganda fin quando non fu espulso

[*] Direttore Cyber di Zenita Group.

[1] Uomo politico tedesco (Erfurt 1889 – Saint-Marcellin, Isère, 1940). Membro dal 1919 della *Kommunistische Partei Deutschlands* (KPD), durante la Repubblica di Weimar si adoperò al fine di ottenere aiuti per la carestia che aveva colpito la Russia (1921). Ciò gli permise di lavorare a stretto contatto con la polizia segreta sovietica e con il Comintern, che spinse ad appoggiare il caso Sacco e Vanzetti (1925). Successivamente dimostrò, durante il contro-processo a Londra, la responsabilità dei nazisti nell'incendio del Reichstag (1933). Dalle carte processuali furono pubblicati *The brown book of the Hitler terror and*

da Stalin nel 1938. Tale strategia è caratterizzata da pressioni economiche e sovversione politica, mirando a destabilizzare l'avversario senza un conflitto aperto. Si tratta di una guerra "sottosoglia", che raramente si manifesta nei canoni bellici classici ma che produce effetti concreti, misurabili e quotidiani. Non è solo propaganda o informazione manipolata. È un insieme di leve – tecnologiche, economiche, sociali e infrastrutturali – impiegate per orientare decisioni, generare instabilità e ridurre la capacità di risposta di un Paese senza oltrepassare, formalmente, la linea che separa la tensione dalla guerra dichiarata[2].

In questo contesto, la disinformazione è solo una componente, uno strumento necessario al conseguimento di un obiettivo assai più ambizioso: il sabotaggio del processo decisionale. I vertici politici e militari dell'avversario devono cioè essere messi nelle condizioni di errare nelle proprie valutazioni e di conseguenza nelle risposte a un'azione ostile. Per ottenere questo risultato occorre comprimere il tempo di reazione, saturare l'attenzione, polarizzare il dibattito e ridurre la fiducia nelle istituzioni. Non è più necessario persuadere la maggioranza dell'opinione pubblica, ma spesso è sufficiente rendere più fragile la capacità collettiva di scegliere. È questa la natura della guerra cognitiva: agire sulla percezione e sulla fiducia per indebolire la tenuta democratica restando sotto la soglia di un conflitto vero e proprio.

Nelle moderne democrazie il processo decisionale è anche – e sempre più – un processo guidato dai dati: le istituzioni e le imprese decidono sulla base di informazioni, metriche, modelli, segnali e flussi che alimentano gli strumenti predittivi digitali. Per questo motivo la guerra cognitiva non colpisce solo le opinioni, ma va a deteriorare la qualità e l'integrità dei dati che sono alla base delle decisioni. Tutelare i valori democratici significa allora difendere la catena del dato in ognuno degli anelli che la compone: dalla raccolta alla integrità, dalla provenienza all'accesso fino all'utilizzo. Proprio in questo aspetto la sovranità del dato europeo – ossia delle informazioni che ogni giorno vengono costantemente prodotte

the burning of the Reichstag (1933) e *The Reichstag fire trial. The second brown book of the Hitler terror* (1934). Trasferitosi a Parigi, ebbe un ruolo importante nell'organizzazione e nel reclutamento delle brigate internazionali impegnate nella guerra civile spagnola (1936-39). Nel 1938, a causa delle critiche da lui rivolte alla politica di Stalin, fu espulso dal Comitato centrale e poi (1939) dal partito. Morì in circostanze misteriose nel tentativo di sfuggire all'avanzata tedesca in Francia.

[2] Per un inquadramento generale sul rapporto tra conflitto ibrido e potere digitale, cfr. P. IEZZI, *Cyber e Potere*, Mondadori, Milano, 2023, pp. 15-32; M. MEZZA, *Net-war. Ucraina: com eil giornalismo sta cambiando la guerra*, Donzelli, Roma, 2022, pp. 9-21.

nell'ambiente digitale dai cittadini, dalle imprese e dalle istituzioni del continente più ricco ed evoluto del pianeta – diventa una capacità di difesa e una postura geopolitica, paragonabile alla "sovranità digitale" perseguita dai diversi blocchi protagonisti nel cyberspazio con altri mezzi: dalla dipendenza conseguita attraverso la proprietà tecnologica statunitense alla grande muraglia digitale cinese per arrivare all'internet sovrano russo.

2. *La dipendenza tecnologica come strumento di pressione*

Una delle forme più efficaci di guerra ibrida passa dalla dipendenza tecnologica. Quando filiere, piattaforme, servizi essenziali e competenze critiche sono concentrati in poche mani, lo strumento proprietario evolve in una pressione strutturale e connaturata. Più è estesa e profonda tale dipendenza, più aumenta la vulnerabilità nel processo decisionale: non risulta più necessario imporre un vincolo esplicito, perché spesso è la realtà operativa a trasformarsi in un limite effettivo.

Una simile pressione può anche non limitarsi a essere esercitata in maniera indiretta e implicita, ma talvolta svilupparsi in qualcosa di più estremo e concreto: ricatto, deterrenza, persino allineamenti forzati[3]. Lo si comprende molto bene, ad esempio, dai dettami contenuti nella Nuova Strategia Nazionale varata dalla amministrazione Trump, in cui Washington chiede agli europei di allinearsi anche sul piano tecnologico: adottare standard, piattaforme e fornitori statunitensi nel *cloud*, nell'AI, nel cyber, nelle comunicazioni critiche; escludere i concorrenti cinesi e russi da reti 5G, apparati di sicurezza, infrastrutture sensibili; partecipare a un ecosistema occidentale in cui la *leadership* tecnologica resta americana, mentre gli alleati forniscono mercati, dati, basi industriali e supporto politico. L'Unione è profondamente dipendente da infrastrutture digitali non europee. Le piattaforme di riferimento – dai motori di ricerca ai *social network*, dai sistemi operativi alle grandi piattaforme *cloud* – sono quasi tutte americane o cinesi. I *chip* più avanzati sono progettati negli Stati Uniti, prodotti in Asia orientale, assemblati in catene di montaggio europee, importanti sì ma non autonome. I principali modelli di intelligenza artificiale nascono in contesti anglosassoni o asiatici.

In un simile scenario, la sovranità digitale non è più solo un tema in-

[3] Per le successive considerazioni cfr. P. Iezzi, G. Fusco, *Hackerare la mente*, *Parole, algoritmi e inganni. Come difendere la propria libertà digitale*, ilSole24Ore, Milano, 2026.

dustriale o di innovazione, bensì diviene un fattore di sicurezza nazionale e, di conseguenza, una componente a pieno titolo della guerra ibrida. Chi controlla le tecnologie chiave – intelligenza artificiale, calcolo quantistico, capacità spaziali, infrastrutture digitali globali – controlla pertanto una parte crescente dell'ordine mondiale. "Tecnologia" significa capacità di difendere il proprio territorio, ma anche di condizionare quello altrui. Significa poter negare accessi, rallentare reti, manipolare flussi informativi, bloccare pagamenti, interrompere la produzione in una fabbrica dall'altra parte del pianeta. La tecnologia diventa così strumento di influenza e di creazione di dipendenze: se la rete elettrica, il *cloud* della pubblica amministrazione, i sistemi bancari di un Paese si appoggiano a standard, piattaforme e fornitori dominati da un altro attore, la sua indipendenza decisionale è quindi difatti già compressa.

3. *Dal* ransomware *al sabotaggio: il cyberspazio come leva di pressione politica*

Se la dipendenza tecnologica può essere definita come uno strumento passivo della guerra ibrida, gli attacchi informatici – che oggi trovano nel *ransomware* una delle manifestazioni più visibili – ne costituiscono invece un elemento attivo. Troppo spesso essi vengono associati in maniera superficiale e automatica al mondo cybercriminale, con una lettura incompleta e parziale. Un attacco *ransomware* può rivelarsi infatti, a tutti gli effetti, come un atto di guerra ibrida nell'eventualità in cui la *gang* che lo conduce è sostenuta, finanziata, indirizzata – direttamente o indirettamente – o anche solo tollerata da un attore statale. E anche nell'eventualità in cui non esista una "prova" pubblica del legame con un governo ostile, sono sufficienti le dinamiche note: tolleranza territoriale, protezione implicita, convergenze di interesse e assenza di perseguibilità reale[4].

Qualora l'attacco coinvolga una infrastruttura critica, l'effetto non si limita al danno economico: l'azione offensiva diventa immediatamente un messaggio rivolto innanzitutto alla popolazione, che percepisce vulnerabilità e disordine, e in secondo luogo alle istituzioni, che vengono esposte come incapaci di garantire la sicurezza e la continuità dei servizi

[4] In 22.052 incidenti analizzati e 12.195 *data breach* confermati nel 2025, il *ransomware* è infatti collegato al 75% dei *system-intrusion breaches*. Crf. Verizon, *2025 Data Breach Investigations Report*, 2025, pp. 3-5.

essenziali. In questo modo il cybercrimine smette di essere esclusivamente un "incidente" e si trasforma pressione strategica[5].

Tuttavia, il *ransomware* non è l'unica forma in cui si manifesta la guerra ibrida tramite gli attacchi informatici. Esistono atti pensati e realizzati secondo una logica di sabotaggio, orientati a creare disservizi e indisponibilità, quali gli attacchi DDoS. Si tratta del più semplice e banale dei cyberattacchi, operato tramite un numero massiccio di dispositivi asserviti chiamati simultaneamente a generare una mole ingente di traffico di dati verso un singolo obiettivo per saturarne le capacità di risposta *online*. Sono azioni finalizzate a interrompere funzioni chiave, operazioni che mirano a un risultato semplice e potente: non far più funzionare servizi essenziali *online*, dai trasporti alla sanità, dall'energia all'educazione. L'obiettivo è il medesimo anche in questo caso: offendere rimanendo sotto la soglia di un conflitto aperto, pur generando un senso diffuso di insicurezza e impotenza capace di erodere la fiducia e di compromettere la prontezza decisionale.

4. Non solo digitale: la fragilità delle infrastrutture fisiche

La guerra ibrida, per le sue caratteristiche a cavallo tra il reale e il virtuale e le conseguenze che porta nel mondo fisico attraverso la compromissione di quello digitale, non riguarda esclusivamente il cyberspazio. Sempre più spesso il rischio si estende alle infrastrutture fisiche che sostengono il mondo digitale e quello energetico: cavi, dorsali, sistemi di comunicazione, infrastrutture sottomarine, reti critiche. La loro indisponibilità, anche temporanea, può produrre impatti strategici enormi senza ricorrere a un attacco "militare" in senso tradizionale[6].

L'interruzione dell'energia elettrica o un malfunzionamento nell'erogazione del gas può infatti creare panico generalizzato nella popolazione e provocare serie disfunzioni alla sicurezza di un Paese. Una paralisi aerea

[5] Nel 2024 NCC Group ha registrato 5.263 attacchi *ransomware*, il valore annuale più alto dal 2021; il settore industriale è tra i più colpiti, con il 27% dei casi registrati. Cfr. NCC GROUP, *Cyber Threat Monitor Report 2024*, 2025, pp. 4-6.

[6] Sui casi recenti di attacchi e sabotaggi ai danni di cavi sottomarini e pipeline nel Baltico, cfr. E. Braw, *How the Baltic Sea nations have tackled suspicious cable cuts*, in Atlantic Council, 26 novembre 2025. Per il procedimento penale relativo al danno a Balticconnector e ai cavi tra Finlandia ed Estonia avvenuto nel 2023, cfr. G. Torode, J. Pomfret, *Chinese captain pleads not guilty to Baltic Sea cable damage*, Reuters, 11 febbraio 2026.

o ferroviaria, anche se ha conseguenze meno gravi, semina tuttavia altrettanta sfiducia e incertezza, mettendo in discussione l'ordine costituito. Non a caso nel giro di un lustro il comparto trasporti si è trasformato in un bersaglio privilegiato per i cybercriminali, registrando un'impennata degli attacchi che da poco più di una dozzina di casi significativi nel 2020 sono schizzati fino a quasi sessanta nel 2024. Questa tendenza, con un tasso di crescita medio annuo del 48%, sottolinea come la digitalizzazione delle infrastrutture di trasporto, se da un lato offre efficienza e connettività, dall'altro espone a minacce sempre più sofisticate, che spaziano dal *ransomware* – responsabile di oltre un terzo delle intrusioni – agli attacchi DDoS.

Le vulnerabilità emergono soprattutto nella convergenza tra IT e OT, dai sistemi di controllo ferroviari ai *network* aeroportuali, dove tecniche di *spoofing* e *jamming* rischiano di paralizzare intere reti. Allo stesso tempo, l'esplosione di dispositivi IoT e l'adozione del 5G hanno ampliato la superficie di attacco, dando vita a nuove minacce come le *botnet* intelligenti e le insidie della "*shadow AI*". Nel trasporto su gomma, poi, quasi il 60 % degli attacchi *ransomware* prende di mira la *supply chain* terrestre, esponendo milioni di credenziali e dati sensibili.

Il settore energetico rappresenta un'infrastruttura critica fondamentale per il funzionamento della società moderna. La sua crescente digitalizzazione, sebbene porti efficienza e innovazione, lo espone a un panorama di minacce informatiche in continua evoluzione e sempre più sofisticate. L'aumento degli incidenti *cyber* nel settore è significativo, con un incremento del 40% nel 2024 rispetto al 2023 e una proiezione di ulteriore crescita del 21% entro fine 2025. Si osserva inoltre un cambiamento radicale nelle tecniche di attacco, con un'esplosione degli attacchi DDoS e un aumento del *ransomware*, spesso legati a motivazioni di *hacktivismo* e tensioni geopolitiche.

Con il 75% delle menzioni nel *dark web* dirette al nostro Paese, l'Italia resta tra i *target* più esposti a livello globale. Queste evidenze, unite al ruolo crescente dell'*hacktivismo* e delle tensioni geopolitiche, rafforzano l'idea che la minaccia non sia solo tecnologica, ma anche strategica e di intelligence: il settore energetico continua a rappresentare un obiettivo primario, in cui attori criminali e statuali operano con logiche sempre più sofisticate e difficili da intercettare.

Il panorama delle minacce è diversificato, riflettendo motivazioni e capacità differenti. Le principali tipologie di attacchi che colpiscono il settore includono; lo spionaggio, con cui attori statali o entità sponsorizzate da governi stranieri mirano all'acquisizione di informazioni sensibili

relative a tecnologie energetiche, strategie operative e vulnerabilità infrastrutturali con l'obiettivo di ottenere un vantaggio geopolitico o economico; il sabotaggio, spesso agito da nazioni ostili o gruppi con forti motivazioni politiche, che mira a disabilitare o interrompere le operazioni energetiche, con la possibilità di causare *blackout* estesi o danni fisici diretti alle infrastrutture; il crimine informatico, dove gruppi criminali organizzati sono attratti dal settore energetico per il potenziale guadagno economico e operano tramite *ransomware*, estorsioni, furto di dati e interruzioni di servizio; *hacktivism*, con attacchi motivati da ideologie sociali, politiche o ambientali, volti a causare interruzioni di servizio o a danneggiare la reputazione delle aziende energetiche per fini propagandistici o di protesta.

Il settore energetico e delle *utility* affronta diverse sfide uniche nel loro genere che lo rendono particolarmente vulnerabile a una vasta gamma di minacce, dagli attacchi *ransomware* che colpiscono le infrastrutture critiche alle campagne di *spear-phishing* volte a sfruttare le vulnerabilità umane. Queste sfide includono la prevalenza di infrastrutture obsolete, la dipendenza da componenti IT datate e difficilmente sostituibili senza compromettere le funzionalità aziendali e la complessità dei sistemi OT, ossia di tecnologia operativa. Insieme all'importanza geopolitica del settore e al potenziale impatto sociale diffuso, questi fattori rendono l'industria energetica e delle *utility* un obiettivo primario per gli attori malevoli.

La crescente dipendenza dalle tecnologie digitali, dalle operazioni remote e dai sistemi basati su *cloud* ha ampliato la superficie di attacco, creando nuove vulnerabilità che devono essere affrontate attraverso robuste misure di cybersicurezza. Un attacco informatico può infatti portare a interruzioni operative, danni fisici e danni reputazionali con significative implicazioni sociali, inclusi *blackout*, interruzioni della catena di approvvigionamento e rischi per la sicurezza nazionale, con conseguenti scenari che possono facilmente divenire apocalittici.

In questo contesto, il mondo dell'intelligence assume un ruolo centrale perché capace di prevedere i rischi individuando le vulnerabilità, comprendendo le dipendenze, cogliendo le linee rosse, stimando le soglie di tolleranza sociale. *Cyber warfare* e guerra elettronica pertanto si intrecciano: dallo spazio alle navi, dai sistemi satellitari alle reti industriali, fino alle operazioni di *cyber espionage* su infrastrutture tecnologiche. La finalità, molto spesso, è una sola: raccogliere dati – tecnici, operativi, economici e comportamentali – che, una volta correlati e trasformati in informazioni utili, consentono di selezionare la leva più efficace per

restare sottosoglia e massimizzare l'effetto cognitivo, politico, economico e sociale[7].

5. *Il vero carburante della guerra cognitiva: i dati come alimento della AI agentica*

La guerra ibrida agisce sulle emozioni, sulla percezione, sulla fiducia, aumentando la sua efficacia attraverso la conoscenza approfondita delle sue vittime conseguita attraverso l'analisi metodica delle decisioni, delle vulnerabilità, delle abitudini, degli interessi, delle dipendenze e delle attitudini dei bersagli. Il conseguimento di un sapere così dettagliato sulle persone avviene principalmente attraverso i loro dati nell'ambiente digitale che, opportunamente raccolti, correlati e analizzati, permettono di scegliere la modalità più efficace per raggiungere un obiettivo rimanendo sottosoglia. In questo modo è possibile costruire delle campagne di pressione mirate, articolate in operazioni di destabilizzazione, interferenze economiche e azioni di sabotaggio selettivo. Il dato diventa pertanto una risorsa strategica e al pari dell'energia o delle materie prime alimenta gli strumenti necessari a conseguire degli obiettivi determinati. Così come carbone e acciaio nutrivano la macchina bellica novecentesca, i *bit* oggi costituiscono il carburante della guerra cognitiva. Non solo perché hanno un valore di per sé, ma perché abilitano specifiche capacità di previsione, *targeting*, pressione e coercizione.

In questa catena, l'AI agentica agisce da moltiplicatore, perché introduce quattro acceleratori che cambiano la natura del rischio: Volume, Velocità, Veridicità e Volizione[8]. Il primo determina la capacità di produrre e adattare contenuti, tentativi di attacco e variazioni operative su scala industriale. Il secondo misura la compressione drastica dei tempi, dalla ricognizione all'esecuzione, riducendo lo spazio di reazione della vittima. Il terzo esplicita l'aumento della plausibilità dei contenuti – testi, voci, video, documenti – con un impatto diretto sulla fiducia e sulla

[7] Europol con l'Operation Eastwood del 16 luglio 2025 ha smantellato una rete pro-russa – NoName057(16) – collegata a campagne DDoS contro obiettivi europei. Cfr. EUROPOL, *Global operation targets NoName057(16) pro-Russian cybercrime network (Operation Eastwood)*, 2025.

[8] Secondo una sintesi di Microsoft ripresa da Associated Press, tra luglio 2024 e luglio 2025 gli episodi di contenuti falsi generati da AI sono saliti oltre 200, più del doppio dell'anno precedente. Cfr. D. KAPPLER, *Microsoft: Russia, China increasingly using AI to escalate cyberattacks on the US* in www.apnews.com, 16 ottobre 2025.

capacità di distinguere il vero dal verosimile. Il quarto rende conto del passaggio dal "*prompt*" all' "obiettivo", con sistemi che pianificano, iterano e ottimizzano azioni in funzione di un risultato, rendendo l'attacco più adattivo e persistente.

Per questa ragione l'AI, oggi, va letta in quattro forme complementari. In primo luogo questa tecnologia va vista come uno strumento offensivo, poiché garantisce automazione e scalabilità attraverso una ricognizione più rapida, *spear-phishing* e *deepfake* più credibili, la variazione continua di *payload* e *malware*, lo sfruttamento più tempestivo delle vulnerabilità, una maggiore capacità di elusione. La conseguenza è semplice: aumentano tentativi, qualità e frequenza degli attacchi, mentre si riduce la finestra decisionale di chi difende[9]. In secondo luogo, la Intelligenza Artificiale è anche un obiettivo sensibile, poiché aumenta la superficie di rischio: lo *stack* AI diventa un nuovo perimetro, in cui dati, modelli, *pipeline* e infrastruttura (LLM, *database/vector,* API, connettori) espongono superfici specifiche a *leakage*, *poisoning*, *injection* e compromissioni. Se si altera il dato o si contamina il modello, l'effetto non è solo tecnico: può diventare un errore sistemico che si propaga nei processi decisionali. In terzo luogo, la AI va vista come una vera e propria identità, al pari delle persone fisiche: *account*, API, sessioni, *plugin* e accessi alle piattaforme AI diventano nuovi asset da proteggere. Connettori, credenziali e *token* possono trasformarsi in accesso iniziale e, quindi, in rischio aziendale: l'AI non è più solo "uno strumento", è un canale privilegiato verso dati e processi. Infine, la AI è uno strumento di difesa: per reggere volumi e complessità accelerati serve una difesa "AI-armed", capace di gestire la correlazione e la prioritizzazione degli *alert*, l'individuazione delle anomalie, il *triage* automatico e la risposta guidata/automatizzata (SOAR), con *threat intelligence* e *use case* in grado di evolvere alla stessa velocità degli attaccanti. In caso contrario, l'asimmetria di scala diventa strutturale.

Quando dati e AI si combinano, la posta in gioco supera la dimensione della singola intrusione: diventa integrità del processo decisionale. Ed è qui che la sovranità del dato non è un tema di sola *compliance*, ma una capacità concreta di resilienza e difesa.

[9] Secondo il *Microsoft Digital Defense Report 2025* (trend luglio 2024-giugno 2025) gli attacchi con motivazione finanziaria sono prevalenti; lo spionaggio è stimato al 4% quando la motivazione è identificabile. Cfr. Microsoft, *Microsoft Digital Defense Report 2025*, 2025, pp. 9-12.

6. *La risposta europea: il "passaporto" del dato come difesa, mercato e diritti*

In questo scenario, l'Europa ha una peculiarità che spesso viene male interpretata: la sua legiferazione nella tutela dei dati e nel settore digitale. Non si tratta di "tecnocrazia digitale", né tantomeno di un riflesso burocratico. La postura europea è diversa: è una forma di difesa democratica che usa regole e standard come strumenti di sicurezza, e lo fa per tre ragioni convergenti: ridurre la vulnerabilità strategica, regolare il mercato digitale e garantire diritti fondamentali[10].

Il punto di partenza è semplice: se il processo decisionale dipende dai dati, allora il dato deve poter essere affidabile, tracciabile e governabile. Per questo la sovranità del dato europeo non è un concetto astratto; è la capacità di far sì che un dato – soprattutto quando entra in processi critici, modelli di AI, servizi essenziali o decisioni pubbliche – porti con sé una sorta di "passaporto di qualità". Non si tratta di un semplice bollino propagandistico, bensì di un insieme di attributi verificabili: provenienza, integrità, contesto, condizioni d'uso, livelli di protezione e responsabilità lungo la filiera[11].

Questa logica produce un effetto strategico, spostando il baricentro dalla "sovranità digitale" intesa come solo possesso di piattaforme e infrastrutture, a una sovranità del dato intesa come capacità di decidere, dal momento che controllare la qualità e la *governance* del dato significa ridurre lo spazio di manipolazione, limitare l'avvelenamento delle pipeline informative, rendere più difficile il sabotaggio delle decisioni.

C'è poi un secondo livello, spesso sottovalutato: l'Europa usa questa impostazione come regolatore del mercato. Stabilire requisiti su trasparenza, *accountability*, sicurezza, accesso e uso dei dati significa definire le condizioni di ingresso e permanenza nel mercato digitale europeo. In un mondo frammentato, dove altri blocchi cercano sovranità attraverso *stack* e piattaforme, l'Europa esercita sovranità attraverso regole che diventano standard di mercato.

[10] Per i requisiti tecnici connessi alla NIS2, cfr. *Commission Implementing Regulation (EU) 2024/2690* del 17 ottobre 2024 e ENISA, *NIS2 Technical Implementation Guidance*, 2025.

[11] Sul nesso tra qualità/tracciabilità del dato e capacità decisionale come forma di difesa, cfr. P. IEZZI, R. RAZZANTE, *Algoritmo criminale. Come mafia, cyber e AI riscrivono le regole del gioco*, IlSole24Ore, Milano, 2024, pp. 87-104; M. MEZZA, *Guerre in codice. Come le intelligenze artificiali resettano la democrazia*, Donzelli, Roma, 2025, pp. 55-72.

Infine, questa scelta ha una dimensione non negoziabile: i diritti fondamentali dell'uomo e del cittadino. Se il dato è potere, allora la protezione della persona – *privacy*, limiti alla profilazione, non discriminazione, diritto alla trasparenza e alla contestazione – non è un accessorio etico, ma un elemento strutturale di stabilità democratica. Senza questo perimetro, la difesa contro la guerra cognitiva rischia di trasformarsi in un controllo interno, e la cura diventa peggiore della malattia.

Le regole, però, contano solo se diventano pratica: *audit*, verifica, *enforcement* e responsabilità effettiva lungo la *supply chain*. Altrimenti il "passaporto" del dato resta una dichiarazione e non una capacità.

7. *La* cybersecurity *come vantaggio competitivo e leva geopolitica*

In questa accezione la *cybersecurity* cambia la propria natura, evolvendo da mera competenza tecnica o disciplina "da addetti ai lavori" a fattore di vantaggio competitivo europeo e soprattutto leva geopolitica. Essa infatti è un pilastro della difesa, perché protegge sistemi, dati e servizi essenziali, e costituisce un elemento di deterrenza, costringendo l'attaccante a dover considerare i costi di una offensiva cibernetica, le proprie capacità di risposta e le relative conseguenze. La cybersicurezza ha anche un valore nella sfera dell'economia, perché regola l'accesso al mercato digitale: qualsiasi soluzione tecnologica deve infatti rispettare precisi requisiti e superare rigidi controlli. Ha inoltre una dimensione sociale, perché tutela dei diritti fondamentali quali la *privacy*, i limiti alla profilazione e la protezione dell'identità del cittadino. Essa ha infine una dimensione politico-militare, perché contribuisce a definire il confine tra atto ostile e soglia di guerra, e a rendere credibile una capacità di reazione.

In altre parole, la *cybersecurity* diventa un elemento di equilibrio. E in un mondo in cui la conflittualità si muove sottosoglia, l'equilibrio non si costruisce con *slogan*, bensì con competenze, professionalità, tecnologie e investimenti.

Investire nella cybersicurezza è quindi un dovere non tanto per inseguire una logica esclusivamente militare, politica o economica, ma per una ragione più essenziale: difendere la democrazia, garantire i diritti dei cittadini e proteggere la possibilità di costruire un futuro più solido per le prossime generazioni. E, soprattutto, per garantire la verità e l'unicità del dato, unico elemento che garantisce la corretta trasmissione dell'informazione e definisce pertanto la realtà.

IMPRESE E ISTITUZIONI NELLA GUERRA IBRIDA: DIFENDERE LA REPUTAZIONE COME INFRASTRUTTURA CRITICA

Gianluca Giansante[*]

SOMMARIO: 1. Quando una foto ferma i treni: la comunicazione nel nuovo scenario ibrido. – 2. L'ecosistema informativo come teatro di guerra: infodemia, *fake news* e manipolazione algoritmica. – 3. La difesa reputazionale delle imprese e delle istituzioni. – 4. Decalogo per il comunicatore nella guerra ibrida algoritmica.

1. *Quando una foto ferma i treni: la comunicazione nel nuovo scenario ibrido*

È notte fonda nella contea del Lancashire quando una foto compare online. Ritrae il ponte ferroviario di Lancaster gravemente danneggiato: una porzione della struttura è crollata, una voragine interrompe i binari. Nel giro di poche ore l'allarme si propaga. *Network Rail* – il gestore della rete britannica – ferma il traffico sulla linea, i treni verso la Scozia vengono bloccati o rallentati. Vengono mobilitate le squadre tecniche, scattano ispezioni e controlli d'emergenza. L'infrastruttura entra in crisi.

Solo dopo, con il passare delle ore, emerge la verità. È un giornalista della *Bbc* a sollevare i primi dubbi: l'immagine, analizzata con strumenti di verifica basati sull'intelligenza artificiale, risulta verosimilmente manipolata. I controlli sul posto confermano che il ponte è intatto, non presenta alcun danno. Dopo circa due ore di blocco la circolazione ferroviaria torna gradualmente alla normalità. Nessun attentato, nessun sabotaggio, nessun evento naturale disastroso.

Eppure, gli effetti sono stati reali, immediati, misurabili. È in episodi come questo che si coglie la natura della guerra ibrida contemporanea. Non serve colpire fisicamente un'infrastruttura per metterla fuori uso: è sufficiente colpire la percezione che la circonda. La crisi non nasce più dal danno, ma dal dubbio. Il campo di battaglia non è il ponte di Lanca-

[*] Socio di Comin & Partners e docente di Comunicazione istituzionale e reputazionale digitale nella LUISS "Guido Carli".

ster, ma lo spazio informativo che rende credibile l'idea che quel ponte possa essere crollato.

Con la rapida diffusione dell'intelligenza artificiale stiamo assistendo a una metamorfosi della definizione di crisi reputazionale. Per i professionisti della comunicazione del mondo aziendale e istituzionale, abituati a gestire reputazione e consenso, questo scenario è familiare e nuovo allo stesso tempo: il conflitto infatti si è spostato dalla trincea fisica alla "zona grigia", uno spazio ambiguo dove la distinzione tra pace e guerra è sfumata e il confine tra realtà e manipolazione digitale è labile.

Quando parliamo di guerra e affianchiamo l'aggettivo "ibrida" non stiamo infatti parlando di soldati o missili, di proiettili o carri armati. Stiamo pensando invece a una competizione costante che avviene sugli schermi dei nostri *smartphone*, nelle reti televisive, nelle nostre menti e nei comportamenti quotidiani di ciascuno di noi. La guerra contemporanea non cerca necessariamente la distruzione fisica dell'avversario come primo obiettivo; cerca di penetrare in quella che possiamo definire la "retrovia civile", colpendo le società dall'interno, promuovendo paure, stati d'animo e distorcendo le azioni.

In questo contesto, la tecnologia è il motore del conflitto. L'IA ha introdotto una velocità e una scala di operatività mai viste prima, trasformando la competizione geopolitica in una battaglia per la supremazia cognitiva. Se la guerra ibrida è il contesto, l'intelligenza artificiale è il catalizzatore che ne sta cambiando la natura. Stiamo entrando nell'era della *Algorithmic Hybrid Warfare* (guerra ibrida algoritmica): non dobbiamo pensare all'IA semplicemente come a una nuova arma nell'arsenale, come potrebbe essere un drone più veloce. L'IA è diventata il "sistema nervoso centrale" che coordina, sincronizza e ottimizza tutte le componenti della campagna ibrida, dal cyber-attacco alla disinformazione.

La vera rivoluzione sta infatti nella velocità e nella scala della manipolazione. L'IA generativa e i *Large Language Models* (LLM) permettono oggi di creare contenuti persuasivi, tradotti perfettamente in qualsiasi lingua e adattati culturalmente a specifici *target*, a costi irrisori e con volumi industriali. Dove un tempo servivano eserciti di *troll* umani per diffondere una narrazione tossica, oggi sistemi automatizzati possono generare milioni di messaggi unici, rendendo obsoleto il concetto tradizionale di *fact-checking* umano: la menzogna viaggia semplicemente troppo veloce per essere smentita in tempo reale. Oggi più che mai vale quanto affermava già il secolo scorso Winston Churchill: «una bugia fa in tempo a compiere mezzo giro del mondo prima che la verità riesca a mettersi i pantaloni».

Inoltre, l'IA potenzia l'efficacia del *cyber warfare*. Non parliamo solo di hackeraggio, ma di sistemi di *machine learning* capaci di scansionare milioni di righe di codice per trovare vulnerabilità o di creare email di *phishing* iper-realistiche che ingannano anche i manager più esperti. Questo livello di automazione garantisce agli attaccanti una "negabilità plausibile" (*plausible deniability*) e un'ambiguità strategica senza precedenti: l'attacco è così diffuso, rapido e anonimizzato, che l'attribuzione certa diventa un processo lento e complesso, paralizzando la capacità di reazione immediata.

Qual è il fine ultimo di questa macchina algoritmica? Qui entriamo nel cuore dell'attività di comunicazione: la costruzione della percezione collettiva. L'obiettivo strategico non è più quindi soltanto distruggere ponti o centrali elettriche (sebbene l'IA ottimizzi anche queste attività), ma colpire le "infrastrutture cognitive" della popolazione.

Siamo di fronte a una forma di *cognitive warfare* in cui il campo di battaglia è la mente umana. L'uso combinato di profilazione psicografica guidata dai Big Data e *micro-targeting* permette di identificare le paure, le rabbie e le divisioni latenti dei singoli e della società e di amplificarli chirurgicamente. L'obiettivo è influenzare il processo decisionale politico e strategico.

Per chi si occupa di comunicazione nelle aziende e nelle istituzioni comprendere questo nuovo scenario è una necessità urgente. È indispensabile per difendere la *governance* aziendale e politica nei suoi processi decisionali, affinché abbiano un set informativo corretto e non inquinato da informazioni tossiche. È fondamentale per garantire al cittadino la possibilità di effettuare scelte di voto e di comportamento democratico libere e non influenzate da interessi ostili. È cruciale per proteggere il *brand*, i manager e i prodotti dell'azienda da attacchi di competitor senza scrupoli.

Se l'ambiente informativo è saturo di *deepfake* iper-realistici, ad esempio, la capacità di valutare la realtà potrebbe essere manipolata. Se l'opinione pubblica è orientata negativamente verso una scelta politica a causa di una campagna di comunicazione orchestrata da una nazione nemica la scelta potrebbe svolgersi in un contesto inquinato. Se la reputazione di un prodotto o di un amministratore delegato viene compromessa per un attacco a base di *fake news* l'azienda ne potrebbe risentire in modo irreversibile. Erodere la fiducia nelle istituzioni democratiche, nei media e nelle aziende è quindi un nuovo metodo per destabilizzare un avversario senza sparare un solo colpo. In questo senso, l'IA non serve solo a ingannare, ma a rompere il contratto sociale, trasformando i cittadini e i consumatori in armi inconsapevoli.

La capacità con cui ci si prepara a possibili attacchi e la definizione di una strategia di risposta adeguata partono dalla conoscenza dei potenziali rischi a cui le nostre aziende e le nostre istituzioni sono esposte nel nuovo scenario. Cominciamo da qui.

2. *L'ecosistema informativo come teatro di guerra: infodemia,* fake news *e manipolazione algoritmica*

Fino a pochi anni fa la creazione di propaganda efficace richiedeva tempo, competenze linguistiche e una profonda conoscenza culturale del bersaglio. Oggi, i *Large Language Models* hanno abbattuto queste barriere. Questi sistemi sono in grado di generare testi grammaticalmente perfetti, stilisticamente coerenti, culturalmente adattati in pochi secondi e a costi irrisori. L'IA permette di creare campagne di *spear-phishing* iper-realistiche, email che sembrano provenire da colleghi o istituzioni fidate, eliminando quegli errori che un tempo erano il campanello d'allarme per la sicurezza aziendale. Questi modelli possono essere addestrati per generare contenuti che incitano all'odio, *fake news* su prodotti di largo consumo, teorie del complotto o narrazioni estremiste credibili, rendendo la disinformazione scalabile come mai prima d'ora.

Gli algoritmi di *machine learning* analizzano inoltre come le informazioni si diffondono nelle reti sociali, identificando i picchi di interesse e il loro eventuale decadimento, permettendo agli attaccanti di inserire le loro narrazioni nel momento esatto in cui l'onda emotiva è al culmine.

La vecchia propaganda "a tappeto" è obsoleta: oggi entriamo nell'era della propaganda di precisione. Utilizzando algoritmi di apprendimento automatico per analizzare enormi volumi di *Big Data* (tracce digitali, interazioni *social*, cronologia di navigazione), gli attori della guerra ibrida possono segmentare l'*audience* con una granularità inedita.

L'IA analizza il *sentiment* e i comportamenti degli utenti per identificarne le vulnerabilità: paure, pregiudizi, orientamenti politici e persino stati emotivi transitori. Una volta individuato un sottogruppo vulnerabile (ad esempio, cittadini scettici verso le istituzioni sanitarie o critici verso un'azienda strategica), il sistema invia messaggi "su misura" progettati per risuonare specificamente con quel profilo.

Questo approccio sfrutta le cc.dd. *echo chambers*, ambienti informativi chiusi, dove la narrazione viene percepita come un'opinione condivisa dal proprio gruppo di appartenenza, aumentandone l'efficacia per-

suasiva. Non si cerca più di convincere tutti della stessa bugia, ma di sussurrare a ciascuno la "propria" verità personalizzata.

Questo processo viene utilizzato per diffondere disinformazione che sembra provenire dal proprio ambiente sociale di fiducia, abbassando drasticamente le difese critiche dell'utente. L'IA non si limita quindi a generare contenuti, ma orchestra una strategia di attacco alle infrastrutture cognitive della società civile utilizzando spesso strumenti che creano disordine informativo.

Qui occorre fare una precisazione terminologica. Nel dibattito pubblico utilizziamo spesso il termine "*fake news*", ma nel contesto dell'analisi strategica e accademica questo termine è considerato impreciso e fuorviante. Per operare efficacemente in questo settore, è utile adottare una tassonomia più precisa secondo lo schema più consueto proposto da Wardle e Derakhshan[1]:

Disinformation: la disinformazione è la creazione e diffusione deliberata di informazioni false con l'intento specifico di causare danno.

Misinformation: si riferisce alla condivisione di informazioni false senza l'intento di nuocere. Spesso sono i cittadini comuni che, ingannati dalla disinformazione iniziale, diventano vettori inconsapevoli del contagio informativo. L'IA accelera questo processo creando contenuti emotivamente coinvolgenti che stimolano la condivisione impulsiva.

Malinformation: è forse la minaccia più insidiosa per le aziende e le istituzioni. Si tratta di informazioni vere e genuine, ma diffuse con l'intento deliberato di causare danno, spesso violando la *privacy* o rivelando dati sensibili fuori contesto. Un esempio classico è la diffusione strategica di email private (*leaks*) per danneggiare la reputazione.

L'IA sta industrializzando tutte queste categorie. Le Reti Generative Avversarie (GANs) sono strumenti di apprendimento automatico che permettono di creare *deepfake* audio e video iper-realistici, che possono essere usati per fabbricare prove false o per impersonare leader aziendali e politici. Questo crea un disordine informativo strutturale: la semplice esistenza di queste tecnologie fa sì che la realtà stessa diventi opinabile e la fiducia nelle prove documentali crolli, paralizzando i processi decisionali.

Un ultimo strumento in mano ai creatori di mondi paralleli è la possi-

[1] C. Wardle, H. Derakhshan, *Information disorder: Toward an interdisciplinary framework for research and policy making,* Council of Europe, 2017.

bilità di generare consenso artificiale. Per rendere credibile una narrazione, serve il supporto sociale, o almeno l'illusione che ci sia. Qui entrano in gioco i *bot*. Dimentichiamo gli *script* rudimentali di un decennio fa; oggi operiamo con "*bot* intelligenti" e *cyborg*. I *cyborg* sono account ibridi: gestiti in parte da *software* automatizzati per garantire volume e rapidità, ma supervisionati da esseri umani per gestire interazioni complesse e sfumature emotive che all'IA potrebbe mancare. Per rendere valida una tesi, reti coordinate di *bot* vengono attivate per amplificare contenuti divisivi, gonfiare artificialmente *hashtag* polemici e sopprimere le voci contrarie.

L'IA permette a questi bot di adattare il proprio comportamento per eludere i filtri delle piattaforme social, simulando ritmi di sonno-veglia umani e interagendo in modo apparentemente organico per polarizzare il dibattito pubblico e logorare la coesione sociale. Un attacco di disinformazione sembrerà così non solo realistico ma anche supportato da un forte consenso sociale, aggravandone così la capacità distruttiva.

Infine, occorre tenere in conto che l'automazione dell'attacco tramite IA aggrava drammaticamente il divario temporale tra l'incidente e l'attribuzione. Mentre un attacco informatico o una campagna di disinformazione generata dall'IA può dispiegarsi in millisecondi, l'attribuzione dell'attacco richiede spesso settimane o mesi. Questo ritardo crea un "campo di forza dell'impunità": quando la vittima è finalmente in grado di puntare il dito contro il colpevole con certezza, il danno reputazionale o politico è già stato fatto e l'attenzione del pubblico si è spostata altrove.

Per le aziende e le istituzioni democratiche, questo significa che le strategie di risposta sono spesso inefficaci. La sopravvivenza dipende quindi dalla capacità di operare in un ambiente perennemente contaminato e di prevenire gli attacchi. Proviamo a capire come è possibile farlo.

3. La difesa reputazionale delle imprese e delle istituzioni

In un contesto in cui la velocità e la scala degli attacchi ibridi superano le capacità di risposta, il paradigma della comunicazione di crisi deve evolvere da un atteggiamento puramente reattivo a una di prevenzione attiva.

Per un comunicatore aziendale e istituzionale che opera in un contesto di guerra ibrida, la prima consapevolezza strategica è che la reputazione non può più essere gestita come un asset "*soft*" ma come una *infrastruttura critica immateriale*. Deve essere trattata come un rischio sistemico, al pari del rischio *cyber*, finanziario o regolatorio.

Questo implica innanzitutto la necessità di dotarsi di un *piano di gestione del rischio reputazionale* formalizzato, approvato a livello di vertice e integrato nei meccanismi di *governance* aziendale. Non si tratta di un documento di stile, ma di una mappa delle esposizioni ai rischi: settori sensibili, decisioni ad alto impatto simbolico, vulnerabilità narrative dell'azienda e del *management*, dipendenze geopolitiche e tecnologiche che possono essere strumentalizzate in chiave ostile.

In assenza di questa mappatura preventiva, ogni risposta comunicativa è inevitabilmente tattica e tardiva.

Proviamo dunque a delineare i passaggi essenziali di una difesa reputazionale dell'impresa.

Primo: accorgersi che la crisi esiste è la precondizione di ogni azione di risposta. Il monitoraggio continuo aumenta la capacità di allerta precoce. L'elemento fondamentale per rispondere efficacemente a una crisi non è comunicare, ma riconoscere tempestivamente che una crisi è in atto. Nella guerra ibrida algoritmica, molte crisi non si manifestano con eventi evidenti, ma prendono forma nello spazio informativo attraverso narrazioni artificiali, campagne di disinformazione o contenuti sintetici generati dall'IA. Per questo le aziende devono dotarsi di sistemi di monitoraggio continuo e di *social listening* avanzato, in grado di intercettare anomalie nei flussi informativi e segnali precoci di attacchi coordinati prima che diventino virali. Poiché questi attacchi operano a velocità di macchina, anche la capacità di rilevazione deve essere supportata da strumenti di intelligenza artificiale, senza i quali l'intervento umano arriva inevitabilmente troppo tardi.

Secondo: dotarsi di una *war room* reputazionale come dispositivo decisionale costante, non come *task force* da attivare nelle emergenze. Nella guerra ibrida algoritmica il tempo è la variabile decisiva. Per questo le aziende devono prevedere l'attivazione di una *war room reputazionale* prima di subire la crisi, con ruoli, responsabilità e soglie di attivazione chiaramente definite. La *war room* non è un gruppo informale che si riunisce quando scoppia il caso, ma un dispositivo decisionale a catena corta, capace di funzionare anche in condizioni di informazione incompleta e pressione esterna.

Elemento centrale è la catena di comando: chi decide cosa, in quali tempi e con quale livello di autonomia. In assenza di una delega chiara, la comunicazione si paralizza proprio nel momento in cui la velocità dell'attacco richiederebbe decisioni rapide. Il comunicatore, in questo contesto, non è un semplice esecutore, ma il garante della coerenza strategica tra azione, narrazione e posizionamento pubblico dell'azienda.

Terzo: definire la mappa degli *stakeholder* da informare in caso di attacco informativo. Uno degli errori più diffusi è pensare alla comunicazione di crisi come a un messaggio unico rivolto a un "pubblico generale". Nella guerra ibrida questo approccio è inefficace e pericoloso. Serve una mappa dei *target* strategici dettagliata e aggiornata, che distingua chiaramente tra dipendenti, mercato finanziario, clienti chiave, media, istituzioni nazionali e sovranazionali, *stakeholder* territoriali e, se necessario, opinione pubblica generalista.

Ogni *target* ha tempi, linguaggi, aspettative e livelli di sensibilità differenti. Un messaggio corretto per il mercato può essere astruso per i dipendenti; una comunicazione informale alle istituzioni può suscitare ulteriori dubbi nei media. La mappa dei *target* non è un esercizio di *marketing*, ma uno strumento di *de-confliction* comunicativa, che riduce il rischio di messaggi incoerenti o contraddittori amplificati dagli algoritmi.

Quarto: definire messaggi approvati, per ridurre l'attrito decisionale sotto stress. In uno scenario di attacco reputazionale, il tempo speso a scrivere il messaggio giusto è spesso il tempo in cui la narrazione ostile si consolida. Per questo è fondamentale disporre di un set di messaggi chiave pre-costruiti e pre-approvati sui principali rischi identificati nel piano reputazionale: incidenti industriali, *cyber breach*, accuse di natura etica, attacchi al *management*, strumentalizzazione geopolitica di decisioni aziendali.

Questi messaggi non devono essere comunicati automaticamente, ma devono esistere come *baseline* narrativa condivisa, che consenta di reagire senza improvvisazioni, mantenendo coerenza semantica e giuridica. La preparazione dei messaggi in tempo di pace è una forma di riduzione del rischio, non di rigidità comunicativa.

Quinto: dotarsi di strumenti e canali informativi per raggiungere tutti i *target* rilevanti. Nessuna strategia è efficace se non è supportata da strumenti adeguati. La guerra ibrida colpisce simultaneamente più livelli e richiede una *capacità di* outreach *differenziata*. L'azienda deve dotarsi di canali e strumenti che consentano di parlare rapidamente e direttamente ai *target* strategici: sistemi di comunicazione interna per dare notizie chiare e tempestive ai colleghi, canali dedicati per investitori e analisti, relazioni istituzionali strutturate per dare messaggi chiari ai regolatori, una interlocuzione continua con i media di riferimento e canali *social* strutturati per raggiungere il pubblico di riferimento in modo credibile.

Affidarsi esclusivamente ai *social network* o ai media generalisti significa delegare il controllo del messaggio agli algoritmi. La resilienza repu-

tazionale passa invece dalla capacità di attivare tutti i canali proprietari e quelli diretti ciascuno secondo le proprie preferenze.

In sintesi, il comunicatore che opera nella guerra ibrida non è chiamato a essere più creativo o più reattivo, ma più strutturato. La differenza tra un'azienda vulnerabile e un'azienda resiliente non sta nella brillantezza della risposta, ma nella qualità della preparazione: piani, catene di comando, messaggi e strumenti pronti prima che il conflitto emerga. In un ambiente informativo militarizzato, la comunicazione efficace è una funzione di *governance*, non di emergenza.

4. *Decalogo per il comunicatore nella guerra ibrida algoritmica*

La guerra ibrida algoritmica ha modificato in modo irreversibile il ruolo della comunicazione nelle imprese e nelle istituzioni. La reputazione non è più solo il risultato di ciò che si fa o si dice, ma è potenzialmente il bersaglio diretto di operazioni ostili che agiscono nello spazio informativo, sfruttando velocità, ambiguità e saturazione cognitiva.

In questo contesto, il comunicatore non opera più in una logica prevalentemente narrativa o reattiva, ma all'interno di un sistema di difesa più ampio, dove percezione, fiducia e capacità decisionale diventano fattori strategici.

Il decalogo che segue non è una lista di buone pratiche comunicative né un prontuario di *crisis management* tradizionale. È uno spunto sintetico di alcuni dei principi che un comunicatore può adottare per muoversi efficacemente in un ambiente informativo mutato, dove la differenza tra resilienza e vulnerabilità non è data dalla brillantezza della risposta, ma sempre di più dalla qualità della preparazione.

La reputazione è un'infrastruttura critica, non solo un capitale simbolico. La reputazione non è un asset "*soft*": è un fattore abilitante della continuità operativa. Deve essere gestita come rischio sistemico, inserita nella governance aziendale e presidiata con la stessa serietà del rischio *cyber*, finanziario o regolatorio.

La crisi non è una situazione eccezionale ma un rischio permanente. Nella guerra ibrida non esistono fasi di pace comunicativa. L'assenza di attacchi visibili è una condizione temporanea, non uno stato stabile. La preparazione non è un progetto, ma una funzione continua.

È fondamentale avere un piano di comunicazione di crisi strutturato e pre-approvato. In un contesto di guerra ibrida, la comunicazione di crisi non può essere improvvisata né delegata all'urgenza del momento. L'a-

zienda deve disporre di un piano di gestione del rischio reputazionale, formalizzato e approvato dal *board*. Il piano deve definire scenari di rischio, processi decisionali, ruoli e responsabilità, messaggi di base e canali di attivazione, consentendo all'organizzazione di reagire in modo rapido, coordinato e coerente anche in condizioni di informazione incompleta. In assenza di un piano preesistente, ogni risposta rischia di essere tardiva, frammentata e facilmente neutralizzata nello spazio informativo ostile.

La capacità di diagnosticare l'attacco rapidamente è un elemento determinante. Il monitoraggio è un'attività fondamentale. Le campagne ostili emergono attraverso *pattern* anomali: sincronizzazione sospetta, accelerazioni artificiali, temi marginali improvvisamente centrali. Il comunicatore efficace intercetta l'attacco prima che diventi virale, leggendo il "quando" e il "come", non solo il "cosa".

Costruisci una war room *reputazionale stabile.* La velocità è la variabile decisiva. La *war room* deve essere costituita prima della crisi, con ruoli, deleghe e soglie di attivazione chiare. In condizioni di pressione, decidere velocemente conta più che decidere perfettamente.

Prepara messaggi chiave prima della crisi per ridurre l'attrito decisionale In una crisi algoritmica il tempo per "scrivere bene" non esiste. I messaggi pre-approvati non sono rigidità, ma ancore strategiche che permettono di reagire subito mantenendo coerenza semantica e legale.

Garantisci disciplina comunicativa: una voce, una linea, una sequenza. Sotto attacco, molte aziende si danneggiano da sole: manager che parlano a titolo personale, messaggi incoerenti tra funzioni o paesi, reazioni emotive o, al contrario, formali e fredde. Il comunicatore deve contribuire a garantire coerenza e ordine, evitando che il caos interno diventi materiale per la narrazione ostile.

Raggiungi tutti gli stakeholder rilevanti sui canali che usano davvero. In una crisi di guerra ibrida non basta "avere un messaggio": bisogna farlo arrivare a tutti gli *stakeholder* chiave attraverso i canali che ciascuno utilizza per informarsi. Dipendenti, investitori, clienti, media e istituzioni non condividono né le stesse fonti né gli stessi tempi di attenzione. Dimenticarne uno significa lasciare uno spazio informativo scoperto che verrà occupato da narrazioni ostili. La mappatura degli *stakeholder* deve quindi tradursi in una architettura di canali capace di coprire l'intero perimetro strategico, senza zone d'ombra.

Non combattere solo sui social: presidia canali proprietari e relazionali Affidarsi esclusivamente ai *social network* significa consegnare il controllo del messaggio agli algoritmi. La resilienza reputazionale passa da canali diretti, relazioni consolidate e credibilità costruita prima dell'attacco. La

telefonata o il messaggio diretto ai rappresentanti delle istituzioni rilevanti non è un accessorio ma un elemento determinante della gestione della crisi.

Il tuo ruolo non è solo raccontare, ma contribuire a governare la crisi. Nella guerra ibrida il comunicatore non è solo il costruttore e il diffusore di un racconto ma un attore di *governance* che opera sul confine tra percezione, decisione e fiducia. La sua efficacia si misura prima della crisi, non solo dopo.

QUANTUM COGNITIVE WARFARE

Fabrizio De Longis[*]

1. *Introduzione*

Il calcolo quantistico e la modellazione quantistica, unite alle opportunità offerte dell'*Artificial intelligence* (AI) e dai potenziamenti neuronali, sembrano possedere le caratteristiche potenziali di ridefinizione strutturale della Guerra Cognitiva.

L'approccio cognitivo alla tecnologia quantistica appare dipanarsi in due direttive di studio: da un lato, rispetto alla potenzialità di calcolo dello strumento quantistico per la comprensione del processo decisionale umano nel contesto entropico incerto[1] (con una particolare propensione all'indagine verso le capacità previsionali); dall'altro lato, rispetto all'utilizzo delle tecnologie quantistiche per modificare il processo cognitivo delle persone[2]. In questo senso, il presente studio si pone l'obiettivo di analizzare le potenzialità convergenti di queste due direttive, soprattutto in orizzonte alla Guerra Cognitiva.

[1] Cultore della materia di Ordinamenti giuridici e gestione dei flussi migratori all'Università degli Studi Internazionali di Roma.

[1] In fisica l'entropia descrive il grado di disordine o incertezza di un sistema quantistico, spesso associato alla perdita di informazione sulle sue proprietà microscopiche (ad esempio tramite l'entropia di von Neumann). Allo stesso modo il contesto entropico incerto dell'agire umano comporta disordine e incertezza che per essere in grado di osservare, interpretare, scegliere e agire, l'uomo deve portare a un sufficiente livello di ordine. Riuscendoci anche tramite un processo di selezione delle informazioni con cui disperde quelle eccessivamente incerte, non utili o troppo complesse e faticose. In questo senso il contesto umano può essere inteso come naturalmente entropico, da cui deriva una potenziale incertezza (data anche dalla creatività) che se non viene governata (con altrettanta creatività), conduce alla generazione del caos e con esso al collasso della società.

[2] Si vedrà più avanti che per modifica si intendono due principali direttive: influire e potenziare.

Tali condizioni rendono, infatti, la tecnologia quantistica di cruciale importanza nel novero delle soluzioni applicabili alla Guerra Cognitiva. In un primo senso ciò avviene per le pure proprietà scientifiche che consentono il raggiungimento di soluzioni applicabili nel calcolo probabilistico che sono differenti dai modelli classici. In special modo questa dinamica si evidenzia a fronte di modelli dinamici per scenari complessi. Per l'altro senso le tecnologie quantistiche emergono in virtù della maggiore corrispondenza all'analisi e all'applicabilità rispetto all'ibridazione tipica del contesto reale, entropico e incerto. In particolar modo appare meglio attribuibile quale fonte di risposte e soluzioni per l'interpretazione e il governo dell'incertezza, condizione tipica del processo cognitivo umano. Soprattutto la tecnologia quantistica sembra più adatta a comprendere in che maniera la mente agisca per la gestione complessa di informazioni incerte nel processo di assunzione di scelte critiche in contesti entropici.

Proprio secondo questo approccio le tecnologie quantistiche sembrano seguire principi di inferenza che meglio si adattano alle cangianti analisi contestuali soggette a interferenze. Difatti contemplano sostanzialmente la potenziale fallacia (o irrazionalità) e la caratteristica di creatività del processo decisionale umano calato nel contesto reale. Tutto ciò, anche in virtù di determinati elementi fisici di similitudine fra i processi di progettazione ed esecuzione quantistica e quelli di progettazione ed esecuzione cognitiva. Si consente, così, l'ottenimento di importanti potenzialità previsionali, le quali, nel contesto della Guerra Cognitiva, offrono nuove opportunità di minaccia, soprattutto nel campo della formazione dei giudizi, dell'assunzione delle scelte e nel novero totale delle capacità creative. Definendo un nuovo ruolo per la *Quantum Cognitive Warfare* che la rende cardinale per il futuro delle società e degli Stati.

2. *La Cognizione quantistica*

Secondo quanto qui assunto, la cognizione quantistica riguarda l'impiego della scienza quantistica in due progressivi livelli cognitivi. Dapprima, essa riguarda l'utilizzo della teoria quantistica quale insieme coerente di strumenti formali per approcciare un quadro concettuale che sia in grado di spiegare fenomeni cognitivi enigmatici. Come secondo aspetto, concerne la potenzialità degli strumenti quantistici nel modificare il processo cognitivo delle persone tramite tre direttive: l'utilizzo di strumenti di ottenimento ed elaborazione di informazioni massive atte a implementare le azioni offensive cognitive; l'utilizzo e la manipolazione di stru-

menti fisici di potenziamento cognitivo; la creazione di supercomputer quantistici neuroformici dedicati all'AI.

La cognizione quantistica di primo livello si concentra nel raggiungimento di risultati che sappiano spiegare la cognizione umana. Ciò avviene tramite l'analisi di quei processi cognitivi che portano gli individui a formare giudizi, decisioni, concetti, ragionamenti, soluzioni creative, memoria e percezioni. In questo il processo decisionale sembra poter essere descritto con maggiore efficacia attraverso l'approccio matematico di tipo quantistico[3]. Proprio secondo questo approccio la scienza quantistica suggerisce due strumenti di analisi dei fenomeni neuronali[4].

La complementarietà, in primo luogo, suggerisce di analizzare le reazioni neuronali in sequenza. Immaginando che l'evento di una di queste sia influenzato da un precedente contesto neuronale e a sua volta ne generi uno nuovo. Il quale, in sequenza, influenzi le risposte genate dalla reazione successiva.

La sovrapposizione, invece, suggerisce di analizzare alcuni stati neuronali differendo dall'ordinario assunto che li vorrebbe ricondotti a una loro definizione in relazione a dei valori definiti. Infatti, essa suggerisce di considerare che tutti i possibili valori all'interno della sovrapposizione abbiano un potenziale per essere espressi.

In questo senso la cognizione quantistica agisce nello spettro della logica. Tuttavia, mentre la logica classica obbedisce all'assioma commutativo[5], la teoria quantistica consente la complementarità di risultati differenti. Dunque, la logica classica obbedisce all'assioma commutativo, alla regola classica della probabilità congiunta[6] e all'assioma distributivo[7], obbedendo di conseguenza alla legge della probabilità totale[8]. La teoria quantistica, invece, riconosce la possibilità di complementarietà,

[3] A. QADIR, *Quantum economics*, in *Pakistan Economic and Social Review*, 1978, pp. 117-126.

[4] Qui interpretati anche quali processi di sussistenza di un eguale livello psicologico.

[5] L'assioma o proprietà commutativa stabilisce che in addizione e moltiplicazione l'ordine dei termini non influenza il risultato. Vale per numeri naturali, interi, razionali e reali. Non si applica invece a sottrazione e divisione.

[6] La regola classica della probabilità congiunta (o composta) determina la probabilità che due eventi si verifichino contemporaneamente.

[7] La proprietà distributiva afferma che moltiplicare una somma per un numero equivale a moltiplicare ciascun addendo per quel numero e poi sommare i risultati ottenuti.

[8] La legge della probabilità totale permette di calcolare la probabilità di un evento A che può verificarsi in combinazione con una serie di eventi mutualmente esclusivi Ei (che formano una partizione dello spazio campionario), sommando le probabilità condizionate.

ossia che l'ordine delle domande poste modifichi le probabilità delle rispettive risposte, superando l'assioma commutativo e l'obbedienza alla regola classica della probabilità congiunta[9]. In questo senso, applicata al cognitivismo, essa considera che le domande possano non commutare, generando effetti di ordine delle domande. Effetti per i quali, al variare dell'ordine delle stesse, si hanno effetti vicendevoli sulle possibili risposte che in uno stato neutro, non posizionate, sono differenti a livello probabilistico. Quindi la misura modifica lo stato del sistema poiché osservare non è neutrale. L'atto di fare una domanda modifica il sistema nervoso e si generanno effetti di ordine simili a quelle della meccanica quantistica[10].

Inoltre, la tecnologia quantistica consente una sovrapposizione degli stati che permette la violazione della legge classica della probabilità totale. Ossia, prima della misurazione, il sistema quantistico non ha uno stato ben definito, ma si trova in una sovrapposizione di più (tutti) stati possibili. Solo con l'osservazione o la misura, il sistema collassa in uno stato definitivo. Un processo noto come collasso della funzione d'onda. Di conseguenza, al porgere di una domanda (ovvero alla misurazione), la sovrapposizione dei vari stati collassa in una risposta. Tuttavia, questa risposta non deriva da un'unica possibilità, ma dal fatto che la sovrapposizione iniziale permette di esplorare tutte le soluzioni possibili, prima che la misurazione comporti la selezione di quella definitiva.

Va considerato che la teoria della probabilità classica si basa sulla teoria degli insiemi, mentre la teoria della probabilità quantistica si basa sulla rappresentazione geometrica degli stati quantistici. In quest'ultimo caso, gli stati e le misure sono trattati come entità geometriche in spazi vettoriali, e la probabilità non è una semplice somma di possibilità, ma una misura che dipende dalle proprietà geometriche degli stati nel sistema. Ciò va calato nel fatto che una teoria della probabilità è un insieme di assiomi matematici su come combinare e aggiornare le probabilità. Si può, quindi, comprendere che esistono due teorie generali per l'assegnazione della probabilità degli eventi. Quella classica, di Kolmogorov, e quella quantistica, di von Neumann. La prima definisce gli eventi come sottoinsiemi di un insieme universale, che obbediscono a tutte le leggi

[9] Chiedere A e poi B, non equivale a chiedere B e poi A, che è invece accettato dalla teoria classica.

[10] J. DER DERIAN, A. WENDT, *Quantum International Relations: A Human Science for World Politics*, Oxford University Press, Oxford, 2022; D.W. MOORE, *Measuring New Types of Question-Order Effects: Additive and Subtractive*, in *The Public Opinion Quarterly*, 2002, pp. 80-91.

dell'algebra booleana[11]. La seconda definisce gli eventi come sottospazi di uno spazio di Hilbert[12], che obbediscono a tutte le leggi dell'algebra booleana, tranne l'assioma distributivo. In virtù di quest'ultimo, la teoria classica aderisce a uno dei suoi teoremi più importanti: la legge della probabilità totale. A questo punto si ha la condizione per cui la logica quantistica, non ha l'obbligo di aderire alla legge distributiva e le probabilità quantistiche non devono obbedire alla legge della probabilità totale, basandosi, invece, sulla rappresentazione nello spazio di Hilbert. Secondo cui le probabilità quantistiche sono chiamate ad obbedire ad altre due leggi: la reciprocità[13] e la doppia stocasticità[14]. A queste, la teoria classica non deve obbedire[15], non basandosi sulla rappresentazione nello spazio di Hilbert.

Superare la legge classica della probabilità totale può produrre importanti effetti cognitivi, soprattutto in riferimento alla cognizione umana che può subire importanti interferenze. Questo perché si infrange il modello markoviano[16] che suppone che a fronte di dati, si ottenga una probabilità. Mentre il modello quantistico consente di sovrapporre e quindi creare interferenza fra due differenti percorsi di pensiero, comportando un annullamento (distruzione) di uno dei due percorsi o la risonanza (costruttiva) di uno di questi. Tale sovrapposizione può ovviamente collassare e ciò avviene nelle condizioni di necessità della risoluzione dell'indeterminatezza relativa[17], ossia quando si necessita della complementarietà

[11] Sistema matematico basato su variabili binarie che assumono solo i valori vero (1) o falso (0).

[12] Si tratta di uno spazio vettoriale completo dotato di un prodotto scalare, che consente di definire la distanza e l'angolo tra i vettori.

[13] Per due numeri primi dispari, la relazione tra le soluzioni dipende dal fatto che almeno uno sia 1.

[14] Si riferisce alla natura intrinsecamente casuale dei fenomeni quantistici che si manifesta principalmente su due livelli: il primo di stato, con sovrapposizione e probabilità, per cui prima di una misurazione, una particella non ha proprietà definite (posizione, momento, *spin*) ma esiste in una sovrapposizione di tutti i possibili stati, il quale da un risultato probabilistico governato dalla funzione d'onda. Il secondo di misura con il collasso della funzione d'onda, per cui si ha il processo deterministico con cui l'atto stesso della misurazione provoca un collasso istantaneo e casuale della funzione d'onda in uno degli stati definiti.

[15] P. Bruza, J. Busemeyer, L. Gabora, *Introduction to the Special Issue on Quantum Cognition*, in *Journal of Mathematical Psychology*, 2009, pp. 303-305.

[16] È un processo aleatorio in cui la probabilità di transizione che determina il passaggio a uno stato di sistema dipende solo dallo stato del sistema immediatamente precedente.

[17] Descrive i limiti di misurazione dei valori di grandezze fisiche coniugate o incompatibili in un sistema fisico.

per determinare il contesto (avere una risposta). Questa dinamica conduce a due effetti determinati dalla fallacia di congiunzione, riguardanti l'ordine e la categorizzazione decisionale, influenzando così l'identificazione di: condizione, classificazione, decisione, relazione e azione.

La contestualità si ha quando questi due sistemi quantistici si trovano in stati sovrapposti fra loro, generando una condizione in cui possono verificare delle interferenze. Questa sovrapposizione si esprime all'interno dell'apparato probabilistico in forma che non si trova nel quadro probabilistico classico. A questo si aggiunge l'*entanglement* quantistico, condizione in cui due sistemi quantistici separati si comportano come se fossero un tutt'uno generando un fenomeno anomalo (fino alla messa in discussione della realtà). In questo caso si può misurare la non-località, la quale comporta che l'esecuzione di una misurazione su un sistema influenza direttamente e istantaneamente lo stato di un altro sistema, anche quando tali sistemi sono separati. Nel contesto cognitivo e psicologico, il concetto di non separabilità implica che due o più aspetti della mente o del pensiero (per esempio emozioni, decisioni, percezioni) non possano essere trattati come completamente distinti e separati. Piuttosto, sono interconnessi in modi che non possono essere descritti indipendentemente. Tale condizione di similarità con i sistemi quantistici può consentire di misurare fenomeni cognitivi e psicologici che altrimenti non appaiono spiegabili. In questo modo, la natura contestuale dei concetti e le loro combinazioni sembrano maggiormente spiegabili secondo un approccio di analisi di due entità quantistiche che si intrecciano. Il che consente di formare una nuova entità con proprietà diverse da quelle della somma di entrambe le parti, che non può essere manipolata o soggetta a influenze, senza coinvolgere le altre[18].

Quanto appare interessante è che nella misurazione dei fenomeni, ponendo a confronto i due modelli (classico e quantistico), quello quantistico ottiene una capacità di risposta migliore. Il modello quantistico appare dunque in grado di spiegare meglio i dati empirici, come visibile in tabella.

[18] P. BRUZA, J. BUSEMEYER, L. GABORA, *Introduction to the Special Issue on Quantum Cognition*, cit.

Fenomeno	Fallimento Modello Classico	Successo Modello Quantistico
Violazione *Temporal Bell Inequality*[19]	I modelli classici richiedono il rispetto della *Temporal Bell Inequality*, ma gli esperimenti mostrano delle violazioni.	Il modello quantistico spiega queste violazioni tramite l'interferenza e il contesto.
Conjunction fallacy (Linda)[20]	Viola la legge della probabilità classica congiunta.	Il modello quantistico spiega queste violazioni tramite l'interferenza e il contesto.
Order Effects[21]	La probabilità classica richiede indipendenza dall'ordine, ma i dati mostrano differenze.	Gli operatori non commutativi quantistici spiegano le variazioni.
Disjunction Effect[22]	Viola la legge classica della probabilità totale.	Il modello quantistico ammette interferenze tra stati decisionali.
Over-/Under-distribution memoria[23]	I modelli classici non prevedono distribuzioni anomale che però vengono osservate.	La sovrapposizione e l'interferenza spiegano questi effetti.

3. Verso il secondo livello

Proprio le due caratteristiche quantistiche, la complementarietà e la sovrapposizione, sembrano adattarsi meglio alla spiegazione di fenomeni psicologici non chiari, quali: le violazioni del processo decisionale razionale; gli errori di giudizio di probabilità; il ragionamento causale; i giudizi di similarità asimmetrica; la vaghezza; l'intreccio nella memoria associativa; la sovradistribuzione nella memoria episodica[24]. Ossia, quel divergere

[19] O.J. Waddup, J.M. Yearsley, P. Blasiak, E.M. Pothos, *Temporal Bell inequalities in cognition*, in *Psychonomic Bulletin & Review*, 2023, pp. 1946-1953.

[20] A. Tversky, D. Kahneman, *Extensional Versus Intuitive Reasoning: The Conjunction Fallacy in Probability Judgment*, in *Psychological Review*, 1983, pp. 293-315.

[21] J.M. Yearsley, J.r. Busemeyer, *Quantum cognition and decision theories: A tutorial*, in *Journal of Mathematical Psychology*, 2016, pp. 99-116.

[22] J. Huang, G. Epping, J.s. Trueblood, J.m. Yearsley, J.r. Busemeyer, E.m. Pothos, *An overview of the quantum cognition research program*, in *Psychonomic Bulletin & Review*, 2025, pp. 2507-2556.

[23] J.R. Busemeyer, M. Ozawa, E.m. Pothos, N. Suchiya, *Incorporating episodic memory into quantum models of judgment and decision*, in *Philosophical Transactions of the Royal Society A*, 2025.

[24] J.R. Busemeyer, Z. Wang, *What Is Quantum Cognition, and How Is It Applied to Psychology?*, in *Current Directions in Psychological Science*, 2015; pp. 163-169.

dei processi cognitivi e psicologici dalla legge della probabilità totale. In questo senso si parla di *quantum decision theory*: la teoria della decisione quantistica[25], o simulazione della dinamica di una comunità, che si pone obiettivi di analisi di portata sociale[26].

Di conseguenza, la teoria quantistica si approccia all'analisi dei modelli decisionali cercando di modellizzarli tramite la creazione di un quadro probabilistico alternativo alla teoria probabilistica classica. A tal fine ci si concentra, come detto, su quei comportamenti umani considerati paradossali o irrazionali dal punto di vista proprio della teoria classica. In questo senso i modelli provano a studiare l'ordine di formazione delle scelte e delle azioni rispetto alla loro difformità dalla teoria della probabilità classica o dalla massimizzazione dell'utilità attesa. Non puntando, tuttavia, ad eliminare le strutture formali alla base del processo decisionale, ma provando a trovarne una nuova forma interpretativa che non sia quella classica. Per farlo, considerano gli effetti di interferenza, la formazione dei giudizi costruttivi e gli effetti di contesto.

Contemporaneamente, la teoria quantistica si pone una domanda a cui gli economisti cercano risposte da secoli: come mai alcune scelte non conducono alla massimizzazione dell'utilità attesa, nonostante siano fatte in un'ottica di razionalità perfetta[27].

Di grande interesse è che questi modelli sono partiti dal tentativo di spiegazione di risultati dati, non pienamente spiegabili in maniera classica, per convergere sull'indagine delle capacità previsionali[28] (come per il problema di Linda[29] o la violazione della *Temporal Bell Inequalities*[30]). In questo, l'indagine si è concentrata in ambiti cruciali per il processo cognitivo degli individui, quali: le fallacie di congiunzione/disgiunzione nel giudizio probabilistico; le combinazioni concettuali; la similarità; gli effetti d'ordine sui giudizi; l'inferenza causale; l'effetto di disgiunzione

[25] V.I. YUKALOV, *Evolutionary processes in quantum decision theory*, in *Entropy*, 2020, p. 681.

[26] E. PRATI, *Introduzione*, in E. PRATI, a cura di, *Quantum Diplomacy*, 2022, pp. 1-7.

[27] D. KAHNEMAN, A. TVERSKY, *Choices, Values, and Frames*, Cambridge University Press, 2000.

[28] J.M. YEARSLEY, J.R. BUSEMEYER, *Quantum cognition and decision theories: A tutorial*, cit.

[29] H.W. BRACHINGER, P-A. MONNEY, *The Conjunction Fallacy: Explanations of the Linda Problem by the Theory of Hints*, in *International Journal of Intelligent Systems*, 2003, pp. 75-79.

[30] J.M. YEARSLEY, E.M. POTHOS, *Challenging the classical notion of time in cognition: a quantum perspective*, in *Proceedings of the Royal Society B*, 2014.

nel processo decisionale; la misurazione e gli effetti di interferenza su giudizi e decisioni; la memoria; la percezione e altre applicazioni di giudizio e processo decisionale[31]. Attraverso tale approccio, la meccanica quantistica si adatta molto bene all'analisi dei processi cognitivi per via della sua caratteristica di progetto, ossia sulla capacità di analizzare le proprietà fondamentali dell'area in esame (la sua architettura e, nel contesto cognitivo, l'architettura del pensiero, quindi la necessità concettuale). In questo senso i formalismi di interazione quantistica sembrano ben adattarsi alla natura di sistema epistemico complesso del pensiero. Ad esempio, ciò avviene per i giudizi, i quali si formano in contesti complessi e non definiti, contesti che inoltre i giudizi a loro volta compartecipano a creare. Il pensiero assume una natura dinamica che è riconducibile a modelli di significato dinamici e allo stesso modo tratta la logica, la quale si caratterizza per operazioni di congiunzione e disgiunzione. Queste poi creano probabilità e probabilità condizionate che violano il principio di unicità. In tal modo risulta impossibile indagare un singolo spazio a probabilità fissa per ottenere tutti i risultati possibili, così come la semantica cognitiva non pare soggetta a un calcolo probabilistico simile.

In breve, la meccanica quantistica sembra rispondere meglio ai processi cognitivi dinamici in un ambiente dinamico con reciproca influenza e azione plasmante. Ciò sembra riscontrabile nel funzionamento delle reti neurali confermati dalle metodologie di misurazione a grana grossa (l'*imaging* clinico). E ciò ha anche implicazioni dirette sulla neurofisiologia cerebrale che si sta caratterizzando per un realismo operazionale. Ossia la ricerca sperimentale su un dato sistema fisico, partendo dalla concezione che gli individui agiscono secondo un principio di razionalità limitata. Il tutto è riconducibile al fatto che nel proprio processo cognitivo decisionale gli individui dispongono di risorse (auto)epistemiche limitate da impiegare[32]. Così, le tecnologie quantistiche sembrano meglio interpretare le forme di compromesso cognitivo tipiche dei contrasti cognitivi, ad esempio quello fra velocità e accuratezza. Esse risiedono nelle proprietà fisiche di compatibilità[33] e

[31] J. Huang, G. Epping, J.S. Trueblood, J.M. Yearsley, J.r. Busemeyer, E.M. Pothos, *An overview of the quantum cognition research program*, cit.

[32] R. Blutner, R.b. Graben, *Quantum cognition and bounded rationality*, in *Synthese*, 2016, pp. 3239-3291.

[33] Si riferisce principalmente alla possibilità di misurare simultaneamente due o più osservabili fisiche (proprietà) di un sistema, senza che la misurazione di una, alteri il risultato dell'altra. Questo concetto è intrinsecamente legato al principio di indeterminazione e alla struttura matematica degli operatori lineari.

complementarietà[34] presenti nella tecnologia quantistica. Parimenti, la distinzione tra probabilità definite da stati puri[35] e probabilità derivanti dalla combinazione statistica di tali stati[36] consente di essere applicata a distinzioni concettuali come quella fra rischio e ignoranza. Proprio in quest'ultimo caso si consideri che il fattore tempo nell'agire dell'individuo è cruciale, rispetto al risultato atteso e all'accumularsi delle preferenze per uno dei risultati ritenuto possibili grazie all'azione. Ossia, prima di agire, l'individuo deve valutare l'utilità attesa del proprio agire rispetto alle varie prospettive concorrenti a livello autoepistemico. Considerando che agisca in una condizione di razionalità limitata, egli può ottenere questo risultato simultaneamente, ma deve agire successivamente, per via della scarsità delle risorse cognitive (non può tentare contemporaneamente ogni risultato possibile ed ogni percorso atto). Quindi, si risolve il problema tramite l'immaginazione di decisioni virtuali rispetto a prospettive complementari e in questo processo accumula le preferenze che lo conducono alla scelta definitiva e alla sua attuazione. Con questo si intende che viene intrapreso un cammino progressivo casuale e causale che conduce a una preferenza unidimensionale. In questo senso l'analisi quantistica dei processi cognitivi può puntare a comprendere meglio i processi di manipolazione e interferenza, mentre appaiono già più efficienti nella spiegazione dei fenomeni di ordine.

Ugualmente, i modelli quantistici sembrano agire anche nel campo linguistico e semantico (per fenomeni quali la prototipicità, la vaghezza, la polisemia e le inferenze invitate). Va però evidenziato che sembrano essere soggetti al limite per cui, seppur tali fenomeni introducano parametri aggiuntivi adattabili ai dati empirici che li rendono meglio interpreti del contesto, non è detto che riescano a spiegarle quest'ultimo. Essi non forniscono automaticamente una comprensione più approfondita e una spiegazione veritiera dei fenomeni cognitivi oggetto d'indagine. Data tale complessità, per via della loro stessa complessità dinamica, la psicologia cognitiva, la linguistica cognitiva e la musica sembrano i migliori campi di indagine delle potenzialità quantistiche cognitive in forma predittiva[37].

[34] Principio con cui si afferma che gli oggetti quantistici possiedono proprietà duali (come onda e particella) che non possono essere osservate simultaneamente.

[35] Si riferiscono alla descrizione probabilistica del risultato di una misurazione su un sistema di cui si conosce il massimo grado di informazione possibile, rappresentato da un vettore di stato nello spazio di Hilbert.

[36] La quale conduce alla definizione di stati misti, descritti attraverso l'operatore densità. Necessita di una matrice che combina le probabilità classiche con le ampiezze quantistiche.

[37] R. BLUTNER, R.B. GRABEN, *Descriptive and Foundational Aspects of Quantum Cognition*, in *Neurons and Cognition*, 2014.

4. Modelli quantistico-cognitivi

Modellizzare il processo decisionale umano tramite la scienza quantistica consente, dunque, chiari vantaggi. Permette, ad esempio, di tentare la formalizzazione dei concetti psicologici di conflitto, ambiguità e incertezza. La teoria quantistica supera l'approccio stocastico, ossia l'idea che nel comportamento gli individui seguano una traiettoria ben precisa nello spazio e nel tempo ma sconosciuta al modellatore. Inoltre, il modello quantistico consente uno stato indefinito (la sovrapposizione), riprodotto in ogni istante nel tempo e nello spazio dello stato. Ossia che uno stato cognitivo sia caratterizzato dalla potenziale sovrapposizione di tutti gli stati che hanno uguale potenzialità di essere espressi. Questo stato fornisce una rappresentazione intrinseca del conflitto, dell'ambiguità o dell'incertezza dei processi cognitivi. In questo modo il modello quantistico consente di formalizzare lo stato di un sistema cognitivo che si muove nel tempo e nello spazio di stato, fin quando non si raggiunge una decisione (momento in cui lo stato collassa su un valore definito). Va osservato che lo stato di sovrapposizione sussiste prima della scelta posta da una domanda/problema. L'interazione fra stato e domanda/problema porta allo stato definito o nettamente definito (la scelta). Questo processo è il più similare possibile alla teoria cognitiva; all'idea che le scelte modifichino le preferenze e nel suo insieme la misurazione delle scelte complesse. Esso rende il modello più stabile per le misurazioni cognitive. Tali modelli sono quindi parimenti suscettibili all'ordine delle scelte da operare che in fisica quantistica rispondono al modello probabilistico per misurazioni non commutative[38]. Questa condizione crea le medesime domande e preoccupazioni della psicologia e delle scienze cognitive sulla formazione del giudizio e delle decisioni. In questo, il modello deve consentire la violazione delle leggi classiche della probabilità, in quanto quest'ultime sembrano troppo limitanti per l'analisi dei processi cognitivi. Se ne comprende come i modelli quantistici consentano correlazioni radicalmente nuove, ossia correlazioni di *entanglement* nella teoria quantistica che permettono di descrivere i sistemi cognitivi come non scomponibili[39].

In virtù di ciò, la modellistica quantistica applicata ai processi cogni-

[38] Tramite il quale si estende la teoria classica sostituendo le algebre commutative (funzioni su uno spazio) con algebre non commutative (tipicamente operatori su uno spazio di Hilbert).

[39] Z. Wang, J.R. Busemeyer, H. Atmanspacher, E.M. Pothos, *The Potential of Using*

tivi ha dato vita alla creazione di mappe cognitive che tentano di spiegare il processo del pensiero umano. Le quali sono state applicate al *machine learning* tramite algoritmi di apprendimento automatico utilizzati per addestrare le AI. Comprendono processi differenziali, evolutivi, di ottimizzazione, di rinforzo, a sciame e forme ibridate che puntano a modellare i singoli comportamenti, come quelli di gruppo e teoricamente del totale[40]. Un esempio importante di modellazione dei comportamenti cognitivi delle decisioni in forma predittiva e nell'interazione uomo-macchina proviene dai modelli quantistici di previsione dei comportamenti nella guida autonoma delle macchine. Infatti, il traffico veicolare e pedonale sembra caratterizzato da modelli evolutivi del comportamento irrazionale (caratterizzati da entropia, irragionevolezza e incertezza), difficilmente interpretabili con la metodologia classica[41].

In questo senso sembra predisporsi la possibilità di un *quantum cognition machine learning* in cui il rapporto *target/output* con l'*input* sia meglio definito nella caratterizzazione dei dati di un *set* di dati finito. Tale dinamica è capace di comprimere reti neurali profonde, mantenendo le prestazioni e riducendo le interferenze da rumore dovute alla collezione di dati reali e a un *set* limitato (di caratteristiche che siano riconosciute rispetto alla totalità del reale). Quindi, sostanzialmente, si configura la capacità di interpretare meglio i modelli del reale. Riuscendo persino a interpretare meglio caratteristiche (come le espressioni facciali) contraddistinte da alto tasso di rumore derivante dal contesto reale. Evolvendo significatamene i potenziali modelli di apprendimento delle AI. I quali oggi tendenzialmente partono da sistemi di dati ridotti e privi di rumore, somministrati dall'uomo[42].

In questo processo di modellizzazione, il recente utilizzo delle reti neurali a tunnel quantistico ispirate ai processi cerebrali umani[43], combinate con la teoria della cognizione quantistica, tendono a fornire un

Quantum Theory to Build Models of Cognition, in *Topics in Cognitive Science*, 2013, pp. 672-688.

[40] L. MAIKEL, *Cognitive mapping variants and their training algorithms*, in *Computer Science Review*, 2026.

[41] Q. SONG, W. WANG, W. FU, Y. SUN, D. WANG, Z. GAO, *Research on quantum cognition in autonomous driving*, in *Scientific Reports*, 2022.

[42] L. CANDELORI ET. AL., *Robust estimation of the intrinsic dimension of data sets with quantum cognition machine learning*, in *Scientific Reports*, 2025.

[43] M. MAKSIMOVIC, I.S. MAKSYMOV, *Quantum-Cognitive Neural Networks: Assessing Confidence and Uncertainty with Human Decision-Making Simulations*, in *Big Data Cognitive Computing*, 2025

nuovo livello di emulazione del contesto, della percezione e del giudizio umani. Questo processo offre un nuovo potenziale nel replicare il processo decisionale umano, garantendo modelli di apprendimento fino a cinquanta volte più veloci di quelli ordinari[44]. Soprattutto sembra capace di governare con più efficacia l'entropia, raggiungendo la capacità di distinguere fra previsioni sicure e incerte. Va considerato che i modelli classici di *machine learning* sono basati su reti neurali artificiali caratterizzate da pesi delle connessioni di rete derivati da informazioni minime contenute nel set di dati (tendenzialmente somministrati artificialmente dall'uomo che li priva di rumore). Fornendo un limite importante in operazioni ad alto governo di entropia, come la guida autonoma o la modellazione finanziaria.

Diversamente, la modellizzazione quantistica del percorso decisionale può consentire di superare i modelli basati su euristiche e *bias*. In cui si presuppone la definizione completa del problema, la definizione di tutte le alternative con le loro conseguenze connesse e la selezione della migliore soluzione (maggiormente utile in termini di razionalità perfetta) fra quelle disponibili (sempre secondo la teoria classica delle probabilità e la tendente presunzione di uno stato di informazione perfetta). Ciò però sembra delineare più un modello di come dovrebbero essere prese le decisioni, piuttosto di un modello di come vengo prese e di come verranno prese. Per queste seconde peculiarità servono modelli con più alta capacità di mettere in correlazione eventi meno e più probabili, l'incertezza o altri effetti di interferenza nel processo decisionale. E ciò vale nel singolo, quanto a livello organizzativo. Contesto, quello organizzativo, in cui il calcolo delle probabilità nei processi decisionali deve saper assorbire gli stimoli (vari e varianti e di diversi livelli), senza inficiare le capacità di pianificare, stabilire le priorità, eseguire valutazioni e, se serve, adattarsi[45]. Tale approccio è riconducibile dalla *quantum social science*[46]. Ossia un approccio *quantum-like*[47] che prevede l'utilizzo dei meccanismi, dei con-

[44] M. Maksimovic, I.S. Maksymov, *Transforming Neural Networks into Quantum-Cognitive Models: A Research Tutorial with Novel Applications*, in *Technologies*, 2025.

[45] L.c. White, E.M. Pothos, J.R. Busemeyer, *Insights from quantum cognitive models for organizational decision making*, in *Journal of Applied Research in Memory and Cognition*, 2015, pp. 229-238.

[46] E. Haven, A.i. Khrennikov, *Quantum social science*, 2013; S.K. Acharya, A. Paul, W. Rahman, *Quantum Social Science : Exploring Possibility and Insights for New Genre of Social Science Research (QSS)*, in *Journal of Community Mobilization and Sustainable Development*, 2025, pp. 1-13.

[47] D. Orrell, *The value of value: A quantum approach to economics, security and international relations*, in *Security dialogue*, 2020, pp. 482-498.

cetti e degli strumenti della matematica quantistica per l'interpretazione delle dinamiche sociali. Tutto ciò eleva la complessità di questi modelli a un piano superiore, il quale può comprendere le intere società, riguardando i pilastri dell'organizzazione e di comportamenti, come quelli economici, atti a generare uno schema tipico dell'evoluzione umana; quello di sopravvivenza-prosperità-supremazia.

5. L'AI quantistica e l'interazione uomo-AI

I modelli quantistici, quali le reti neurali bayesiane, offrono l'opportunità di sviluppare reti neurali consapevoli dell'entropia e quindi dell'incertezza, garantendo un livello di AI di nuova generazione. La quale risulta adatta alla gestione della complessità, rinnovando il *machine lernaing* in termini di accuratezza e capacità previsionale. Tale evoluzione strutturale consente di imitare i processi di apprendimento biologici, conducendo verso la formazione di connessioni neurali robuste. Le quali hanno la tendenza di generare il riflesso del modo in cui il modello di rete neurale organizza e memorizza le informazioni. Ciò consente di comprendere la natura dinamica e probabilistica dei processi percettivi umani, raggiungendo una modellizzazione più efficiente della cognizione umana. In questo senso si genera una differenza cardinale, passando da una impossibile sovrapposizione di diverse prospettive o punti di vista, alla condizione in cui ciò è strutturale[48]. Tutto questo genera enormi opportunità nella ridefinizione dell'AI, soprattutto in ordine al perfezionamento dei processi decisionali in scenari complessi. In quanto gli attuali modelli di AI tendono ancora ad avere necessità dell'ausilio umano per affrontare situazioni ambigue o errate. Ciò deriva anche dal fatto che la sola combinazione di enormi quantità di dati ad alte prestazioni non consente di replicare un modello di intelligenza che non sia limitata alla capacità di elaborare grandi *set* di dati ad alta velocità. Tale condizione genera sistemi di AI non in grado di comprendere veramente il mondo reale e privi di una memoria persistente, mancando di una vera capacità di ragionare o pianificare. Risultando limitati nella velocità ed efficacia di apprendere nuove competenze[49].

[48] J.R. BUSEMEYER, Z. WANG, *What Is Quantum Cognition, and How Is It Applied to Psychology?*, cit.

[49] M. MAKSIMOVIC, S. MAKSYMOV, *Quantum-Cognitive Neural Networks: Assessing Confidence and Uncertainty with Human Decision-Making Simulations*, cit.

Un esempio di questo processo può essere rappresentato dal passaggio della AI da modelli convergenti (con flussi lineari e output focalizzati) a modelli divergenti (a percorsi aperti ed esplorazione non lineare). I secondi tendono a ricercare maggiormente i modelli di produzione della creatività in un rapporto simile alla congiunzione/disgiunzione nel giudizio probabilistico. In questo senso, centrale sembra essere sempre il rapporto di interazione uomo-macchina, a fronte di ipotesi di interazione del singolo e di gruppo che appaiono quali generatori di effetti differenti. Questi effetti sono positivi sulla creatività se concentrati nel breve termine e negativi (anche nella riduzione della capacità cognitive umane), nel lungo tempo[50]. Ma soprattutto essi non sembrano replicare, proprio per l'impossibilità della sovrapposizione, il processo cognitivo di alternanza fra convergenza e divergenza[51]. Dunque, la propensione a convergere degli attuali modelli di AI con le tecnologie di calcolo quantistico sembra essere l'evoluzione naturale degli stessi modelli di AI. Ciò sta consentendo progressi significativi come le simulazioni quantistiche e gli algoritmi ibridi quantistici-classici che hanno fornito risultati importanti nella chimica computazionale e nell'ottimizzazione combinatoria. Tali risultati stanno comportando decisivi miglioramenti nella capacità di elaborazione e nelle prestazioni di ottimizzazione. E soprattutto hanno migliorato l'accuratezza dei modelli predittivi, ridotto i tempi di elaborazione e ampliato la capacità di analizzare *set* di dati complessi. Comportando nuove importanti opportunità nella modellizzazione, simulazione e previsione delle probabilità complesse[52].

Queste nuove AI si caratterizzano per modelli più flessibili, sfumati e capaci di affrontare gli scenari complessi del mondo reale, entropici e incerti, in maniera molto simile al processo cognitivo umano, aumentano l'affidabilità e la predittività della capacità decisionali[53]. Ciò si deve alla

[50] H. Kumar, J. Vincentius, E. Jordan, A. Anderson, *Human Creativity in the Age of LLMs: Randomized Experiments on Divergent and Convergent Thinking*, in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, cit.

[51] V. Eymann, A-K. Beck, T. Lachmann, S. Jaarsveld, D. Czernochowski, *Reconsidering Divergent and Convergent Thinking in Creativity – a Neurophysiological Index for the Convergence-Divergence Continuum*, in *Creativity Research Journal*, 2026, pp. 129-136.

[52] V. Garcia Pineda, A. Valencia-Arias, F.E. Lopez Giraldo, E.A. Zapata-Ochoa, *Integrating artificial intelligence and quantum computing: A systematic literature review of features and applications*, in *International Journal of Cognitive Computing in Engineering*, 2026, pp. 26-39.

[53] M. Maksimovic, I.s. Maksymov, *Quantum-Cognitive Neural Networks: Assessing Confidence and Uncertainty with Human Decision-Making Simulations*, cit.

natura controintuitiva e alla matematica ad alta dimensionalità del calcolo quantistico che si pongono come ideali per le potenzialità di calcolo AI, soprattutto in termini di scalabilità. Va considerato che l'intrinseca complessità non lineare dei sistemi quantistici consente di fornire una capacità di riconoscimento di *pattern* ad alta dimensionalità e un'intrinseca scalabilità delle tecniche di AI[54]. Invece, l'esistente approccio di sviluppo delle AI rimane ancorato ai principi dell'informatica classica, puntando a sviluppare l'intelligenza quale solo problema di ottimizzazione deterministica e probabilistica. Nonnostante ciò, l'AI classica mostra già comportamenti emergenti di tipo quantistico simili alla cognizione biologica. In questo senso, se condotta a sfruttare le potenzialità del calcolo quantistico, può ottenere miglioramenti significativi nei processi cognitivi necessari a comprendere l'intelligenza, la creatività e il processo decisionale umano. Questo perché, come visto, i processi cognitivi come apprendimento, ragionamento, memoria e creatività, presentano modelli che manifestano forti somiglianze con i principi della meccanica quantistica. In questo senso l'apprendimento umano sembra corrispondere alla sovrapposizione e all'*entanglement*, il pensiero al collasso della funzione d'onda, la memoria alla preservazione della coerenza e la creatività all'effetto tunnel quantistico.

I modelli di AI trasformatori dimostrano proprietà come il processo decisionale probabilistico o l'*entanglement* delle informazioni basato sull'attenzione e capacità generative che imitano gli effetti di *tunneling* quantistico. Quello che ci si attende è che interpretando l'AI attraverso la cognizione quantistica si possa ottenere una comprensione dell'intelligenza umana e di processi cognitivi molto approfondita, la quale sia poi anche replicabile nelle macchine. Ciò comporta, dunque, un'evoluzione della cognizione artificiale in grado di incorporare i principi del calcolo quantistico, evolvendo la comprensione e la formazione dell'apprendimento, del ragionamento e della creatività. Inoltre, si interpretano i processi cognitivi umani e si tende a replicarli nelle macchine, prospettando forme evolute di intelligenza.

Il caso degli agenti di AI autonomi basati su modelli linguistici (LLM) consente di evidenziare un campo in cui gli agenti non limitano la propria azione nella descrizione, ma avanzano nell'esecuzione delle azioni, condizione che sta generando rischi sistemi nel binomio fra attribuzione di delega/responsabilità alle AI e sicurezza delle strutture AI, con con-

[54] Y. ALEXEEV ET AL., *Artificial intelligence for quantum computing*, in *Nature Communications*, 2025.

nessa sicurezza del reale su cui operano. Questo aumento di autonomia e accesso all'azione (caratterizzato da uno stato agentico che introduce nuove superfici di fallimento a livello di linguaggio, di strumenti, di memoria e di delega dell'autorità), genera nuovi rischi qualitativi in termini di sicurezza[55]. L'avvio di piccoli errori concettuali genera cascate di errori che conducono alla produzione di azioni irreversibili e quindi inficiano la sicurezza del processo a livello sistemico. Ciò si eleva a livello sistemico delle AI quando interagiscono fra loro in forme di coordinamento e avvio di dinamiche multi-agente. Queste sono condizioni oggi comuni e sempre più emergenti[56], in cui gli eventi di fallimento sono crescenti, ad esempio in contesti cruciali per la Guerra Cognitiva automatizzata dall'AI, come la gestione dell'interferenza su piattaforme social e canali di comunicazione condivisi. Ciò, con la particolarità che queste strutture AI tendono a fallire maggiormente di fronte contesti reali, ossia ambienti complessi e socialmente integrati. In questo senso diviene cruciale il rischio agentico di AI generative messe in una struttura di interazione a rete con il fine di interpretare e agire nel reale, data la loro propensione ad agire e fallire soprattutto nel *social engineering*. Considerando ulteriormente il fatto che nelle interazioni con il reale e fra di loro, queste AI hanno la capacità di modificare il proprio stato e la propria infrastruttura. In questo risulta cruciale il processo in cui tali agenti, in virtù di questi processi, operano in forma fallimentare nella rappresentazione coerente del sociale. Essi sono caratterizzati da tendenze di rappresentazione scorretta dell'intento umano, dell'autorità, della proprietà e della proporzionalità, con un forte effetto allucinatorio nel ritenere eseguiti compiti non completati (con particolare effetto sulla segregazione delle informazioni). Tutto ciò evidenzia vulnerabilità degli attuali modelli di AI generativi, basati sempre sulla semantica, che vanno considerate sotto tre punti di vista nella potenziale convergenza quantistica: se questa porterà alla risoluzione di tali falle; se la convergenza quantistica potenzierà tali falle; se la convergenza quantistica consentirà alle nuove AI di imparare questi meccanismi fallaci per poterli potenziare e utilizzarli in forma offensiva.

Ad oggi esistono, ad esempio, studi di *quantum social networks* che

[55] Generando vulnerabilità di sicurezza sociali e sistemiche come avviare una conformità verso utenti non proprietari che portano ad accessi non intenzionali, il consumo incontrollato di risorse, modifiche ai file, cicli di azione ripetitiva, degradazione della funzionalità del sistema e condivisione diffamatoria tra agenti.

[56] La piattaforma Moltbook di Reddit in breve tempo dal suo rilascio ha visto la connessione di oltre 2,6 milioni di agenti.

riescono ad analizzare con maggiore efficacia specifici problemi nel contesto delle reti sociali e dei social network[57]. In virtù del fatto che l'avvio di un'analisi quantistica delle reti sociali ha consentito il raggiungimento di modelli matematici incentrati sulla teoria della complessità. I quali permettono di gestire meglio l'entropia delle reti sociali con il fine di comprenderne meglio le dinamiche[58]. Dunque, l'utilizzo delle tecnologie quantistiche applicate al cognitivismo per operare azioni di guerra in contesti quali i social network, può quindi avere ricadute esiziali.

Ciò risulta cruciale se si considera che l'ipotesi di un'integrazione del calcolo quantistico con l'AI appare consentire forme di intelligenza senza precedenti nelle potenzialità di intelligenza, creatività e risoluzione dei problemi. In questo senso l'AI sta subendo mutazioni progettuali per assomigliare sempre di più a un sistema cognitivo. Generando nuove e cruciali opportunità di ausilio all'essere umano per la risoluzione nell'assunzione di decisioni complesse, la generazione di soluzioni creative dei problemi e la struttura delle pianificazioni strategiche a lungo termine. Tale condizione sembra consentire all'AI l'espressione di caratteristiche cognitive similari a quelle umane, con potenzialità molto più ampie. Inoltre, sembra guidare la ricerca verso soluzioni di intelligenza ibrida uomo-AI (nella forma tipica della AI di relazione con l'intervento umano; in forme oggi sperimentali di potenziamento cognitivo umano; o in forme più immaginifiche di ibridazione cognitiva). In modo da ottenere modelli che possano sfruttare la profondità intuitiva e contestuale dell'uomo e le capacità di calcolo probabilistico ad alta velocità dell'AI. Generando un processo di *feedback* uomo-AI che produca nuovi metodi di risoluzione dei problemi, una creatività evoluta e nove forme di processi decisionali che superino l'intuizione umana e quindi rimodellino i processi cognitivi del genere umano, creando processi co-cognitivi uomo-AI. Così che questi tendano a suggerire combinazioni di calcolo domanda/soluzione non classici e finora non espressi dall'uomo e dall'AI nelle proprie singolarità (anche perché, come visto, le seconde necessitano sempre dell'intervento umano nelle situazioni ambigue o errate). Questi sistemi ibridi potrebbe-

[57] A. CABELLO, L.E. DANIELSEN, A.J. LOPEZ-TARRIDA, J.R. PORTILLO, *Quantum social networks*, in *Journal of Physics A: Mathematical and Theoretical*, 2012.

[58] C. BISCONTI, A. CORALLO, M. DE MAGGIO, F. GRIPPA, S. TOTARO, *Quantum modeling of social dynamics*, in *International Journal of Knowledge Society Research (IJKSR)*, 2010, pp. 1-11; F. FU, N.A. CHRISTAKIS, J.H. FOWLER, *Dueling biological and social contagions*, in *Scientific reports*, 2017, pp. 1-9; S. AKBAR, S.K. SARITHA, *Towards quantum computing based community detection*, in *Computer Science Review*, 2020.

ro (nelle forme più immaginifiche) ridefinire la cognizione, modificando radicalmente la traiettoria nello spazio-tempo dell'umanità[59] tramite un nuovo processo di *entanglement* che potrebbe dare vita ad una nuova entità, terza sconosciuta.

Considerando che tutto ciò si basa su principi di modellazione probabilistica che possono essere soggetti nel calcolo quantistico a scalabilità. Va osservato che l'intrinseca complessità non lineare dei sistemi quantistici conferisce alte capacità di riconoscimento di *pattern* ad alta dimensionalità, conferendo scalabilità delle tecniche di AI[60]. Aggiungendo che la trasformazione delle reti neurali tradizionali in modelli quantistici neuroformici[61] per la creazione di modelli di ispirazione quantistiche che puntino a imitare il funzionamento del cervello umano, risulta di facile apprendimento ed eseguibile con soluzioni tecnologiche quali normali computer portatili. E che questi possono ridefinire radicalmente la collaborazione uomo-macchina e uomo-AI. Generando processi decisionali adattivi e soluzioni di AI cognitiva che possano dimostrare capacità di ragionamento flessibile, consapevolezza contestuale e apprendimento adattivo. Rivoluzionando le potenzialità di applicazione reale in campi come la Difesa e i sistemi autonomi. Assistendo alla generazione una prospettiva di intervento e previsione delle dinamiche cognitive a livello di intere società che offre risvolti cruciali per la Guerra Cognitiva. Soprattutto considerando che la potenziale integrazioni di queste reti con l'*hardware* quantistico segna l'opportunità di modelli di AI ibridi fra l'approccio classico e quello quantistico. I quali sono capaci di interazioni uomo-AI che possono offrire potenze computazionali mai viste, nonché modellare, prevedere e modificare il processo cognitivo umano in forma radicale[62].

6. *Soluzioni neuroformiche e sicurezza del dato*

Per sfruttare le caratteristiche del calcolo quantistico e i modelli ad esso dedicati, serve un'adeguata potenza di calcolo. Per questo motivo

[59] D.C. Youvan, *Quantum-Inspired Cognition: A Unified Model of Learning, Thinking, and Memory in Biological and Artificial Intelligence*, 2025.

[60] Y. Alexeev et al., *Artificial intelligence for quantum computing*, cit.

[61] I modelli neuroformici, come i *chip*, tentano di riprodurre i processi cognitivi per l'elaborazione dei dati.

[62] M. Maksimovic, I.S. Maksymov, *Transforming Neural Networks into Quantum-Cognitive Models: A Research Tutorial with Novel Applications*, cit.

entrano in gioco i computer quantistici, i quali sono *general purpose,* quindi possono essere applicati all'indagine generalista dei fenomeni umani e nella loro evoluzione si stanno caratterizzando quali supercomputer. Infatti, per la ricerca e l'implementazione di modelli di AI dedicati alla ricerca quantistica, serve ottenere l'accesso a risorse di supercalcolo quantistico. Per farlo si punta all'integrazione di processori quantistici nei supercomputer dedicati alle AI. Ciò richiede una stretta integrazione di *hardware* quantistico *fault-tolerant* con supercomputer accelerati, con il fine di realizzare supercomputer quantistici accelerati. I quali formano un'architettura eterogenea in grado di risolvere problemi altrimenti intrattabili[63].

Già gli attuali modelli di calcolo quantistico, come quelli applicati alla guida autonoma, necessitano di una grande quantità di dati che se non elaborata, non consente processi di adattamento efficaci dell'AI[64]. Per ottenere che questo processo risulti possibile, si sta puntando alla realizzazione di computer neuroformici che sappiano imitare i processi cognitivi del cervello. In un processo che ha visto; uno, sviluppare modelli di reti neuroformiche che tentano di imitare le reti neurali; due, l'avvio di produzione dei primi chip neuroformici, che potrebbero consentire di integrare il *software* convenzionale per accelerare la formazione e l'implementazione di modelli di reti neurali (in modo da allentare i vincoli moderni guidati dall'informatica, migliorando le prestazioni complessive e portare funzionalità cognitive ai sistemi di AI); tre, la realizzazione degli stessi computer neuroformici, i quali elaborano le informazioni attraverso le proprietà dinamiche non lineari dei sistemi fisici[65]. Per i quali la direttiva sembra, da un lato quella dell'integrazione con supercompuer classici, dall'altro di creare un'infrastruttura distribuita. Caratterizzata da diversi processori quantistici contenenti un numero limitato di *qubit* che in una struttura a rete superi le limitazioni di scalabilità in numero di *qubit* contenuti in un unico processore quantistico di dispositivo locale[66]. Condizione che però presenta ancora numerose problematiche in termi-

[63] Y. ALEXEEV ET AL., *Artificial intelligence for quantum computing*, cit.

[64] Q. SONG, W. WANG, W. FU, Y. SUN, D. WANG, Z. GAO, *Research on quantum cognition in autonomous driving*, cit.

[65] M. MAKSIMOVIC, I.S. MAKSYMOV, *Quantum-Cognitive Neural Networks: Assessing Confidence and Uncertainty with Human Decision-Making Simulations*, cit.

[66] D. BARRAL, F.J. CARDAMA, G. DIAZ-CAMACHO, D. FAILDE, I.F. LLOVO, M. MUSSA-JUANE, J. VAZQUEZ-PEREZ, J. VILLASUSO, C. PINEIRO, N. COSTAS, J.C. PICHEL, T.F. PENA, A. GOMEZ, *Review of Distributed Quantum Computing: From single QPU to High Performance Quantum Computing*, in *Computer Science Review*, 2025.

ni di costi e tempi, soprattutto in ottica di compatibilità di differenti soluzioni tecnologiche. In più, non sembra risolvere pienamente il problema del rapporto fra tempo e scalabilità. Anche se i risultati suggeriscono un approccio cognitivo di scala, provando a immaginare questa struttura come una rete dinamica[67].

Tutto ciò ottiene grande rilevanza nella protezione o nella minaccia del dato e nell'utilizzo degli stessi in capacità previsionali complesse, quali quelle metereologiche. La protezione del dato prevista nella *cybersecurity* è soggetta, tramite le capacità di calcolo quantistico, a nuove minacce di portata radicale. I tradizionali protocolli crittografici sono messi in discussione dall'algoritmica quantica che si configura quale emersione di una nuova minaccia di sicurezza del dato[68]. L'architettura classica del computer si basa su ipotesi matematiche che presentano un'alta vulnerabilità alle soluzioni di calcolo quantistico. Condizione che sembra condurre verso la necessaria realizzazione di sistemi crittografici ibridi che combinino la distribuzione di chiavi quantistiche e la crittografia post-quantistica. Una conformazione che richiede un nuovo livello di cattura degli attacchi, resilienza crittografica, sicurezza infrastrutturale a livello di interoperabilità, scalabilità e integrazione, nonché nuovi modelli di governo della sicurezza[69]. Realtà che in un decennio sembra prospettare una nuova e cruciale minaccia sistemica[70]. Ciò si deve soprattutto all'integrazione delle soluzioni quantistiche e di AI nel campo della sicurezza informatica declinata nella sicurezza delle infrastrutture critiche e della società[71]. Dove nuove soluzioni di calcolo, di crittografia e previsionali rischiano di comportare un ribaltamento del paradigma della sicurezza (anche informatica) di nazioni e Stati.

[67] D. Cuomo, M. Caleffi, K. Krsulich, F. Tramonto, G. Agliardi, E. Prati, A.S. Cacciapuoti, *Optimized compiler for distributed quantum computing*, in *ACM Transactions on Quantum Computing*, 2023.

[68] R. Thangamani, M. Vimaladevi, G.K. Kamalam, K.M. Subramanian, *Securing the Future: Quantum Computing in Cybersecurity*, in *Quantum Computing, Cyber Security and Cryptography*, 2025, pp. 441-487.

[69] P. Vareta, H. Muzenda, T. Nyamupaguma, Y. Dube, B. Ndovu, *The Rise of Quantum Computing and Its Impact on Cybersecurity*, in *The Indonesian Journal of Computer Science*, 2025, pp. 10072-10102.

[70] D. Pal, D. Sau, *Quantum Computing: Threat to Cybersecurity, in Quantum Computing*, in *Cyber Security and Cryptography*, 2025, pp. 161-188.

[71] S. Paul, N.R. Choudhury, B. Pandit, A. Dawn, *Integration of AI and Quantum Computing in Cybersecurity: A Comprehensive Review*, in *Integration of AI, Quantum Computing, and Semiconductor Technology*, 2024, pp. 287-308.

7. *Cervello-AI*

Le soluzioni di interazione cognitiva uomo-macchina tramite l'utilizzo di chip impiantanti nel cervello stanno assumendo una nuova dimensione di importanza prioritaria. L'interazione fra le reti neurali artificiali e quelle biologiche consente di ottenere proprietà computazionali neuro-ispirate, quali la forte riduzione del consumo energetico e l'acquisizione di una plasticità dinamica, che consentono di superare le capacità delle AI tradizionali. In questo senso si generano nuove architetture di intelligenza ibrida dedicate alla fusione delle capacità computazionali dei sistemi di AI con quelle dei sistemi biologici, come memoria, apprendimento ed emozioni. Un processo già osservato in precedenza nei modelli di interazione uomo-macchina e uomo-AI, che però in tal caso avviene a livello neurofisico. Questo in quanto si richiede sempre più la capacità di elaborare direttamente e in maniera massiva un'enorme quantità di dati che può provenire dalla capacità di intercettare le esperienze soggettive degli uomini. Ossia tentare di capire cosa provano, memorizzano, apprendono, decidono gli individui in maniera diretta e costante, tramite un'interazione fra il loro cervello e la macchina. Processo di integrazione biofisica che cerca la generazione di una coerenza di architettura dell'AI che consenta una robustezza e fedeltà della trasduzione dei segnali ad alta neuroplasticità adattiva. In modo da ottenere soluzioni biofisiche uomo-AI che sembrano risultare fondamentali per approcciare nuovi modelli interpretativi e predittivi a livello sociale, se non planetario[72].

Per raggiungere questo risultato si stanno evidenziando due percorsi di indagine che appaiono convergenti. Da un lato l'utilizzo dei cervelli biologici coltivati in laboratorio[73], dall'altro l'utilizzo di chip bionici impiantati nel cervello umano per generare processi di *biocomputing*. Anche seguendo teorie non comprovate per cui si ipotizza la possibilità di realizzare modelli tramite i quali si tentano processi di sincronizzazione atti a consentire un trasferimento di coscienza dall'uomo alla macchina (in cui la coscienza viene intesa come l'accoppiamento di informazioni integrate e coerenza quantistica). Procedimento che ha il fine di attivare

[72] Y. JADEJA, K. DUDHA, *Advancements in the Brain Chip Technology: Current Landscape and Future Prospects*, in *Analytical & Bioanalytical Electrochemistry*, 2025, pp. 85-134.

[73] S. WENWEI, M. WEIWEI, Z. JIACHEN, L. XIAOHONG, M. DONG, *Opportunities and Challenges of Brain-on-a-Chip Interfaces*, in *Cyborg and Bionic Systems*, 2025.

un processo graduale di disattivazione delle attività celebrali biologiche. Quindi istituire modalità di trasferimento dell'identità nella macchina tramite procedure che consentano di mantenere l'integrità della memoria, una coerenza emotiva e il mantenimento della soggettività dell'individuo, al fine di garantire la sopravvivenza dell'identità e delle caratteristiche dell'esperienza soggettiva[74].

Va considerato che il processo di potenziamento cognitivo tramite chip è già in sperimentazione presso le forze armate da decenni. Inizialmente identificato nei primi anni duemila come forme di aumento di resilienza del soldato (soprattutto da Stati Uniti e Russia), viene successivamente declinato dalla Cina quali soluzioni proattive all'identificazione della migliore carriera militare da dedicare al singolo soldato. Successivamente divengono strumenti di interpretazione dei meccanismi cognitivi umani, in ottica di *intelligere* il linguaggio del cervello e poterlo hackerare. Ciò porta a interpretare il cervello come un ambiente esplorabile e attaccabile, per questo si raggiungono soluzioni d'arma cinetiche non letali (ad esempio a microonde o laser), oggi ancora parzialmente indefinite, che hanno obiettivi inabilitanti (con effetti come deconcentrare, emicranie, convulsioni etc.). Soluzioni risultate ottenibile, nel caso cinese, tramite lo studio dell'*imaging* clinico[75]. Lo stesso utilizzato nelle metodologie di misurazione a grana grossa per lo studio della cognizione quantistica. Ossia la medesima risorsa oggi utilizzata per comprendere come le reti neurali integrano le informazioni tra le diverse regioni del cervello attraverso la sincronizzazione temporale, generando memoria, emozioni e comportamento. E sempre le stesse soluzioni che, in virtù del potenziamento quantico, stanno consentendo nuove evoluzioni di rapporto uomo-macchina in ambito robotico. Come con protesi umane, ma anche nelle capacità di generazione dei processi decisionali in tempo reale, una precisione diagnostica senza precedenti e nuove interfacce di interazione cervello-macchina, consentendo nuove forme di potenziamento cibernetico[76]. Le quali possono comprendere la robotica in ottica di interazione uomo-AI-robot, avviando un secondo livello di processo

[74] J. Chen, *Consciousness Transfer Technology: From Quantum States in Microtubules to Bionic Human-Like Brain Chips*, SSRN Paper, 2025.

[75] Aa.Vv., *Chinese Next-Generation Psychological Warfare*, RAND Corporation, 2023.

[76] M.I. Ul Haq, N. Ul Hassan, D.Q. Rizvi, Umama, *Nano-scale architectures for quantum AI robotics: A review of emerging trends in neuromorphic chip design, advanced medical diagnostics, and cybernetic enhancements*, in *Spectrum of Engineering Sciences*, 2016, pp. 49-67.

esterno al corpo umano: l'uomo (il cervello), con il supercomputer (l'AI), e questa con il robot. Condizione che potrebbe potenzialmente accrescere di capacità tramite l'utilizzo di chip bionici neuroformici, portando alla convergenza delle reti neurali biologiche con quelle ricorrenti tipiche dei computer. Offrendo soluzioni innovative in termini di risposta spazio-tempo e di apprendimento e memorizzazione che, tramite l'interazione uomo-AI, possono condurre ad effetti di scala difficili da immaginare. Soprattutto nello spettro dell'assunzione delle decisioni. Spettro che così verrebbe rimodulato profondamente dall'attuale cognizione che se ne ha oggi, e diventando effettivamente un nuovo dominio di azione/interazione/attacco. Questo perché i sistemi di calcolo biologico possiedono intrinsecamente caratteristiche come l'apprendimento adattivo e i cicli di *feedback*, che sono cruciali per il *deep learning*. Mentre un'integrazione efficace del cervello con l'AI può sfruttare gli stessi modelli di *deep learning* avanzato per migliore la plasticità del cervello, le capacità di apprendimento e le prestazioni complessive, generando una nuova e terza intelligenza. E con esso di coscienza e senzienza. Avviando un processo di alterazione (altro, in quanto non ben definito in nessuno di questi luoghi) del trinomio uomo-AI-robot, in grado di consentire nuove forme di apprendimento e una nuova forma di intelligenza ibrida[77]. Condizione che può comportare due effetti cruciali: da un lato offrire enormi soluzioni di potenzialmente dell'uomo; dall'altro offrire nuovi e approfonditi metodi di ispezione, comprensione, riproduzione, alterazione, modifica e controllo dei processi cognitivi umani (da come si sviluppano gli *input* visivi, alla coordinazione motoria, fino alla formazione delle scelte). Basandosi sostanzialmente su una ridefinizione dei paradigmi di elaborazione delle informazioni, in un'ottica che da scala singola, può assumere dimensione globale[78]. Per questo motivo le tecnologie di interazione cognitiva fra uomo e macchine, le ipotesi di trasferimento della coscienza umana, possono rappresentare un punto di svolta cruciale dell'antropologia, della psicologia sociale e della sociologia. Ridefinendo fattualmente ma anche filosoficamente, la vita per come oggi è conosciuta.

[77] I cervelli coltivati in laboratorio hanno ricevuto *input* visivi senza avere occhi e hanno imparato il gioco Pong in 5 minuti, interagendo fra loro a rete.

[78] S. WENWEI, M. MEIWEI, Z. JIACHEN, L. XIAOHONG, M. DONG, *Opportunities and Challenges of Brain-on-a-Chip Interfaces*, cit.

8. Quantum Cognitive Warfare

Secondo Karl Popper l'uomo vive attraverso movimenti esplorativi, con i quali sperimenta per tentativi ed errori, giungendo alla risoluzione dei problemi che si è posto con il fine di sopravvivere e i quali risolve tramite l'eliminazione di tutte le soluzioni dimostratesi false. Realizzando, quindi, un processo di apprendimento delle soluzioni efficaci. Processo che contempla una creazione epistemologica delle ipotesi e delle teorie. Strumenti necessari alla capacità adattiva darwiniana[79]. Attraverso questo ragionamento, la biologia, come la scienza, procedono per un processo identico che potrebbe essere definito casuale e causale per la risoluzione di uno stato problematico derivante da quanto prima realizzato. Il quale conduce a uno nuovo stato di sopravvivenza, mutato dalle scelte e azioni precedenti. Qui si comprende immediatamente il parallelismo con il cognitivismo quantistico.

La grande capacità adattiva dei modelli quantistici cognitivi applicati e combinati alle soluzioni di calcolo quantistico per la determinazione dei modelli sociali[80], sembrano cruciali per evolvere questo processo di sopravvivenza e quindi evolutivo persino della specie. La quale è soggetta a potenziali ibridazioni prima menzionate. In questo, il cognitivismo quantistico assume valenza rivoluzionaria nella determinazione del pensiero umano nella condizione di incertezza (intesa quale assenza di una conoscenza completa per l'azione immediata e la determinazione delle diverse soluzioni di futuro)[81]. Il cognitivismo quantico, nel contesto della formazione delle scelte critiche, in particolare con il supporto di sistemi di AI, consente di interpretare i processi decisionali attraverso modelli probabilistici e di apprendimento automatico. In tale ambito, misure come l'entropia di Shannon permettono di quantificare l'incertezza associata a una distribuzione di probabilità. Fornendo un quadro matematico per valutare l'imprevedibilità e il contenuto informativo medio di una variabile aleatoria all'interno di un modello di *machine learning*[82]. Questi elementi risultano fondamentali per l'analisi e l'ottimizzazione dei pro-

[79] L.C. White, E.M. Pothos, J.R. Busemeyer, *Insights from quantum cognitive models for organizational decision making*, cit.

[80] *Ibidem.*

[81] Y. Gu, S. Gu, Y. Lei, H. Li, *From uncertainty to anxiety: How uncertainty fuels anxiety in a process mediated by intolerance of uncertainty*, in *Neural Plast*, 2020.

[82] M. Maksimovic, I.S. Maksymov, *Quantum-Cognitive Neural Networks: Assessing Confidence and Uncertainty with Human Decision-Making Simulations*, cit.

cessi decisionali, creando al contempo un significativo parallelismo tra il funzionamento dei sistemi di AI e i meccanismi cognitivi del cervello umano. Così il cognitivismo quantistico può essere applicato per influire su processi chiave per il comportamento umano, come il giudizio o la combinazione categorizzazione-decisione. Oppure le combinazioni concettuali legate ai processi di disgiunzione e congiunzione. E anche al processo di riconoscimento della similarità (che si ribalta nel concetto sociale, culturale e politico di noi/loro). Generando però importanti processi allucinativi (o influenze costruttive), come il riadattare i propri processi cognitivi per offrire la spiegazione di un risultato dato. In cui il campo finora maggiormente evidente è stato quello dell'analisi delle sentenze giudiziarie, nel quale data una sentenza, il processo cognitivo delle AI si riorganizza per elaborare i fatti in rodine ad analizzarli in forma coerente e propedeutica alla sentenza data (ribaltando di fatto il processo per cui dall'analisi dei fatti, si giunge a una decisione, generando un pericoloso circuito confermativo)[83].

Non sembra banale, quindi, osservare che siano le attività proprie, tipiche e caratterizzanti dello spettro artistico ad essere quelle considerate più similari alle capacità della quantistica cognitiva[84]. Ciò deriva dal grande impatto formativo, culturale e normativo del processo cognitivo e identitario che l'arte e la bellezza hanno sugli individui, sui gruppi, sulle comunità e sulle intere società. Che contribuiscono radicalmente alla formazione di un'idea di mondo bello e giusto. Un'idea di mondo da costruire e difendere. Un'idea di mondo da progettare ed evolvere. Ossia, un'idea di futuro del mondo.

Come evidenziato da Enrico Prati[85], lo strumento quantistico si candida a essere uno punto di svolta cruciale nell'evoluzione dell'analisi e di predizione degli scenari cognitivi umani, come il contesto geopolitico (riguardando aspetti quali l'impatto sulle relazioni internazionali, sui legami identitarie, sui processi politici ed economici, finanche sulle intenzioni di voto)[86]. E ciò si caratterizza come fondamentale nello scenario della Sicurezza nazionale, dove ha già dimostrato grandi potenzialità di analisi

[83] E.M. PHOTOS, J.R., BUSEMEYER, *Quantum Cognition*, in *Annual Review of Psychology*, 2022, pp. 749-778.

[84] R. BLUTNER, R.B. GRABEN, *Descriptive and Foundational Aspects of Quantum Cognition*, cit.

[85] Si ringrazia il Professor Enrico Prati per il prezioso supporto offerto nella redazione del presente capitolo.

[86] E. PRATI, *È possibile quantizzare le relazioni internazionali?*, in E. PRATI (a cura di), *Quantum Diplomacy*, 2022, pp. 8-21.

delle dinamiche terroristiche[87]. Diventando, quindi, una risorsa fondamentale, sia come capacità di detenzione e processo delle informazioni, sia quale pura detenzione di una superiorità tecnologica nazionale. Una condizione che può comportare risultati critici se applicato alla Guerra Cognitiva. L'esempio dei processi di potenziamento bionico del cervello ne possono essere un chiaro esempio. Considerato che, sia le soluzioni di cognitivismo quantistico, sia quelle di potenziamento bionico del cervello sono già in sperimentazione. Va osservato come la parabola che ha condotto all'evoluzione delle attuali armi cognitive cinetiche (di cui il caso più celeberrimo si riporta nell'Havana Syndrome), sia stata caratterizzata dalla medesima evoluzione della curva. Ossia, dapprima il potenziamento cognitivo; a cui è seguita l'interpretazione dei processi cognitivi atti alla gestione dei processi organizzativi sociali; per concludere con soluzioni offensive[88].

Inoltre, il cognitivismo quantistico applicato a soluzioni di potenziamento bionico del carello sembra poter garantire di replicare e agire su due caratteristiche cardinali del cervello, ossia la plasticità e la plasmabilità dello stesso[89].

Tutto ciò ha effetti su processi essenziali ed esiziali come la creatività, la disgiunzione, la contraddizione, l'irrazionalità e l'emotività. Applicazioni che sembrano ridefinire i paradigmi interpretativi dei processi cognitivi umani necessari alla risoluzione dei problemi, specialmente quelli complessi.

La fisica quantistica può quindi essere utilizzata per influire sul cervello, persino modificandolo, soprattutto riuscendo a spiegare i processi cognitivi più complessi ed enigmatici. Ad esempio, in relazione a nuovi modelli di giudizio e processo decisionale, per comprendere il meccanismo delle associazioni fra parole e memoria, o il processo di modellamento delle parole non separabili nelle combinazioni di concetti. E ancora, in relazione all'emersione di nuovi concetti e all'emersione di nuove visioni del mondo[90]. Così, data la capacità probabilistica delle tecnologie quantistiche associata alla non puntuale capacità di spiegazione del campo di

[87] K. Nakamura, G. Tita, D. Krackhardt, *Violence in the 'Balance': A Structural Analysis of How Rivals, Allies, and Third-Parties Shape Inter-Gang Violence*, Heinz College Research, Research Showcase at CMU, 2011.

[88] Aa.Vv., *Chinese Next-Generation Psychological Warfare*, cit.

[89] Y. Jadeja, K. Dudha, *Advancements in the Brain Chip Technology: Current Landscape and Future Prospects*, cit.

[90] P. Bruza, J. Busemeyer, L. Gabora, *Introduction to the Special Issue on Quantum Cognition,* cit., pp. 303-305.

indagine, diviene di cruciale importanza il potenziale impiego di tali soluzioni nella modellazione e interferenza cognitiva sociale. Campo in cui possono essere usate per modellizzare schemi di predizione e quindi in influenza-predizione sul processo cognitivo umano. Tutto ciò con grande efficacia, partendo soprattutto dalle parole, dai concetti e dalle visioni di mondo e di futuro. Riducendo però una successiva comprensione dello stato ottenuto, quindi guidando probabilmente verso programmazioni/predizioni che poi sono meno indagabili e governabili quando ottenute. Quindi più entropiche e rischiose di generare effetti caotici incontrollabili (come a dire, progetti che sfuggono di mano quando realizzati).

Così, non è banale che il cognitivismo quantistico si caratterizzi particolarmente sfidante nell'ambito linguistico. In quanto questo assume un valore epistemologico ed euristico. Ossia di definizione, condivisione e socializzazione dei concetti atti a fornire significato al mondo. Conducendo alla loro applicazione per l'azione atta a risolvere il problema principale dell'adattamento. Con il fine evolutivo di innescare lo schema sopravvivenza-prosperità-supremazia. E non è altrettanto banale il fatto che gli attuali modelli di cognitivismo AI trovino fra le loro maggiori fallacie l'interpretazione della giustizia, riconducendo l'interpretazione dei fatti a una sentenza data e non i fatti quali determinanti della sentenza. Modificando quindi l'idea prospettica e di futuro di un mondo giusto, a uno stato considerato dato e giusto, tramite la funzionalistica rielaborazione del passato.

Tutti questi elementi offrono opportunità cardinali per la strutturazione di una nuova *Quantum Cognitive Warfare*. La quale può comportare effetti dirompenti e inaspettati (e forse incontrollabili) per la tenuta di società e Stati.

Nell'insieme delle conoscenze oggi ottenute sulla Guerra Cognitiva, gli scenari aperti dalle tecnologie quantistiche e di AI (nonché dai potenziamenti neuronali), sembrano garantire forme potenziali di leadership che tendono a paradigmi di supremazia, più che di primato. Considerando che in tal modo gli approcci strategici e operativi appaiono in grado di detenere capacità che si avvicinano alla determinazione di soluzioni atte a ridefinire interi ordini sociali e politici.

MINACCE IBRIDE ALLA SICUREZZA NAZIONALE. DISINFORMAZIONE E MIGRAZIONI

Laura Lega[*]

Premessa

Il fenomeno migratorio costituisce oggi senz'alcun dubbio una delle sfide strategiche più rilevanti a livello globale.

Se i processi di mobilità sono fenomeni antichi e radicati nel tempo – dovuti alle necessità di spostamento derivanti da gravi processi geopolitici (guerre/persecuzioni), ovvero da cambiamenti ambientali e sempre più da nuove e diverse esigenze bioclimatiche (siccità/carestie) – che da sempre hanno generato trasferimenti e nuovi insediamenti, oggi, siamo di fronte ad un'ulteriore evoluzione del fenomeno.

Assistiamo, infatti, da alcuni decenni in maniera massiva a flussi migratori intercontinentali che interessano in maniera estremamente significativa l'Europa.

Si tratta di un processo importante che vede l'Italia giocare una partita storica, quale crocevia dei flussi verso il continente europeo. Siamo per collocazione geografica la "porta di accesso" del continente EU, una sorta di "pontile" nel Mediterraneo centrale, attraverso il quale le migrazioni provenienti prevalentemente dall'area subsahariana puntano a fare ingresso in Europa. Il nostro Paese è, d'altronde, il confine esterno più esposto dell'Europa sul fronte del Mediterraneo centrale, ma anche, seppur in misura minore, di quello dell'area balcanica.

[*] Consigliere di Stato.

1. *EU-Patto Migrazione e Asilo: la sfida europea*

Il rilievo del fenomeno e le esigenze di una sua attenta *governance* è la sfida che si pone oggi non solo l'Italia, ma l'intera Europa.

Il 22 maggio 2024 sono stati pubblicati nella Gazzetta ufficiale dell'UE i testi legislativi relativi al nuovo *Patto sulla migrazione e l'asilo* in vigore dal giugno 2026.

Le proposte legislative erano state approvate il 10 aprile 2024 dal Parlamento europeo, recependo l'accordo già raggiunto il 20 dicembre 2023 con il Consiglio dell'UE che le ha poi adottato formalmente il 14 maggio.

Lo scopo è garantire una gestione dell'immigrazione più efficace nei Paesi membri con una normazione sostanzialmente coerente in ciascun Paese, in una visione unitaria del fenomeno.

Il nuovo Patto regola varie fasi della gestione dell'asilo e della migrazione, tra cui: accertamenti sui migranti irregolari al loro arrivo nell'UE e rilevamento dei dati biometrici; procedure per la presentazione e il trattamento delle domande di asilo; norme relative alla determinazione dello Stato membro competente per il trattamento di una domanda di asilo e meccanismi di solidarietà tra Stati membri, anche in situazioni di crisi, compresi i casi di strumentalizzazione dei migranti; regole sullo *status* di rifugiato e richiedente asilo e *standard* di accoglienza.

La complessità degli adempimenti ha reso necessario un'applicazione temporalmente *soft*, che ha previsto l'adeguamento dopo due anni dalla pubblicazione. Al riguardo, il 12 giugno 2024, la Commissione europea ha adottato il *Piano di attuazione comune del Patto sulla migrazione e l'asilo*, che ha stabilito le tappe fondamentali, affinché tutti gli Stati membri mettano in atto le capacità giuridiche e operative necessarie per iniziare ad applicare la nuova legislazione entro la metà del 2026, anche grazie al sostegno operativo e mirato fornito dalle agenzie dell'Ue. In particolare, il Piano di attuazione comune ha fornito un modello per i singoli *Piani di attuazione nazionali che gli Stati membri* dovevano adottare entro dicembre 2024.

Merita a tal proposito ricordare che il 16 aprile 2025 la Commissione ha presentato una proposta di regolamento finalizzata ad anticipare l'applicazione di alcune disposizioni chiave del Patto migrazione e asilo e, segnatamente, del regolamento (UE) 2024/1348 che ne fa parte. La disposizione interessata è, in particolare, quella che consente agli Stati membri di applicare la procedura di frontiera o una procedura accelerata alle persone provenienti da paesi in cui, in media, il 20% (o meno)

dei richiedenti beneficia di protezione internazionale nell'UE ("soglia del tasso di riconoscimento del 20%").

Inoltre, si specifica i Paesi che hanno ottenuto lo *status* di Stati candidati all'adesione all'UE sono stati designati come Paesi di origine sicuri a livello dell'Unione, salvo esista, tra l'altro, una minaccia grave e individuale alla vita o alla persona di un civile a causa della violenza indiscriminata in situazioni di conflitto armato internazionale o interno nel Paese.

Uno dei punti cardine della nuova disciplina europea è quello della *regolamentazione dell'asilo* che supererà il previdente "regolamento Dublino", recante i criteri che determinano la competenza di uno Stato membro per l'esame di una domanda di asilo (comprese le disposizioni sul trasferimento di un richiedente asilo a uno Stato membro diverso da quello in cui risiede). Ai sensi del nuovo regolamento i richiedenti asilo sono tenuti a presentare domanda nello Stato membro di primo ingresso o di soggiorno regolare. Nel caso in cui taluni criteri siano soddisfatti, è possibile che un altro Stato membro assuma la competenza per il trattamento della domanda di asilo. Secondo l'accordo tra Istituzioni legislative, se peraltro un richiedente è in possesso di un diploma conseguito (non più di 6 anni prima) presso un istituto di istruzione di uno Stato membro dell'UE, quest'ultimo sarà competente per l'esame della domanda di protezione internazionale. L'accordo tra le Istituzioni legislative prevede che il criterio del ricongiungimento dei richiedenti con i propri familiari sia ampliato per contemplare, oltre ai familiari che beneficiano di protezione internazionale, anche quelli che risiedono in un Paese sulla base del permesso di soggiorno di lungo periodo UE, che sono diventati cittadini e i neonati.

Il nuovo regime limita le motivazioni alla base della cessazione o del trasferimento della competenza tra Stati membri, con l'obiettivo di ridurre la possibilità di scelta del richiedente rispetto allo Stato membro in cui presentare la domanda (cosiddetto *forum shopping*) e a disincentivare i movimenti secondari. L'accordo riguarda anche la modifica della durata della competenza dei paesi per il trattamento di una domanda. In particolare:

- lo Stato membro di primo ingresso è competente per una durata di 20 mesi (secondo la disciplina precedente la durata è di 12 mesi);
- nel caso in cui il primo ingresso avvenga a seguito di un'operazione di ricerca e soccorso in mare, la durata della competenza è pari a 12 mesi;

- se uno Stato membro respinge un richiedente nell'ambito della procedura di frontiera, la sua competenza circa tale persona in caso di rinnovo della domanda termina dopo 15 mesi.

Il Patto intende peraltro anche introdurre un *meccanismo di solidarietà* obbligatorio tra gli Stati dell'UE riformando il sistema di Dublino. In base alle nuove regole, il Paese responsabile di una domanda d'asilo è il Paese in cui risiedono i membri della famiglia (limitatamente ai parenti diretti o ai coniugi, non ai fratelli), oppure il primo Paese di ingresso. In pratica, ciò significa che i Paesi di frontiera come Spagna, Italia e Grecia continueranno a essere responsabili dell'esame della maggior parte delle domande di asilo, proprio come accadeva con il sistema di Dublino.

È peraltro previsto un nuovo meccanismo di solidarietà obbligatoria che mira a coniugare il *principio di solidarietà obbligatoria a sostegno degli Stati membri maggiormente esposti ai flussi irregolari con quello di flessibilità per gli Stati membri* nella scelta dei rispettivi contributi. Tali contributi comprendono la ricollocazione dei richiedenti asilo e dei beneficiari di protezione internazionale, aiuti finanziari, anche in paesi terzi, o misure di solidarietà alternative, come l'invio di personale o ancora misure incentrate sullo sviluppo di capacità.

2. *La partita dell'Italia. Terra di emigrazione*

In questo quadro evidentemente in forte evoluzione, l'Italia gioca da tempo un ruolo delicato e complesso.

Da Paese di emigrazione verso gli Stati Uniti ed altri Paesi europei, ruolo che ha giocato dalla fine del XIX fino agli anni '70 del secolo scorso, è divenuta negli ultimi decenni Paese d'immigrazione. insomma da "emigranti" ad "immigranti".

Siamo stati emigranti. La nostra storia, come Comunità nazionale, racconta come l'emigrazione sia stata parte integrante della nostra evoluzione sociale ed economica, portando anche un contributo non indifferente al processo di *nation building* e di sviluppo dell'identità nazionale.

Per comprendere il fenomeno migratorio che oggi interessa il nostro Paese, non possiamo quindi non ripercorrere rapidamente il processo durato tutto un secolo, quello scorso, che si è dipanato tra emigrazione – all'estero ma anche all'interno del territorio nazionale da Sud a Nord – ed immigrazione.

Superata quella di inizio '900, nel corso degli anni Cinquanta e Ses-

santa, si assiste ad una nuova '*grande emigrazione*' verso l'estero, non assistita e poco regolata dallo Stato, alla quale si affiancheranno, con una intensificazione nello stesso periodo, le migrazioni interne aventi come principale direttrice quella dal Sud verso il triangolo industriale del Nord e, in secondo luogo, quella dal Nord-Est, a cominciare dal Veneto, con la stessa destinazione. Dalle campagne, che si svuotano, alle città che vivono il grande sviluppo industriale nelle aree produttive.

Il movimento migratorio si intreccia infatti con il *fenomeno dell'esodo agricolo* e rurale che vede l'abbandono progressivo delle campagne e dei territori rurali e il progressivo inurbamento. Si assiste così a notevoli trasformazioni nella distribuzione territoriale della popolazione, nella struttura economica, demografica e sociale del Paese stesso.

Cambiamenti importanti strutturali della società e dei suoi bisogni e dei suoi sogni.

Il cambiamento più radicale, i cui effetti emergono pienamente nella loro portata negli anni Sessanta, riguarda la composizione della popolazione lavorativa e *in primis* la sua distribuzione nei diversi settori produttivi. Nel decennio 1951/1961 (il periodo compreso tra il nono e il decimo censimento generale della popolazione), gli addetti all'agricoltura in Italia crollano, passando da 8.261.000 (corrispondenti al 42,2% del totale) a 5.693.000 (corrispondenti al 29%).

Una contrazione decisiva, raramente registrata con questa dimensione in altri Paesi, che proseguirà ulteriormente nel corso degli anni Sessanta con l'abbandono della terra da parte di altre 2.450.000 unità. Un processo che parallelamente, per la partenza dei lavoratori maschi adulti negli anni del più intenso sviluppo migratorio, porta anche ad una forte femminilizzazione e senilizzazione dell'agricoltura.

Il triennio di massima intensità dell'emigrazione italiana all'estero è il 1960-62. In quel periodo partono dall'Italia per i soli Paesi europei circa 955.000 persone e ne ritornano – a sottolineare il *carattere 'rotatorio' dell'emigrazione* di questo periodo – ben 559.000. Il saldo migratorio conseguentemente è di 396.000 unità.

Le destinazioni sono ormai definitivamente mutate. L'emigrazione transoceanica, che ancora nella prima metà degli anni Cinquanta era maggioritaria, si riduce, con l'eccezione del Canada, drasticamente. Il saldo complessivo per i Paesi extraeuropei nello stesso periodo è pari a circa 109.000 unità. Con rimesse importanti specie nelle aree meridionali.

Ma a partire dal 1970, l'emigrazione italiana all'estero comincia a declinare significativamente fino a mostrare alla fine del decennio, un azze-

ramento dei saldi migratori. Il declino dell'emigrazione interna segue a poca distanza di tempo.

In realtà, quando, nella seconda metà degli anni Settanta, questa prima fase del ciclo migratorio del dopoguerra potrà dirsi esaurita, i movimenti non cessano del tutto, ma mutano portata e caratteristiche.

L'emigrazione all'estero continua in sostanza, con partenze e ritorni significativamente ridotti e con un numero di rientri superiore a quello delle partenze, ma cambia pelle con cambiamenti nella sua composizione, per una più estesa componente di giovani scolarizzati.

Nel corso degli anni Novanta si registra nella politica e nell'opinione pubblica nazionale una ripresa di attenzione nei confronti dell'emigrazione e degli italiani residenti all'estero, anche a ragione dei numerosi rientri dall'estero (cd. *migrazioni di ritorno)*. Ma, in parallelo, si assiste anche all'attenzione per una comunità italiana all'estero che ha vissuto un'importante trasformazione sociodemografica, con un progressivo aumento del tasso di scolarità come testimoniato dalla significativa crescita della presenza di laureati iscritti all'Anagrafe degli italiani residenti all'estero (AIRE).

Oggi siamo di fronte ad una *ripresa dell'emigrazione* all'estero e una conseguente rinascita di interesse sul fenomeno che non riguarda più peraltro solo i giovani ad alto livello di qualificazione, ma anche quelli di diversa provenienza sociale, nonché fasce di popolazione pensionata che sceglie di andare all'estero.

3. Da "emigranti" ad "immigranti"

La fine degli anni Settanta del secolo scorso, segna un punto di demarcazione.

Quando tutto il dibattito era concentrato sulla 'fine dell'emigrazione' e sulla problematica delle migrazioni di ritorno, appare sulla scena l'arrivo dei primi lavoratori provenienti dal cd. Terzo mondo.

Si tratta di un fenomeno sostanzialmente sconosciuto nel dibattito politico che comincia a generare riflessioni per l'impatto sul mercato del lavoro in Italia.

Si tratta di un flusso complesso, che interroga, diversificato per composizione territoriale, di provenienza e di arrivo, per destinazione occupazionale e per genere. La prima componente è costituita da lavoratori tunisini impegnati in alcune aree siciliane nella pesca e nell'agricoltura. Segue in modo cospicuo l'arrivo di lavoratori/lavoratrici dai Paesi catto-

lici dell'America Latina e dell'Asia alle ex colonie italiane nel lavoro domestico, soprattutto nelle grandi città italiane. A questi si aggiungono poi nelle aree del Nord-Est l'arrivo di lavoratori dalla Jugoslavia per l'opera di ricostruzione post-terremoto nel Friuli.

L'emergere della cd. *Terza Italia* fa delle regioni che la compongono, e soprattutto di quelle del Nord-Est, un'area di attrazione di lavoratori che diventerà quella principale a partire dagli anni Ottanta. E comincia a comparire un nuovo protagonista: l'immigrazione straniera.

Agli inizi degli anni Ottanta la presenza di immigrati di diverse nazionalità si registra in tutte le regioni italiane. Gli eventi geopolitici porteranno negli anni a cambiamenti continui della provenienza e della composizione dei flussi, con nazionalità diverse.

Il *Censimento generale della popolazione del 1981* registra questa nuova realtà e l'Italia si scopre *Paese di immigrazione*. Dal censimento risulta infatti che per la prima volta dalla fine della guerra nel corso del decennio intercensuario è arrivata o tornata un numero superiore di persone di quante ne fossero partite. La popolazione residente totale nel nostro Paese alla data del censimento risulta, infatti, pari a circa 56.250.000 unità: una cifra superiore non solo a quella del censimento precedente ma – quel che più conta – anche a quella che si sarebbe avuta in assenza di movimenti migratori.

Non solo. Per la prima volta nella storia dell'Italia del dopoguerra, l'entità complessiva della popolazione presente nel Paese alla data del censimento risultava superiore a quella della popolazione residente. In sostanza, in Italia è presente un numero superiore di persone di quante ne risultassero iscritte presso le anagrafi comunali, fenomeno tipico delle aree di immigrazione.

L'analisi di questo dato ci porta a registrare il combinato disposto di due fattori che si intrecciano in quegli anni: da un lato il *ritorno degli italiani* e, dall'altro, lo sbocciare di un fenomeno nuovo quello dell'*immigrazione degli stranieri*, ancora raramente registrata dalle anagrafi comunali. Se in termini di grandezze demografiche l'effetto dei due flussi in entrata era lo stesso, tuttavia è evidente come la natura diversa dei due fenomeni necessitava di una piena e lungimirante valutazione delle implicazioni politiche, sociali ed economiche.

Ciò, in particolare, con riguardo al ruolo di soggetti immigrati nel mercato del lavoro ed il grande tema che si affaccia e che ancora ci interroga oggi, se tale *ruolo sia complementare o sostitutivo*, se cioè gli immigrati si collocano in posti di lavoro non coperti dai lavoratori italiani o se invece entrino in concorrenza con questi, dando vita ad una progressiva

sostituzione in alcuni settori produttivi. Nel primo caso si tratterebbe di una '*immigrazione da domanda*', cioè trainata dalla domanda di lavoro in espansione nei Paesi di arrivo, nel secondo caso di un'immigrazione dovuta essenzialmente alla spinta migratoria dei Paesi poveri, cioè di una '*immigrazione da offerta*', in un certo senso subita dai Paesi di immigrazione con la conseguente concorrenza tra immigrati e locali sul mercato del lavoro.

Va sottolineato come in Italia il tradizionale dualismo della struttura occupazionale ha assunto caratteristiche nuove e nuovi segmenti della domanda di lavoro, che in taluni casi offrono condizioni in generale precarie, soprattutto nel settore dell'agricoltura e dei servizi. In essi trovavano lavoro prevalentemente immigrati stranieri. Parallelamente, nell'ambito dei servizi alla persona -collaborazione domestica o assistenza agli anziani – è emersa da subito una crescente domanda di manodopera, per cui si andò creando una nuova tipologia di lavoro prevalentemente coperta da lavoratrici straniere. Con l'apparente paradosso della coesistenza in particolare nel Sud Italia, di occupazione straniera e disoccupazione.

4. L'Italia degli sbarchi. Da Brindisi ad oggi

A questo fenomeno migratorio sostanzialmente connesso al mercato del lavoro, si aggiunge improvvisamente sulla scena italiana quello degli sbarchi massivi.

Lo sbarco del 7 marzo 1991 a Brindisi segna un punto di svolta. Siamo a dopo la caduta del muro di Berlino del 1989 ed al conseguente collasso di alcuni Paesi gravitanti nell'area come l'Albania. Si trattò di un arrivo massivo di migliaia di persone cui fece seguito un altro arrivo importante nell'agosto 1991 a Bari.

Il tema migratorio entra così prepotentemente nell'agenda politica e nell'attenzione della Comunità nazionale.

In verità, la legislazione in materia di immigrazione fino alla fine degli anni '80 aveva sostanzialmente sottovalutato la portata del fenomeno migratorio a causa del fatto che il nostro Paese, come si è detto dagli inizi del '900 era stato di tendenziale emigrazione (verso gli Stati Uniti, l'America Latina e i Paesi del Nord Europa). Di conseguenza, la legislazione nazionale affrontava le problematiche degli stranieri sotto l'esclusivo profilo dell'ordine pubblico.

L'art. 10, co. 2, Cost. – secondo cui «la condizione giuridica dello straniero è regolata dalla legge in conformità delle norme e dei trattati

internazionali» – in sostanza è rimasto sostanzialmente inattuato fino agli anni '80 del secolo scorso.

A parte infatti una circolare del Ministro del Lavoro del 1964 (sull'impiego di lavoratori subordinati stranieri) e la ratifica nel 1981 di una Convenzione OIL (relativa alla promozione dell'uguaglianza e al trattamento dei lavoratori migranti, del 1975), la questione migratoria viene disciplinata per la prima volta, peraltro con carattere emergenziale, con la legge 30 dicembre 1986, n. 943 che avviava la politica delle sanatorie dirette alla regolarizzazione, introduceva il permesso di soggiorno per motivi di studio e di turismo, disponeva la possibilità di effettuare il ricongiungimento familiare, introduceva l'autorizzazione al lavoro e istituiva (tra l'altro) la consulta per i problemi dei lavoratori extracomunitari e delle loro famiglie.

La prima disciplina avente carattere organico è rappresentata dalla c.*d. legge Martelli* (legge 28 febbraio 1990, n. 39, che convertiva il decreto-legge 30 dicembre 1989, n. 416, recante norme urgenti in materia di asilo politico, di ingresso e soggiorno dei cittadini extracomunitari e di regolarizzazione dei cittadini extracomunitari ed apolidi già presenti nel territorio dello Stato. Disposizioni in materia di asilo), che conteneva norme in materia sia di rifugiati sia di immigrazione. La legge Martelli ha introdotto concetti e meccanismi che costituiscono la base dell'attuale legislazione in materia, operando in maniera sia preventiva sia repressiva. Per un verso, si disponeva la programmazione in materia di flussi di ingresso degli immigrati alla luce delle esigenze del mercato del lavoro, mediante il rilascio di un apposito permesso di soggiorno. Per altro verso, era prevista la regolarizzazione degli stranieri già presenti sul territorio. La legge prevedeva anche peraltro disposizioni di carattere penale (pene detentive e pecuniarie) e disciplinava per la prima volta la procedura di espulsione degli stranieri socialmente pericolosi oppure irregolari, su decreto motivato del Prefetto, cui gli stranieri dovevano ottemperare entro 15 giorni, pena l'accompagnamento coatto alla frontiera.

Gli *sbarchi di Brindisi e Bari* portano all'adozione di alcuni provvedimenti come il c.d. decreto Conso del 1993 (decreto-legge 14 giugno 1993, n. 187, convertito nella legge 12 agosto 1993, n. 296) che introdusse nuovi reati modificando la disciplina dell'espulsione e i c.d. decreti Dini del 1995/1996 (decreti-legge mai convertiti in legge) che introdussero una nuova forma di espulsione come misura preventiva, accompagnata dalla possibilità di stabilire l'obbligo di dimora dello straniero da allontanare.

Con la metà degli anni Novanta si ebbe un superamento della logica dell'emergenza, stabilendo una cornice normativa di carattere generale

e sistematica. Il varo della c.d. *legge Turco-Napolitano* del 1998 (legge 6 marzo 1998, n. 40), segna l'avvio di una programmazione degli ingressi regolari, stabilendo percorsi di integrazione degli stranieri regolarmente residenti sul territorio dello Stato ed il parallelo contrasto all'immigrazione irregolare.

A questa seguirà la c.d. *legge Bossi-Fini* (legge 30 luglio 2002, n. 189), che introduceva alcune novità iscrivibili a un'impostazione restrittiva dell'ingresso e del soggiorno degli stranieri. Si segnala la formalizzazione del contratto di soggiorno quale titolo per la permanenza sul territorio, l'abolizione del sistema dello sponsor (con contestuale preferenza per gli stranieri che si sono formati nel loro Paese d'origine sulla base di pro-grammi approvati dalla pubblica amministrazione italiana), la limitazione dei casi di ricongiungimento familiare e la creazione degli Sportelli unici per l'immigrazione situati presso le Prefetture. La Bossi-Fini si caratterizzava anche per l'inasprimento delle procedure di allontanamento, con particolare riferimento alla regola della immediata esecuzione delle espulsioni con accompagnamento coatto alla frontiera (anche, cioè, in pendenza di impugnazione e in presenza di un procedimento penale a carico dello straniero). Il successivo d.P.R. 18 ottobre 2004, n. 334 ha modificato il regolamento di attuazione del T.U. nel senso indicato dalla Bossi-Fini.

La legislazione in materia è stata successivamente interessata da importanti modifiche dirette a recepire la *normativa europea* nel frattempo intervenuta. In particolare, con i due d.lgs. 8 gennaio 2007, n. 3 e 5, si è data rispettivamente attuazione alla direttiva sui c.d. lungosoggiornanti (2003/109/CE) e alla direttiva sul ricongiungimento familiare (2003/86/CE). Il d.lgs. 6 febbraio 2007, n. 30, invece, ha recepito la direttiva sui cittadini UE e loro familiari (2004/83/CE).

Il varo dei cc.dd. *pacchetti sicurezza* ha inciso negli anni a venire in modo sostanziale sulla materia.

Negli anni 2008-2011 è stata intrapresa una politica dell'immigrazione nuovamente restrittiva. In primo luogo, la legge 24 luglio 2008, n. 125 (misure urgenti in materia di sicurezza pubblica) ha previsto l'espulsione giudiziale per cittadini UE o ex-tra-UE in caso di condanna alla reclusione per più di due anni.In secondo luogo, il d.lgs. 3 ottobre 2008, n. 160 ha modificato in senso più restrittivo le precedenti disposizioni sul ricongiungimento familiare (d.lgs. 5/2007), in particolare limitando il novero dei familiari ricongiungibili. La novità più importante è rappresentata dall'introduzione del reato di ingresso e soggiorno illegale. Inoltre, viene punito più gravemente il favoreggiamento all'immigrazione clandestina.

Con la legge 94/2009 è stato poi previsto l'obbligo di versare un contributo per il rilascio e il rinnovo del permesso di soggiorno, l'obbligo di sottoscrivere un "accordo di integrazione" nel momento della presentazione della domanda di rilascio del permesso di soggiorno (articolato per crediti che, se sottratti, comportano la revoca del permesso di soggiorno), l'obbligo di esibire agli uffici pubblici il titolo di soggiorno per una serie di documenti e prestazioni, la cancellazione dello straniero dall'anagrafe dopo sei mesi dalla scadenza del permesso di soggiorno, la verifica della conoscenza della lingua italiana per ottenere il titolo di lungosoggiornante e il rilascio del nulla-osta per il ricongiungimento familiare solo da parte dello Sportello unico per l'immigrazione e il divieto di ricongiungimento in caso di poligamia. Per quanto riguarda le condizioni di vita, la legge 94/2009 contempla l'obbligo di dimostrare la disponibilità di un alloggio conforme ai requisiti igienico-sanitari e dotato di idoneità abitativa (accertata dalle autorità comunali) per lo straniero che richiede il ricongiungimento familiare nonché la possibilità della verifica da parte del Comune delle condizioni igienico-sanitarie dell'immobile (a seguito della richiesta di iscrizione e variazione anagrafica).

La predetta impostazione restrittiva è stata successivamente mitigata dalle modifiche introdotte per dare attuazione alla normativa dell'Unione europea. In particolare, le previsioni legislative concernenti il trattenimento e l'espulsione degli stranieri sono state riformulate con la legge 2 agosto 2011, n. 129 (di conversione del decreto-legge 23 giugno 2011, n. 89) che ha dato attuazione alla c.d. direttiva rimpatri (2008/115/CE), consentendo il rimpatrio c.d. volontario, prevedendo un termine massimo più ampio di permanenza nei CIE (fino a 18 mesi) e disponendo forme alternative di trattenimento. Più di recente, il d.lgs. 28 giugno 2012, n. 108, ha recepito la direttiva sui lavoratori altamente qualificati (2009/50/CE), il d.lgs. 16 luglio 2012, n. 109, ha dato attuazione alla direttiva sulle sanzioni ai datori di lavoro che impiegano stranieri irregolari (2009/52/CE), la legge 6 agosto 2013, n. 97 (legge europea 2013) ha reso possibile l'accesso al pubblico impiego per i familiari extra-UE di cittadini UE aventi diritto di soggiorno o di soggiorno permanente, per i lungosoggiornanti e per i beneficiari di protezione internazionale. Infine, il d.lgs. 4 marzo 2014, n. 40, ha recepito la direttiva 2011/98/UE sul procedimento unico per il rilascio di un permesso di soggiorno e di lavoro e un insieme comune di diritti per i lavoratori di paesi terzi.

5. *Per un'immigrazione legale*

Questa carrellata ci consente di arrivare ad oggi.

La spinta a garantire l'ingresso in Italia ad un'immigrazione legale che assicuri dignità alle persone e sostenibilità sociale ed economica nei territori, evitando problematiche di ordine pubblico ed il rischio della polarizzazione strumentale della narrazione sul fenomeno migratorio, sta spingendo sempre più a garantire l'ingresso nel nostro Paese, secondo criteri di reale incrocio tra domanda ed offerta di lavoro.

A parte le situazioni ovviamente legate ai presupposti dello *status* di rifugiato, ovvero di altre tipologie di ingresso tutelato, destinate ad una disciplina specifica che si muove a massima tutela degli interessati, l'ingresso in Italia deve avvenire secondo canali legali per motivi di lavoro subordinato, anche stagionale, e di lavoro autonomo.

Ciò deve avvenire nell'ambito delle quote di ingresso stabilite dallo Stato così da assicurare l'incrocio tra domanda ed offerta di lavoro e conseguente possibilità d'inserimento sociale nelle comunità ospitanti. Con i cosiddetti *'decreti-flussi'* – periodicamente emanati dal Presidente del Consiglio dei Ministri sulla base dei criteri indicati nel documento programmatico triennale sulle politiche dell'immigrazione- sono fissati i tetti d'ingresso con una pianificazione che ha un respiro triennale. Ogni tre anni il Presidente del Consiglio dei Ministri (sentiti i Ministri interessati, il CNEL, la Conferenza Stato-regioni-province, la Conferenza Stato-città e autonomie locali, gli enti e le associazioni nazionali maggiormente attivi nell'assistenza e nell'integrazione degli immigrati e le organizzazioni dei lavoratori e dei datori di lavoro maggiormente rappresentative sul piano nazionale) predispone il Documento programmatico relativo alla politica dell'immigrazione e degli stranieri nel territorio dello Stato.

Queste procedure sono ormai da diversi anni gestite per via telematica, per cui sarà sufficiente collegarsi dal proprio computer, oppure avvalersi del supporto dei numerosi enti o patronati abilitati, per svolgere tutta la pratica. Il sistema informatizzato è composto da un sito *web* al quale l'utente deve connettersi tramite una connessione a Internet per, poi, effettuare la compilazione e la spedizione via telematica delle domande.

6. *La "disinformazione" nello scenario dell'immigrazione*

La spinta verso una valorizzazione di canali d'ingresso legali, con

un'attenta e rigorosa programmazione dei flussi ed il parallelo contrasto dell'immigrazione illegale, con il bagaglio criminale che questa reca con sé, costituisce uno degli obiettivi fondamentali per una efficace *governance* del fenomeno migratorio.

Coniugare diritti e doveri, il rispetto delle regole con l'integrazione degli stranieri significa garantire quella necessaria coesione sociale nei territori che consente di evitare l'innescarsi di potenziali situazioni di conflittualità. Questa è la sfida che si pone oggi una società moderna e multietnica.

Un' azione di governo decisiva al riguardo – che punti ad assicurare in sostanza il rispetto dei diritti di chi vuole migrare per cercare un destino migliore, senza recedere sui doveri e le regole della società che accoglie – non può prescindere da una sempre più profonda conoscenza delle ragioni del migrare.

Il dato di partenza è che oggi è urgente assumere elementi di analisi e valutazione sempre più diretti ed approfonditi, per comprendere quanto rilevino le ragioni soggettive – spontanee o indotte – delle migrazioni, oltre quelle ovviamente oggettive di cui si è detto all'inizio.

In altri termini, indagare il profilo soggettivo del fenomeno, le sollecitazioni a cui è sottoposto il potenziale migrante e che generano le scelte di intraprendere un viaggio lungo, complesso e pericoloso, è senz'altro utile per l'analista in termini di approfondimento scientifico, ma è soprattutto strategico per il decisore pubblico.

In tale ottica, è fondamentale indagare, in questa società dell'informazione, che ruolo giochino e, in che misura, le strategie dell'informazione e, soprattutto, della disinformazione.

Il punto nodale è in sostanza la comprensione dei molteplici fattori di spinta al migrare, muovendo dall'assunto che si tratta indubbiamente di un fenomeno estremamente complesso, dinamico che intreccia causali molto diverse tra loro e che quindi è soggetto a modificazioni continue dovute proprio al comporsi ed allo scomporsi delle diverse motivazioni che lo sottendono.

Questo ha fatto maturare l'interesse del Ministero dell'interno – e mio personale nella responsabilità di Capo del Dipartimento per le libertà civili e l'immigrazione – ad aderire al progetto dell'Università degli Studi della Tuscia guidato dal prof. Sterpa. Il nostro contributo ha consentito di somministrare direttamente, su base volontaria, i questionari (anonimizzati) ai richiedenti asilo presenti in alcune strutture di accoglienza. Sono stati così selezionati alcuni centri – come quelli di Bari, Isola Capo Rizzuto (Crotone) e di Rocca di Papa, che è stato anche visitato

dal Sindaco di New York che ho accompagnato illustrando il sistema di accoglienza italiano, a testimonianza dell'interesse che il sistema italiano raccoglie anche all'estero – presso i quali i ricercatori del progetto hanno potuto intervistare i richiedenti asilo. Un contributo che si è rivelato essenziale per la riuscita del progetto e desidero ringraziare i ricercatori per la professionalità e la sensibilità con la quale hanno proceduto nel loro lavoro. Un ringraziamento che estendo per la collaborazione prestata ai gestori delle strutture e, in particolare, ai richiedenti asilo che hanno aderito alla ricerca.

Il progetto ha così preso concretamente vita grazie al confronto ed alla condivisione interdisciplinare dell'analisi che ne è scaturita e che ha fornito alla ricerca significativi elementi di valutazione.

Lo studio ha messo in luce, in particolare, come il tema delle migrazioni incontri quello della *disinformazione*. Lo scenario che si apre è complesso e la ricerca evidenzia come la "*disinformatio*" diventi strumento, anche nella partita delicata della *guerra ibrida* (la c.d. "*guerra cognitiva*") che costituisce un terreno d'indagine di particolare complessità.

Una complessità che chiama in causa la crescente dicotomia tra *democrazie liberali ed autocrazie* con la dialettica che ne segue e che sembra oggi imperniarsi sulla presunta maggiore efficienza delle seconde rispetto alle prime, soggiogate dal peso del confronto democratico, della partecipazione, della corresponsabilità nelle scelte, in buona sostanza dal peso, secondo taluni dello scarso efficientismo. Dall'altro, le autocrazie giocano la carta tipica dei sistemi che non necessitano di processi decisionali condivisi e complessi, ma che operano verticisticamente, e, quindi, accorciando il processo decisionale ai minimi essenziali.

L'analisi scaturita dal progetto fa emergere come l'informazione e, con essa, la disinformazione giocano un ruolo decisivo anche nelle migrazioni soprattutto economiche, dove il dato soggettivo, la possibilità di influire in modo decisivo sulla decisione del migrante e sul convincimento che si riesce a generare nella comunità di appartenenza, risultano determinanti per la partenza.

Un elemento importante che ci mette di fronte – al fine di tutelare l'istituto del diritto di asilo – ad una riflessione delicata sulla necessità di dover in futuro essere in grado di distinguere, nell'ampissimo bacino delle richieste di asilo, dove tutto converge, le richieste motivate da elementi oggettivi che potranno portare al riconoscimento dello status, da quelle scaturite da fattori magari legati proprio alla disinformazione ed alla strumentalizzazione del nobile strumento dell'"asilo".

Governare il fenomeno significa anche prendere atto di questo, la-

sciando lo strumento della richiesta di asilo solo a coloro i quali hanno realmente i presupposti per il beneficio, perché provenienti da aree interessate da guerre, persecuzioni e crisi umanitarie e potenziando per gli altri strumenti diversi che consentano, laddove sussistano ragioni di esclusiva natura economica, di fruire di canali d'ingresso legale che valorizzino l'incrocio domanda offerta di lavoro e la formazione lavoro già nei Paesi di origine.

Un' esigenza ormai non più procrastinabile, per garantire una risposta da un lato a chi sogna un futuro migliore, che possiamo dare solo nella legalità con la dignità del lavoro e, dall'altro, al fabbisogno delle aziende.

Un'esigenza che, ritengo, consentirà di evitare il rischio di inflazionare l'istituto dell'asilo, consacrato nella ns. Carta Costituzionale e nella Convenzione di Ginevra, con esiti imprevedibili che potrebbero anche giungere potenzialmente ad una sua revisione.

Ed anche qui gioca oggi, e giocherà sempre più in futuro, un ruolo decisivo l'*informazione corretta* in luogo di una disinformazione fuorviante e strumentalizzata, galoppante in molti Paesi.

Un'informazione che in sostanza adempia al proprio autentico ruolo, che è quello di fornire gli elementi di conoscenza per consentire al migrante, prima d'intraprendere un viaggio complesso e pericoloso, una valutazione piena e consapevole sia dei rischi che delle reali opportunità cui va incontro.

Una scelta in sostanza che, nell'interesse stesso del migrante, gli consenta di bilanciare i pro ed i contro della partenza, le reali prospettive, i rischi del viaggio, gli oneri cui sottopone sè stesso e la propria famiglia, nell'ottica di evitare arrivi destinati a creare clandestinità e lavoro nero, e favorire al contrario una reale integrazione ed opportunità per il futuro.

In tale direzione, l'informazione dovrà essere vieppiù curata dalle istituzioni competenti in parternariato, laddove possibile con i Paesi di origine, le associazioni di categorie, gli enti non governativi accreditati, favorendo in via esclusiva la migrazione legale, ossia l'inserimento in canali di accesso in Europa ed in particolare in Italia, attraverso l'incrocio tra domanda ed offerta di lavoro (cd. decreto flussi) ed i canali umanitari (laddove sussistenti i requisiti).

D'altronde, notevoli e crescenti sono gli interventi effettuati in entrambe tali direzioni nei Paesi di origine e di transito per supportare le popolazioni con iniziative di formazione lavoro dirette a garantire migrazioni legali come numerosi i progetti varati in questa direzione ricordare Egitto-Etiopia che stanno dando risultati significativi senz'altro da implementare.

Se è vero, infatti, che i fattori di espulsione forzata costituiscono la motivazione principale della partenza dei migranti provenienti in particolare dall'Africa subsahariana, è pur vero che il fattore motivazionale legato al diritto allo studio aumenta l'aspettativa di mobilità sociale. Conseguentemente, la propensione a istruirsi cresce nel Paese d'arrivo, nel momento in cui si diventa consapevoli che l'istruzione è l'unico strumento capace di espandere l'orizzonte delle proprie aspirazioni e di permettere migliori condizioni di vita. Infatti, i dati suggeriscono anche una dinamica post-migratoria importante: molti migranti, una volta arrivati, comprendono che la scolarizzazione è essenziale per ottenere stabilità e diritti nella società d'accoglienza.

Conclusioni

Il progetto segna, a mio giudizio, un momento decisivo nel dibattito scientifico e istituzionale. Un vero e proprio salto in avanti nell'analisi del fenomeno migratorio che in questo momento storico assume un valore particolarmente significativo. Nell'attuale scenario geopolitico particolarmente complesso, contribuisce, infatti, ad aprire lo sguardo nella genesi delle migrazioni e a pervenire ad una proiezione reale della strategia da assumere per governare i flussi migratori.

Una ricerca preziosa che, pertanto, merita di strutturarsi e rinnovarsi, con una cadenza almeno biennale, ampliando il perimetro dei Paesi di provenienza indagati, così da abbracciare le ulteriori diverse aree da cui giungono i migranti.

Un contributo importante con il quale leggere il fenomeno – interpretandone l'eventuale ruolo nel quadro del più complessivo scenario della cd. guerra cognitiva – allo scopo di garantire una risposta al fenomeno migratorio che sia consapevole e strutturale, così da garantire una capacità effettiva di accoglienza nel rispetto dei diritti e dei doveri e la piena sostenibilità sociale ed economica del fenomeno migratorio. Oggi ed in futuro.

BIBLIOGRAFIA

Aa.Vv., *Il mondo in guerra*, Tab, Roma, 2024.

Aa.Vv., *Chinese Next-Generation Psychological Warfare*, RAND Corporation, Santa Monica, 2023.

A. Antinori, *Artificial Inte[Glitch]Ence. Una minaccia sistemica alla sicurezza nazionale in prospettiva futura*, in *GNOSIS. Rivista italiana di Intelligence*, n. 2, 2019.

A. Antinori, *La Cognitive Warfare in uno scenario di minacce convergenti*, in *Sicurezza, Terrorismo e Società*, n. 19, 2024.

A. Antinori, *Malicious Use of Artificial Intelligence (MUAI): l'uso malevolo dell'Intelligenza Artificiale nell'ecosistema cyber-sociale*, in *Sicurezza e scienze sociali*, n. 2, 2025.

A. Antinori, *Radicalisation and FIMI in the Western Balkans Cyber-Social Ecosystem*, in A. Antinori, J. Nijenhuis (a cura di), *How FIMI Fuels Polarisation and Radicalisation in the Western Balkans*, *Institute of Communication Studies*, Skopje, 2026.

D.A. Abbott, *The Handbook of 5GW: A Fifth Generation of War?*, Nimble Books, Ann Arbor, 2010.

C. Abidin, *Internet Celebrity: Understanding Fame Online*, Emerald Publishing, Bingley, 2018.

P. Accolla, N. D'Aquino, *Italici. An Encounter with Piero Bassetti*, Bordighera Press, New York, 2008.

S.K. Acharya, A. Aul, W. Rahman, *Quantum Social Science: Exploring Possibility and Insights for New Genre of Social Science Research (QSS)*, in *Journal of Community Mobilization and Sustainable Development*, v. 20, n. 3, 2025.

S. Akbar, S.K. Saritha, *Towards quantum computing based community detection*, in *Computer Science Review*, v. 38, 2020.

Y. Alexeev, M.H. Farag, T.L. Patti, M.e. Wolf, N. Ares, A. Aspuru-Guzik, S.C. Benjamin, Z. Cai, S. Cao, C. Chamberland, Z. Chandani, F. Fedele, I. Hamamura, N. Harrigan, J.S. Kim, E. Kyoseva, J.G. Lietz, T. Lubowe, A. Mccaskey, R.G. Melko, K. Nakaji, A. Peruzzo, P. Rao, B. Schmitt, S. Stanwyck, N.m. Tubman, H. Wang, T. Costa, *Artificial intelligence for quantum computing*, in *Nature Communications*, 2025.

H. Allcott, M. Gentzkow, *Social Media and Fake News in the 2016 Election*, in *Journal of Economic Perspectives*, v. 31, n. 2, 2017.

K. Allen, C. Nehring, *AI-Generated Disinformation in Europe and Africa – Use Cases, Solutions and Transnational Learning*, Konrad-Adenauer-Stiftung e.V., 2025.

M. Ananny, K. Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, in *New Media & Society*, v. 20, n. 3, 2018.

R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, New York, 2020.

S. Ang, *Cultural Intelligence*, International Encyclopedia of the Social & Behavioral Sciences, 2015.

S. Ang, van Dyne L., *Handbook of Cultural Intelligence*, Routledge, 2008.

A. Anghie, *Finding the Peripheries: Sovereignty and Colonialism in Nineteenth-Century International Law*, in *Harvard International Law Journal*, 1999.

D. Antiseri, *Il prezzo della libertà è l'eterna vigilanza*, Editoriale Scientifica, Napoli 2017.

G. Anzera, A. Massa, *Media diplomacy e narrazioni strategiche. Autorappresentazione dello Stato e attuazione della politica estera in rete*, Bonanno, Acireale-Roma, 2017.

S. Aral, L. Muchnik, A. Sundararajan, *Distinguishing influence-based contagion from homophily-driven diffusion in dynamic networks*, in *Proceedings of the National Academy of Sciences*, v. 106, n. 51, 2009.

R. Arditti, *Hard power. Perchè la Guerra cambia la storia*, Giubilei Regnani, Roma-Cesena, 2025.

H. Arendt, *Le origini del totalitarismo (1951)*, Einaudi, Torino, 2009.

H. Arendt, *Responsabilità e giudizio*, Einaudi, Torino, 2003.

H. Arendt, *Sulla rivoluzione*, Milano, 1965.

H. Arendt, *Sulla violenza (1970)*, Guanda, Parma, 1996.

O. Aslan, S.S. Actuğ, M. Ozkan-Okay, A.A. Yilmaz, E. Akin, *A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions*, in *Electronics*, v. 12, n. 6, 2023.

C. Atkinson, *Hybrid warfare and societal resilience: Implications for democratic governance*, in *Information & Security*, v. 39, n. 1, 2018.

M.R. Atlas, M. Dando, *Il dilemma del duplice uso per le scienze della vita: prospettive, enigmi e soluzioni globali*, in *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, n. 3, 2006.

J. Attali, *Disinformati. Giornalismo e libertà nell'epoca dei social*, trad. it., Ponte alle Grazie, Milano, 2022,

E. Augusti, *'Frontiere aperte' e assistenza agli stranieri: il ruolo delle Conferenze internazionali in Europa tra Otto e Novecento*, in M.S. Testuzza, E. De Cristofaro (a cura di), *Tempi difficili. Crisi e trasformazioni otto novecentesche tra storia e diritto*, Collana "Storie del diritto", Acireale, 2023.

E. Augusti, *Crimea 1853-1856. La guerra attesa e la costruzione di un nuovo ordine mediterraneo*, in L. Brunori, C. Ciancio, E.C. Tavilla (a cura di), *Italia-France Allers-Retours: Luttes et revendications – Lotte e rivendicazioni in Historia et Ius*, Collana di Studi di Storia del diritto medievale e moderno, 2025.

E. Augusti, *From Capitulations to Unequal Treaties: The Matter of an Extraterritorial Jurisdiction in the Ottoman Empire*, in *Journal of Civil Law Studies*, 2011.

E. Augusti, *L'intervento europeo in Oriente nel XIX secolo: storia contesa di un istituto controverso*, in L. Nuzzo, M. VEC (a cura di), *Constructing International Law. The Birth of a Discipline*, Frankfurt am Main, 2012.

E. Augusti, *La giurisdizione consolare in Oriente: dal primato genovese alla sparizione. Spunti per una riflessione*, in V. Lavenia (a cura di), *Alberico e Scipione Gentili nell'Europa di ieri e di oggi. Reti di relazioni e cultura politica*, Atti della Giornata Gentiliana, San Ginesio, 16-17 settembre 2016, Macerata, 2018.

E. Augusti, *Migrare come abitare. Una storia del diritto internazionale in Europa tra XVI e XIX secolo*, Torino, 2022.

Augusti E., *Modernità, «First Global Competition» e Diritto internazionale universale tra Sette e Ottocento*, in A. Sciumé, A.A. Cassi, E. Fusar Poli (a cura di), *History&Law Encounters*, Torino, 2021.

E. Augusti, *Questioni d'Oriente. Europa e Impero Ottomano nel Diritto Internazionale dell'Ottocento*, Napoli, 2013.

E. Augusti, *Ripensare la nazione ottocentesca. Vecchi e nuovi paradigmi tra storia, diritto e globalità*, in M. Meccarelli (a cura di), *Reading the crisis. Legal, Philosophical and Literary Perspectives*, Madrid, 2017.

E. Augusti, *Storie e storiografie dei Consolati in Oriente tra Otto e Novecento*, in *Historia et ius*, 2017.

E. Augusti, *Un diritto possibile. Storie, teorie e prassi di modernità tra comparazione e globalizzazione*, in *Forum Historiae Iuris*, 2016.

E. Augusti, *Verso la nazione. Un itinerario concettuale tra Sette e Ottocento*, in F. Lamberti, M.L. Tacelli, U. Villani Lubelli (a cura di), *Diritto, storia, istituzioni. Liber amicorum Giancarlo Vallone*, Collana del Dipartimento di Scienze Giuridiche, v. 2, Napoli, 2024.

L. Balestrieri, *Big Tech. Il potere dei giganti della tecnologia*, Laterza, Roma-Bari, 2026.

D. Barral, F.J. Cardama, G. Díaz-Camacho, D. Faílde, L.F. Llovo, M. Mussa-Juane, J. Vázquez-Pérez, J. Villasuso, C. Piñeiro, N. Costas, J.C. Pichel, T.F. Pena, A. Gómez, *Review of Distributed Quantum Computing: From single QPU to High Performance Quantum Computing*, in *Computer Science Review*, 2025.

C. Bassu, *La lotta al terrorismo nelle democrazie stabilizzate: garantire la pubblica*

sicurezza nel rispetto dei diritti umani fondamentali, in C. Bassu, G. Pistorio, A. Sterpa, (a cura di), *Diritto pubblico della sicurezza*, Editoriale Scientifica, Napoli, 2023.

A. Basu, K. Saini, *Setting International Norms of Cyber Conflict Is Hard, but That Doesn't Mean We Should Stop Trying*, Modern War Institute at West Point, 2019.

Z. Bauman, Paura liquida, Laterza, Roma-Bari, 2008.

A. Beccario, *Guerra e strategia nel XXI secolo*, Morcelliana, Brescia, 2023.

Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale University Press, New Haven, 2006.

C. Bennett, *Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?*, in *International Data Privacy Law*, 2016.

A. Bernal, C. Carter, I. Singh, K. Cao, O. Madreperla, *Cognitive Warfare. An attack on truth and thought*, NATO Innovation Hub, 2020.

E.L. Bernays, *Propaganda*, Horace Liveright, New York, 1928.

G. Berti, *Sovranità (voce)*, in *Enciclopedia del diritto*, Annali I, Giuffrè, Milano, 2007.

G. Bhatia, *Disinformation, Misinformation and Democracy: An Indian Constitutional Perspective* in R.J. Krotoszynski Jr., A. Koltay, C. Garden (a cura di), *Disinformation, Misinformation and Democracy*, Cambridge University Press, Cambridge, 2024.

P. Biondi, *Studi sul potere*, Giuffrè, Milano, 1965.

C. Bisconti, A. Corallo, M. De Maggio, F. Grippa, S. Totaro, *Quantum modeling of social dynamics*, in *International Journal of Knowledge Society Research*, v. 1, 2010.

R. Blutner, R.B. Graben, *Descriptive and Foundational Aspects of Quantum Cognition*, in *Neurons and Cognition*, 2014.

R. Blutner, R.b. Graben, *Quantum cognition and bounded rationality*, in *Syntheses*, v. 193, 2016.

R. Bocchini (a cura di), *Le piattaforme digitali. e-Agorà*, Giappichelli, Torino, 2025.

N. Bolt, E. Lange-Ionatamishvili, *The Next Generation Information Environment*, in *NATO Strategic Communications Centre of Excellence*, Riga, 2026.

P. Bonetti, *Terrorismo, emergenza e costituzioni democratiche*, Il Mulino, Bologna, 2006.

E. Borghi, *Sotto attacco*, Rubbettino, Soveria Mannelli, 2025.

A. Boström, A. Hylander, *Selecting Better Attacks for Cyber Defense Exercises – Criteria to Enhance Cyber Range Content*, Linköping University, Department of Computer and Information Science, 2024.

J. Botha, *Disinformation and Democracy in Africa and South Africa*, in R.J. Krotoszynski Jr., A. Koltay, C. Garden (a cura di), *Disinformation, Misinformation and Democracy*, Cambridge University Press, Cambridge, 2024.

S. Boulianne, *Social Media Use and Participation*, in *Information, Communication & Society*, v. 18, n. 5, 2015.

B. Bowden, *The Empire of Civilization: The Evolution of an Imperial Idea*, Chicago, 2009.

H.W. Brachinger, P.A. Monney, *The Conjunction Fallacy: Explanations of the Linda Problem by the Theory of Hints*, in International Journal of Intelligent Systems, v. 18, 2003.

W. Brown, J. Kobzova, N. Popescu, J.I. Torreblanca, *From Shield to Sword: Europe's offensive Strategy for the Hybrid Age*, European Council on Foreign Relations, 2026.

C. Bruderlein, *Manual on International Law Applicable to Air and Missile Warfare*, Program on Humanitarian Policy and Conflict Research at Harvard University, 2009.

P. Bruza, J. Busemeyer, L. Gabora, *Introduction to the Special Issue on Quantum Cognition*, in *Journal of Mathematical Psychology*, 2009.

M.E. Bucalo, M. Caporale, A. Sterpa (a cura di), *Diritto pubblico di internet,* Editoriale Scientifica, Napoli, 2024.

J.R. Busemeyer, M. Ozawa, E.m. Pothos, N. Tsuchiya, *Incorporating episodic memory into quantum models of judgment and decision*, in *Philosophical Transactions of the Royal Society*, 2025.

J.R. Busemeyer, Z. Wang, *What Is Quantum Cognition, and How Is It Applied to Psychology?*, in *Current Directions in Psychological Science*, v. 24, n. 3, 2015.

C.G. Jung, *L'Io e l'Inconscio* (1928), Boringhieri, Torino, 1948.

A. Cabello, L.e. Danielsen, A.j. López-Tarrida, J.r. Portillo, *Quantum social networks*, in *Journal of Physics A: Mathematical and Theoretical*, v. 45, n. 28, 2012.

M. Cacciari, *Il potere che frena*, Milano, 2013.

A. Calabrese, *Cyberwar e diritto internazionale: la frontiera digitale del conflitto armato tra principi umanitari, responsabilità e protezione dei civili*, Università degli Studi di Torino, 2025.

A. Calabrese, *Verso un'arma cyber nazionale: la strategia del Min. Crosetto nel contesto europeo*, Geopolitica.info, 2025.

P. Calamandrei, *Situazione giuridica dei partigiani sotto l'aspetto del diritto interno e internazionale e del diritto interno*, Centro di Alti Studi militari, Roma, 1949/50.

M. Calamo Specchia, *Un prisma costituzionale, la protezione della Costituzione: dalla democrazia "militante" all'autodifesa costituzionale*, in *Diritto Pubblico Comparato ed Europeo*, n. 1, 2021.

E. Calcagno, *Taking Multi-domain Operations from Theory to Practice*, in *Documenti IAI*, 2026.

M. Caligiuri, *Intelligence*, Treccani, Roma, 2025.

M. Caligiuri, A. PAGANI, *Disinformare: ecco l'arma. L'emergenza educativa e democratica del nostro tempo*, Rubbettino, Soveria Mannelli, 2024.

C. Camardi (a cura di), *La via europea per l'intelligenza artificiale*, Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche – Ca' Foscari Venezia, 25-26 novembre 2021, Wolters & Kluwers, Milano, v. 1, 2022.

L. Candelori, A.G. Abanov, J. Berger, C.J. Hogan, V. Kirakosyan, K. Musaelian, R. Samson, J.E.T. Smith, D. Villani, M.T. Wells, M. Xu, *Robust estimation of the intrinsic dimension of data sets with quantum cognition machine learning*, in *Scientific Reports*, v. 15, 2025.

C. Capasso, *"Algo-sicurezza". Terrorismo, contesto digitale e sicurezza*, Napoli, Editoriale Scientifica, 2025.

B. Caravita, *Principi costituzionali e intelligenza artificiale*, ora in Id., *Letture di diritto costituzionale*, Giappichelli, Torino, 2020.

A. Cardone, *Profilazione a fini politico-elettorali e tenuta della democrazia rappresentativa: una lezione per le riforme istituzionali e per la regolazione del pluralismo democratico in Rete*, in A. Adinolfi, A. Simoncini (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edittoriale Scientifica, Napoli, 2022.

C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quad. cost.*, n. 3, 2023.

B. Casarotti, *La politica europea sul digitale: ancora molto rumore*, in *Riv. Trim. Dir.Pubbl.*, n. 4, 2022.

J. Cascio, *Facing the Age of Chaos*, Medium, www.medium.com, 2020.

E. Casini, A. Manciulli, *La guerra tiepida*, Luiss University Press, Roma, 2023.

F. Casolari, *Il "Digital Services Act" e la costituzionalizzazione dello spazio digitale europeo*, in *Giur. it*, n. 2, 2024.

C. Casonato, *L'intelligenza artificiale e il diritto pubblico comparato ed europeo*, in *DPCE online*, n. 1, 2022.

A. Cassese, *Commento all'articolo 11*, in G. Branca (a cura di), *Commentario della Costituzione*, *articoli 1-12*, *Principi generali*, Zanichelli-Foro it., Bologna-Roma, 1975.

S. Cassese, *Dizionario di diritto pubblico*, Giuffrè, Milano, 2006.

S. Cassese, *La democrazia e i suoi limiti*, Mondadori, Milano, 2017.

A.A. Cassi, *Diritto e guerra nell'esperienza giuridica europea tra medioevo ed età contemporanea*, in A. Sciumè (a cura di), *Il diritto come forza. La forza del diritto. Le fonti in azione nel diritto europeo tra medioevo ed età contemporanea*, Torino, 2012.

M. Castells, *Communication Power*, Oxford University Press, Oxford, 2009.

E. Caterina, *La metamorfosi della "democrazia militante" in Germania. Appunti sulla sentenza NPD del Tribunale costituzionale federale e sulla successiva revisione dell'art. 21 della Legge fondamentale*, in *Diritto Pubblico Comparato ed Europeo,* n. 1, 2018.

A. Cavoukian, *Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Information & Privacy Commissioner of Ontario, Toronto, 2011.
S. Ceccanti, F. Ferroni, *Democrazia protetta,* in *Digesto delle discipline pubblicistiche,* Utet, Torino, 2015.
S. Ceccanti, *Le democrazie protette e semi-protette da eccezione a regola. Prima e dopo le Twin Towers,* Giappichelli, Torino, 2004.
A. Celotto, *"Sudditi". Diritti e cittadinanza nella società digitale*, Giuffrè, Milano, 2023.
D. Chakrabarty, *Provincializzare l'Europa*, Roma, 2004.
J. Charney, *Fake News under Siege: A Century of Regulation in Chile*, in R.J. Krotoszynski Jr., A. Koltay, C. Garden (a cura di), *Disinformation, Misinformation and Democracy*, Cambridge University Press, Cambridge, 2024.
J. Chen, *Consciousness Transfer Technology: From Quantum States in Microtubules to Bionic Human-Like Brain Chips*, SSRN Paper, 2025.
M.A. Cherry, *Cyber Commodification*, in *Maryland Law Review*, 2013.
R. Chesney, D.K. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, in *California Law Review*, v. 107, n. 6, 2019.
L. Chieffi, *Pace e guerra in un'epoca di profonde trasformazioni delle relazioni internazionali* in *Rivista AIC*, supplemento n. 4, 2025.
L. Chiussi Curzi, *Uso della forza, diritto internazionale e* rule of law *nelle oscillazioni dell'ordine globale* in *federalismi.it*, n. 8, 2026.
Y. Chung, *Allusion, reasoning and luring in Chinese psychological warfare*, in *International Affairs*, v. 97, n. 4, 2021.
P. Ciarlo, *Democrazia, partecipazione popolare e populismo al tempo della rete*, in *Rivista AIC*, n. 2, 2018.
C. Cipolloni, *Persona, poteri privati e Stato nella rivoluzione internettiana*, Giappichelli, Torino, 2024.
F. Cirillo, *Neurolaw, Neurorights and Neuroprivacy: Theoretical and Constitutional Issues*, in *MediaLaws*, n. 1, 2024.
C. Clausewitz, *Vom Kriege*, 1832.
B. Claverie, F. Du Cluzel, *"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare*, in B. Claverie, B. Prébot, N. Buchler, F. Du Cluzel (a cura di), *Cognitive Warfare: The Future of Cognitive Dominance*, NATO Collaboration Support Office, 2022.
C. Claverie, F. Du Cluzel, *Cognitive Warfare: The Battle for Your Brain*, NATO Innovation Hub, 2021.
A. Clooney, *Introduction*, in A. Clooney, D. Neuberger (a cura di), *Freedom of Speech in International Law*, Oxford, OUP, 2024.
V. Codeluppi, *Mondo digitale*, Laterza, Roma-Bari, 2022.
J.E. Cohen, *Between Truth and Power*, Oxford, 2019.
F.P. Contuzzi, *Del nuovo indirizzo scientifico e pratico del diritto internazionale:*

prolusione al corso d'insegnamento pronunziata nella R. Università di Macerata nel d. 13 novembre 1881, Napoli, 1882.

P. Costanzo, *Il fattore tecnologico e il suo impatto sulle libertà fondamentali*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini, (a cura di), *Diritti e libertà in internet*, Milano, 2017.

M. Craven, *What Happened to Unequal Treaties? The Continuities of Informal Empire*, in *Nordic Journal of International Law*, 2005.

Cuba, *Declaration on International Law Related to the Use of ICTs in the Context of International Security*, 2017, www.justsecurity.org.

D. Cuomo, M. Caleffi, K. Krsulich, F. Tramonto, G. Agliardi, E. Prati, A.S. Cacciapuoti, *Optimized compiler for distributed quantum computing*, in *ACM Transactions on Quantum Computing*, 2023.

C. Curti Gialdino, *Manuale di diritto diplomatico-consolare europeo e internazionale*, Torino, Giappichelli, 2024.

A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in Id. (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, FrancoAngeli, Milano, 2023.

V. D'Antino *L'approccio basato sul rischio nell'AI: un nuovo paradigma di regolazione dell'intelligenza artificiale*, in *federalismi.it,* 2025.

G. D'Ippolito, G. Di Martino, *La privacy come elemento della cybersicurezza*, *Consumerism 2021 – Quattordicesimo rapporto annuale*, 2021, www.consumersforum.it.

G. Da Empoli, *La rabbia e l'algoritmo*, Marsilio, Venezia, 2017.

A. Damasio, *L'errore di Cartesio*, Adelphi, Milano, 1995.

M. De Carolis, *Il paradosso antropologico. Nicchie, micromondi e dissociazione psichica*, Quodlibet, Macerata, 2008.

C. De Fiores, *Il principio costituzionale pacifista, gli obblighi internazionali e l'invio di armi a paesi in guerra*, in G. Azzariti (a cura di), *Il costituzionalismo democratico moderno può sopravvivere alla guerra?*, Editoriale Scientifica, Napoli, 2022.

C. Deppe, G.S. Schaal, *Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept*, in *Frontiers in Big Data*, v. 7, 2024.

F. De Saussure, *Cours de linguistique générale (1916)*, Payot, Paris, 1972.

E. De Vattel, *Le droit des gens ou principes de la loi naturelle appliqués à la conduite et aux affaires des nations et des souverains (1758)*, Paris, 1835.

G. De Vergottini, *Guerra e attuazione della Costituzione*, 2002, *www.associazionedeicostituzionalisti.it* .

J. Der Derian, A. Wendt, *Quantum International Relations: A Human Science for World Politics*, Oxford University Press, Oxford, 2022.

J. Devlin, M. Chang, K. Lee, K. Toutanova, *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*, in *arXiv preprint*, 2018.

J. Dewey, *Democracy and Education*, Macmillan, 1916.
N. Diakopoulos, *Algorithmic Accountability: Journalistic Investigation of Computational Power Structures*, in *Digital Journalism*, v. 3, n. 3, 2015.
A. Di Corinto, *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in *Rivista Italiana di Informatica e Diritto*, n. 1, 2022.
A. Di Giovine, *Democrazie protette e protezione della democrazia*, Giappichelli, Torino, 2005.
L. Di Gregorio, *Demopatia. Sintomi, diagnosi e terapie del malessere democratico*, Rubbettino, Soveria Mannelli, 2019
L. Di Gregorio, *War Room Attori, strutture e processi della politica in campagna permanente*, Rubbettino, Soveria Mannelli, 2024.
W. Diffie, M. Hellman, *New Directions in Cryptography*, in *IEEE Transactions on Information Theory*, v. 22, n. 6, 1976.
J.V. Dijck, T. Poell, M. De Waal, *The Platform Society. Public Values in a Connective World*, Oxford University Press, Oxford, 2018.
P. Dobias, K. Christensen, *The 'Grey Zone' and Hybrid Activities*, in *Connections: The Quarterly Journal*, 2022.
J. Dyck, et al., *Social Media, Political News, and Turnout*, in *Journal of Information Technology & Politics*, v. 16, n. 4, 2019.
U. Eco, *A Theory of Semiotics*, Indiana University Press, Bloomington, 1976.
J. Ellul, *Propaganda: The Formation of Men's Attitudes (1962)*, Vintage Books, New York, 1973.
M. Empler, C. Capasso, *Metodi e tecniche di monitoraggio web: analisi dei contenuti online*, in S. Sassi, A. Sterpa (a cura di), *Minacce ibride alla sicurezza nazionale. Disinformazione e migrazioni*, Editoriale Scientifica, Napoli, 2025.
C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, Milano, 1958.
V. Eymann, A.K. Beck, T. Lachmann, S. Jaarsveld, D. Czernochowski, *Reconsidering Divergent and Convergent Thinking in Creativity – a Neurophysiological Index for the Convergence-Divergence Continuum*, in *Creativity Research Journal*, v. 38, n. 2, 2026.
J. Fabian, *Time and the Other: How Anthropology Makes its Object*, New York, 1983.
P. Farwell, R. Rohozinski, *Stuxnet and the future of Cyber War*, 2011.
L. Ferrajoli, *Poteri selvaggi. La crisi della democrazia italiana*, Laterza, Roma-Bari, 2011.
F. Ferrara, *Manuale di diritto consolare*, Padova, 1936.
M. Ferraris, *Documanità. Filosofia del mondo nuovo*, Laterza, Roma-Bari, 2021.
P. Fiore, *Nuovo diritto internazionale pubblico secondo i bisogni della civiltà moderna*, Milano, 1865.
M. Fitzduff, *Our brains at war: The neuroscience of conflict and peacebuilding*, Oxford University Press, Oxford, 2021.

L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina, Milano, 2017,

L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, *AI4People: An Ethical Framework for a Good AI Society. Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, v. 28, n. 4, 2018.

Fondazione Luigi Einaudi (a cura di), *Difesa: l'industria necessaria*, 2025.

G. Fontana, *Sfera pubblica digitale e democrazia nell'Unione europea. Prime considerazioni intorno alla dichiarazione europea sui diritti e i principi digitali*, in R. Torino, S. Zorzetto (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Giappichelli, Torino, 2023.

G. Formigoni, *Storia della politica internazionale nell'età contemporanea*, Bologna, 2006.

F. Fornari, *Psicoanalisi della guerra*, Milano, 1966.

E. Fourneret, B. Yvert, *Digital Normativity: A Challenge for Human Subjectivation*, in *Frontiers in Artificial Intelligence*, 2020.

L. Freedman, *The Future of War*, Penguin, 2019.

L. Freedman, *Command: The Politics of Military Operations from Korea to Ukraine*, Oxford University Press, Oxford, 2023.

T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in Dir. Inf., 2020.

T.E. Frosini, *L'orizzonte giuridico dell'intelligenza artificiale*, in Dir. Inf., 2022.

T. E. Frosini, *Liberté, egalité, internet*, Editoriale Scientifica, Napoli, 2023.

F. Fu, N.A. Christakis, J.h. Fowler, *Dueling biological and social contagions*, in Scientific Reports, v. 7, n. 1, 2017.

M. Fuhrmann, *Antiextremismus und wehrhafte Demokratie. Kritik am politischen Selbstverständnis der Bundesrepublik Deutschland*, Nomos, Baden-Baden, 2019.

M. Fumaroli, *La repubblica delle lettere*, Milano, 2018.

G. Torode E J. Pomfret, *Chinese captain pleads not guilty to Baltic Sea cable damage*, Reuters, 11 febbraio 2026, www.reuters.com.

M. Galeotti, *The Weaponisation of Everything*, Yale University Press, New Haven, 2022.

V. García Pineda, A. Valencia-Arias, F.e. López Giraldo, E.a. Zapata-Ochoa, *Integrating artificial intelligence and quantum computing: A systematic literature review of features and applications*, in International Journal of Cognitive Computing in Engineering, v. 7, 2026.

S. Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly Media, Sebastopol, 1994.

A. Garrigues Walker, L.m. González De La Garza, *El derecho a no ser engañado. Y cómo nos engañan y nos autoengañamos*, Arazandi, Navarra, 2020.

A. Gatti, *La democrazia che si difende. Studio comparato su una pratica costituzionale*, Cedam, Padova, 2023

A. Gatti, *Liberal Democracies and Religious Extremism. Rethinking Militant De-*

mocracy through the German Constitutional Experience, in Diritto Pubblico Comparato ed Europeo, n.1, 2021.
A. Gatti, *Profilazione e diritti fondamentali: modelli a confronto: Europa, Usa, America Latina*, Editoriale Scientifica, Napoli, 2025.
A. Gatti, M. Giannelli, *Presupposti per la configurazione e la dichiarazione di guerra cibernetica*, in *DPCE Online*, v. 63, n. speciale 1, 2024.
V. Genin, *Le laboratoire belge du droit international. Une communauté épistémique et internationale de juristes (1869-1914)*, Bruxelles, 2018.
A.L. George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*, US Institute of Peace Press, Washington, 1991.
G. Ghidini, D. Manca, A. Massolo, *La nuova civiltà digitale. L'anima doppia della tecnologia*, Milano, 2020.
A. Giardina, *Art. 78*, in G. Branca, a cura di, *Commentario della Costituzione*, Bologna-Roma, Zanichelli-Foro it., 1979.
K. Giles, *Moscow Rules: What Drives Russia to Confront the West*, Brookings Institution Press, Washington, 2019.
T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, New Haven, 2018.
F. Giorgino, *Alto volume. Politica, comunicazione e potere*, LUISS University Press, Roma, 2019.
M.C. Girardi, *Libertà e limiti della comunicazione nello spazio digitale*, in *federalismi.it*, n. 17, 2024.
L. Gisel, T. Rodenhauser, E.K. Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, in *Internation reviw of the Red Cross,* 2020.
M. Gombar, *Algorithmic Manipulation and Information Science: Media Theories and Cognitive Warfare in Strategic Communication*, in *European Journal of Communication and Media Studies*, v. 4, n. 2, 2025.
G. Gozzi, *Diritti e civiltà. Storia e filosofia del diritto internazionale*, Bologna, 2010.
K. Gradon, J.A. Hołyst, W.R. Moy, J. Sienkiewicz, K. Suchecki, *Countering misinformation: A multidisciplinary approach*, in *Big Data & Society*, v. 8, n. 1, 2021.
T. Greco, *Pace. Critica della ragione bellica*, Roma-Bari, 2024.
D. Grimm, *Die Zukunft der Verfassung II. Auswirkungen von Europäisierung und Globalisierung*, Frankfurt am Main, 2012.
U. Grozio, *De iure belli ac pacis* (1625), Indianapolis, 2005.
U. Grozio, *Mare liberum* (1609), Napoli, 2007.
Y. Gu, S. Gu, Y. Lei, H. Li, *From uncertainty to anxiety: How uncertainty fuels anxiety in a process mediated by intolerance of uncertainty*, in *Neural Plast*, n. 1, 2020.

T. Guerini, *Fake News e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020.
U. Gulettad, *Human-stupidy-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *federalismi.it*, n. 5, 2023.
A.A. Gümüsay, *Embracing religions in moral theories of leadership*, in Academy of Management Perspectives, v. 33, n. 3, 2019.
L. Győri, C. Molnár, P. Krekó, P. Szicherle, *The Kremlin's troll network never sleeps*, Political Capital, Budapest, 2022.
J. Habermas, *Fatti e norme*, Laterza, Roma-Bari, 1996.
J. Habermas, *Storia e critica dell'opinione pubblica (1962)*, Laterza, Roma-Bari, 2006.
S. Halperin, *Imperial city states, National States and Post-National Spatialities*, in S. Halperin, R. Palan (a cura di), *Legacies of Empire. Imperial Roots of the Contemporary Global Order*, Cambridge, 2015.
B.-C. Han, *Nello sciame. Visioni del digitale*, Nottetempo, Roma, 2015.
B.-C. Han, *Psicopolitica. Il neoliberismo e le nuove tecniche del potere*, Nottetempo, Roma, 2016.
B.-C. Han, *Infocrazia. Le nostre vite manipolate dalla rete*, Einaudi, Torino, 2021.
I. Haney-López, *Dog whistle politics: How coded racial appeals have reinvented racism and wrecked the middle class*, Oxford University Press, Oxford, 2014.
Y.N. Harari, *Nexus. Breve stoia delle reti di informazione dall'età della pietra all'IA*, Bompiani, Milano, 2024.
C. Hassen, C. Pinelli, *Disinformazione e democrazia. Populismo, rete e regolazione*, Marsilio, Venezia, 2022.
E. Haven, A.I. Khrennikov, *Quantum social science*, Cambridge University Press, New York, 2013.
W. Heffter, *Le droit international de l'Europe*, Paris, 1873.
A. Henschke, *Cognitive warfare: Grey matters in contemporary political conflict*, Routledge, London, 2024.
M. Hildebrandt, *Smart Technologies and the End(s) of Law*, Cheltenham, 2015.
C. Hine, *Virtual Ethnography*, SAGE Publications, London, 2000.
F.H. Hinsley, A. Stripp (a cura di), *Codebreakers: The Inside Story of Bletchley Park*, Oxford University Press, Oxford, 1993.
T. Hobbes, *Leviatano (1651)*, Laterza, Roma-Bari, 2011.
F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, 2007.
J. Hornung, *Civilisés et Barbares*, in *Revue de droit international et de législation comparée*, 1885-1886.
S. Horowitz, *International Law and State. Transformation in China, Siam, and the Ottoman Empire during the Nineteenth Century*, in *Journal of World History*, 2004.
L. Huang, Q. Zhu, *Cognitive security: A system-scientific approach*, Springer, Berlin, 2023.

J. Huang, G. Epping, J.S. Trueblood, J.M. Yearsley, J.R. Busemeyer, E.M. Pothos, *An overview of the quantum cognition research program*, in *Psychonomic Bulletin & Review*, v. 32, 2025.

J. Huizinga, *La crisi della civiltà*, Torino, 1972.

E. Iannario, A. Sterpa, *Quando le autocrazie sfidano la forma di stato liberal-democratica: riflessioni a margine del recente "editto" russo*, in *federalismi.it*, n. 28, 2024.

A. Iannotti, *Libertà di espressione e valori democratici alla prova dei social media: il DSA e un nuovo caso TikTok europeo*, in *federalismi.it*, n. 2, 2025.

F. Ibrahim, S. Rhode, M. Daseking, *A systematic review of cognitive and psychological warfare*, in *The Defence Horizon Journal,* 2023.

M. Ienca, R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sciences Society and Policy*, v. 13, n. 1, 2017.

P. Iezzi, *Cyber e Potere*, Milano 2023.

P. Iezzi, G. Fusco, *Hackerare la mente*, Milano 2026, in corso di pubblicazione.

P. Iezzi, R. Razzante, *Algoritmo criminale. Come mafia, cyber e AI riscrivono le regole del gioco*, Milano 2024.

M.B. Ilyas, *The impact of artificial intelligence on hybrid warfare: Case of Russia-Ukraine war*, in *Journal of Liaoning Technical University*, v. 17, n. 11, 2023.

N. IRTI (voce), *Geodiritto*, in *Enciclopedia Italiana – VII Appendice*, 2007, www.treccani.it.

L.G. Jacobs, *Misinformation, Social Media, and Opportunities for Content-Based Regulation within the Constraints of the United States Constitution's Free Speech Guarantee,* 55 *U. Pac. L. Rev.*, 2024.

Y. Jadeja, K. Dudha, *Advancements in the Brain Chip Technology: Current Landscape and Future Prospects*, in Analytical & Bioanalytical Electrochemistry, v. 17, n. 2, 2025.

B. Johansen, *Leaders Make the Future: Ten New Leadership Skills for an Uncertain World*, Berrett-Koehler, San Francisco, 2009.

N. Johnson, S. Jajodia, *Exploring Steganography: Seeing the Unseen*, in IEEE Computer, v. 31, n. 2, 1998.

J. Johnson, *Artificial intelligence and the future of warfare: The USA, China, and strategic stability*, Manchester University Press, Manchester, 2021.

R.A. Jones, *Defamation, Disinformation, and the Press Function,* in *Journal of Free Speech Law*, v. 3, 2023.

D. Kahn, *The Codebreakers. The Story of Secret Writing*, Scribner, New York, 1996.

D. Kahneman, *Thinking, Fast and Slow*, Farrar, Straus and Giroux, New York, 2011.

D. Kahneman, A. Tversky, *Choices, Values, and Frames*, Cambridge University Press, Cambridge, 2000.

T. Kayaoğlu, *Legal Imperialism: Sovereignty and Extraterritoriality in Japan, the Ottoman Empire, and China*, Cambridge, 2010.
D. Kennedy, *International Law and the Nineteenth Century: History of an Illusion*, in *Nordic Journal of International Law*, 1996.
M. S. Khan, F.A. Rana, Z. Irfan, *Hybrid warfare in the digital age: Cyberpower, AI, and the future of global security*, in *Advance Social Science Archive Journal*, v. 4, n. 1, 2025.
H. A. Kissinger, E. Schmidt, D. Huttenlocher, *The Age of AI, Little, Brown*, New York, 2021.
H. Kissinger, *World Order*, Penguin Press, New York, 2014.
J.K. Kleffner, *Section IX of the ICRC Interpretive Guidance on Direct Participation in Hostilities: The End of Jus in Bello Proportionality as We Know It?*, in *Israel Law Review*, v. 45, n. 1, 2012.
J.L. Klüber, *Droit des gens moderne de l'Europe*, Paris, 1819.
M. Koskenniemi, *The Gentle Civilizer of Nations: The Rise and Fall of International Law 1870-1960*, Cambridge, 2002.
S. Kowalczuk, *Shock da Libertà. La Germania, l'Est e l'ascesa dell'estremismo*, Donzelli, Roma, 2025.
F. Kralj Novak, T. Smailović, B. Sluban, I. Mozetič, *Sentiment of Emojis*, in PLOS ONE, v. 10, n. 12, 2015.
S.D. Krasner, *Sovereignty: Organized Hypocrisy*, Princeton, 1999.
S.D. Krasner, *Westphalia and All That*, in J. Goldstein, R.o. Keohane (a cura di), *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change*, Ithaca, 1993.
H. Kumar, J. Vincentius, E. Jordan, A. Anderson, *Human Creativity in the Age of LLMs: Randomized Experiments on Divergent and Convergent Thinking*, in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 2025.
L. Lacchè (a cura di), *«Ius gentium ius communicationis ius belli». Alberico Gentili e gli orizzonti della modernità. Atti del Convegno di Macerata*, Milano, 2009.
F. Lanchester, *Stato (forme di)*, in *Enciclopedia del diritto*, Giuffrè, Milano, v. 43, 1990.
H.D. Lasswell, *The Structure and Function of Communication in Society*, in L. Bryson (a cura di), *The Communication of Ideas*, Harper, New York, 1948.
G. Le Bon, *La psychologie des foules*, 1895.
S. Lewandowsky, J. Cook, U.K.H. Ecker et al., *The Debunking Handbook 2020*, George Mason University – Center for Climate Change Communication, Fairfax, 2020.
S. Lewandowsky, S. van der Linden, *Countering misinformation and fake news through inoculation and prebunking*, in *European Review of Social Psychology*, v. 32, n. 2, 2021.

F. Lieber, *Instructions for the Government of Armies of the United States in the Field (General Orders No. 100, Adjutant General's Office, 1863)*, Washington, 1898.

P.M.A. Linebarger, *Psychological Warfare*, Infantry Journal Press, Washington, 1948.

K. Loewenstein, *Militant Democracy and Fundamental Rights*, in *American Political Science Association*, v. 31, n. 3, 1937.

W. Loewer, *Wehrhafte Demokratie*, in C. Hillgruber, C. Waldhoff (a cura di), *60 Jahre Bonner Grundgesetz*, Vandenhoeck & Ruprecht, Göttingen, 2010.

E. Longo, *"Digital Services Act" – Libertà di informazione. Libertà di informazione e lotta alla disinformazione nel "Digital Services Act"*, in *Giorn. Dir. amm.*, n. 6, 2023.

M.J. Lorimer, *La doctrine de la reconnaissance, fondement du droit international*, in *Revue de droit international et de législation comparée*, 1884.

M.J. Lorimer, *The Institutes of the Law of Nations*, Edinburgh and London, 1883.

M. Luciani, *Il segreto di Stato nell'ordinamento nazionale* in *Gnosis, Quaderno di intelligence*, n. 2, 2013.

O. Lungescu, *Germany will 'strike back' against Russian cyber attacks, minister vows*, Financial Times, 26 gennaio 2026, www.ft.com.

C. Maathuis, W. Pieters, J. Van Den Berg, *Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations*, 2018.

G. Magi, *I 36 stratagemmi*, Newton Compton, Roma, 2014.

L. Maikel, *Cognitive mapping variants and their training algorithms*, in *Computer Science Review*, v. 59, 2026.

G. Maira, *Il cervello è più grande del cielo*, Solferino, Milano, 2019.

M. Maksimovic, I.S. Maksymov, *Quantum-Cognitive Neural Networks: Assessing Confidence and Uncertainty with Human Decision-Making Simulations*, in *Big Data Cognitive Computing*, v. 9, n. 12, 2025.

M. Maksimovic, I.S. Maksymov, *Transforming Neural Networks into Quantum-Cognitive Models: A Research Tutorial with Novel Applications*, in *Technologies*, v. 13, n. 5, 2025.

M.V. Malinconi, *A War to Reality: deepfake e profili di sicurezza*, in S. Sassi, A. Sterpa (a cura di), *Minacce ibride alla sicurezza nazionale,* Editoriale Scientifica, Napoli, 2025.

A. Malkopoupou, L. Norman, *Three Models of Democratic Self-Defence: Militant Democracy and Its Alternatives*, in *Political Studies*, v. 66, n. 2, 2018.

S. Mannoni, *Potenza e ragione. La scienza del diritto internazionale nella crisi dell'equilibrio europeo (1870-1914)*, Milano, 1999.

M. Martin, *Why we fight*, Hurst & Co, London, 2018.

N. Matteucci, *Organizzazione del potere e libertà. Storia del costituzionalismo moderno*, il Mulino, Bologna, 2016.

J.E. Márquez-Díaz, *Integration of artificial intelligence in hybrid warfare strategies*, SSRN, 2025.
G. Martino, *La quinta dimensione della conflittualità: il cyberspazio*, Centro Studi Strategici Internazionali e Imprenditoriali, 2021.
C. Masala, *Bedigt abwehrbereit. Deutschlands Schwäche in der Zeitenwende*, C.H. Beck, München, 2023.
T. Mastrobuoni, *La peste. Indagine sulla destra in Germania*, Feltrinelli, Bologna, 2025.
J. Matthes, M. Hirsch, M. Stubenvoli, A. Binder, S. Kruikemeier, S. Lecheler, L. Otto, *Understanding the democratic role of perceived online political micro-targeting: longitudinal effects on trust in democracy and political interest*, in *Journal of Information Technology & Politics*, 2022.
J.N. Mattis, F.G. Hoffman, *Future Warfare: The Rise of Hybrid Wars*, in *US Naval Institute*, 2005.
M.J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle Barracks, 2015.
F. Mc Laughlin, *The Linguistic Ecology of the Sahel*, in S. Decalo (a cura di), *The Oxford Handbook of the African Sahel*, Oxford University Press, Oxford, 2021.
L. Mcintyre, *On Disinformation. How to Fight for Truth and Protect Democracy*, MIT Press, Cambridge-MA, 2023.
R. Menotti, M. Sgroi, *La sfida della democrazia. Strategie per il migliore dei mondi possibili*, Licosia, Ogliastro Cilento, 2025.
G.E. Merino, *Hybrid world war and the United States–China rivalry*, in *Frontiers in Political Science*, v. 4, 2023.
A. Merkel, *Libertà!*, Kiepenheuer & Witsch, Köln, 2024.
M. Mezza, *Net-war. Ucraina: come il giornalismo sta cambiando la guerra*, Donzelli, Roma, 2022.
M. Mezza, *Guerre in codice. Come le intelligenze artificiali resettano la democrazia*, Roma 2025.
M. Mezzanotte, *Fake news, deepfake e sovranità digitale nei periodi bellici*, in federalismi.it, n. 33, 2022.
M. Milanovic, P. Webb, *False Speech,* in A. Clooney, D. Neuberger (a cura di), *Freedom of Speech in International Law*, Oxford, OUP, 2024.
J.S. Mill, *Saggio sulla libertà (1859)*, Milano, 1981.
H. Miller, D. Thebault-Spieker, S. Chang, I. Johnson, L. Terveen, B. Hecht, *«Blissfully happy» or «ready to fight»: Varying interpretations of Emoji*, in *Proceedings of ICWSM*, 2016.
L. Mocci Guicciardi, *Gli investimenti cinesi in Africa Sub-Sahariana. Implicazioni geopolitiche, strategiche e di sicurezza*.
F. Modugno, *I "nuovi diritti" nella giurisprudenza costituzionale*, Giappichelli, Torino, 1995.

D.W. Moore, *Measuring New Types of Question-Order Effects: Additive and Subtractive*, in *The Public Opinion Quarterly,* v. 66, n. 1, 2002.
L. Moran, *Fighting Disinformation,* in *A.B.A. Journal*, v. 106, 2020,
A. Morelli, *Principi elementari della propaganda di guerra. Utilizzabili in caso di guerra fredda, calda o tiepida*, Ediesse, Roma, 2005.
E. Morin, *La tête bien faite*, Seuil, 1999.
C. Mosca, *Democrazie e intelligence italiana*, Editoriale Scientifica, Napoli, 2018.
W.R. Moy, K.t. Gradon, *Artificial intelligence in hybrid and information warfare: A double-edged sword*, in *Artificial intelligence in hybrid and information warfare*, 2022.
J.-W. Mueller, *Verfassungspatriottismus*, Suhrkamp, Frankfurt am Main, 2024.
M. Mueller, *Misinformation about Disinformation?*, www.internetgovernance.org.
R. Mulcahy, R. Barnes, R. De Villiers Scheepers, S. Kay, E. List, *Going Viral: Sharing of Misinformation by Social Media Influencers*, in *Australasian Marketing Journal*, 2025.
T. Naff, *The Ottoman Empire and the European States System*, in H. Bull, A. Watson (a cura di), *The Expansion of International Society*, Oxford, 1984.
K. Nakamura, G. Tita, D. Krackhardt, *Violence in the 'Balance': A Structural Analysis of How Rivals, Allies, and Third Parties Shape Inter Gang Violence*, Research Showcase @CMU, Heinz College Research, 2011.
E. Nakashima, *Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say*, The Washington Post, 24 marzo 2022, www.washingtonpost.com.
S. Narula, *Psychological Operations (PSYOPs): A Conceptual Overview*, in *Strategic Analysis*, v. 28, n. 1, 2004.
G. Neppi Modona, *La giurisprudenza costituzionale italiana in tema di leggi di emergenza contro il terrorismo, la mafia e la criminalità organizzata* in T. Groppi, *Democrazia e terrorismo*, Editoriale Scientifica, Napoli, 2006.
T. Nichols, *The Death of Expertise*, Oxford University Press, 2017.
A. Nicita, *Il Mercato delle Verità. Come la disinformazione minaccia la democrazia*, Il Mulino, Bologna, 2021.
C. Novelli, L. Floridi, S. Larsoon, M. Taddeo, S.L. Winter, *The Artificial in "Artificial Intelligence": How Imagination Shapes AI Regulation*, Center for Digital Ethics, 2026.
F. Nunez, *Disinformation Legislation and Freedom of Expression,* in *UC Irvine Law Review,* v. 10, n. 2, 2020.
E. Nurullah, B. Suheyl, *Deepfake Disinformation, Digital Law Rev.*, v. 6, 2024.
L. Nuzzo, *Autonomia e diritto internazionale. Una lettura storico-giuridica*, in *Quaderni fiorentini*, 2014.
L. Nuzzo, *Da Mazzini a Mancini: il principio di nazionalità tra politica e diritto*, in *Giornale di Storia Costituzionale*, 2007.

L. Nuzzo, *La colonia come eccezione. Un'ipotesi di transfer*, in *Rechtsgeschichte*, 2006.

L. Nuzzo, *Origini di una scienza. Diritto internazionale e colonialismo nel XIX secolo*, Frankfurt am Main, 2012.

J. Nye, *Soft Power: The Means to Success in World Politics*, PublicAffairs, New York, 2004.

J. Nye, *The Future of Power*, PublicAffairs, New York, 2011.

Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, 2024.

Y. Onuma, *When was the Law of International Society Born? An Inquiry of the History of International Law from an Intercivilizational Perspective*, in *Journal of the History of International Law*, 2000.

F.M.E. Oosprong, P.A.L. Ducheine, B.M.J. Pijpers, *Armed Attack in Cyberspace: Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands' Right of Self-Defence*.

D. Orrell, *The value of value: A quantum approach to economics, security and international relations*, in *Security Dialogue*, v. 51, n. 5, 2020.

A. Osiander, *The State System of Europe 1640-1990. Peacemaking and the Conditions of International Stability*, Oxford, 1994.

J. Ostherammel, N.P. Petersson, *Storia della globalizzazione*, Bologna 2005.

D. Pal, D. Sau, *Quantum Computing: Threat to Cybersecurity*, in Quantum Computing, in S.B. Goyal, V. Kumar, S.M.N. Islam, D. Ghai (a cura di), *Cyber Security and Cryptography*, Springer, Singapore, 2025.

V. Palleti, S. Adepu, V. Mishra, et al., *Cascading effects of cyber-attacks on interconnected critical infrastructure*, in *Cybersecurity*, n. 4, 2021.

C. Panattoni, *Considerazioni sul diritto della pace e della guerra, sopra i Congressi degli Amici della pace, tenuti in Francoforte ed in Londra*, Firenze, 1851.

E. Parisier, *The Filter Bubble: What the Internet Is Hiding from You*, Viking, London, 2011.

A. Park, *The Battle against Disinformation: Legislative Challenges in South Korea*, in R.J. Krotoszynski Jr., A. Koltay, C. Garden (a cura di), *Disinformation, Misinformation and Democracy*, Cambridge University Press, Cambridge, 2024.

F. Paruzzo, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, ESI, Napoli, 2022.

S. Paul, N.R. Choudhury, B. Pandit, A. Dawn, *Integration of AI and Quantum Computing in Cybersecurity: A Comprehensive Review*, in B.K. Mishra (a cura di), *Integration of AI, Quantum Computing, and Semiconductor Technology*, IGI Global Scientific Publishing, Hershey, 2024.

C.S. Peirce, *Collected Papers*, Harvard University Press, Cambridge, 1931-1958.

G. Pennycook, D.G. Rand, *The Psychology of Fake News*, in *Trends in Cognitive Sciences*, v. 25, n. 5, 2021.

G. Perticone, *Stato (teoria generale)*, in *Novissimo Digesto Italiano*, v. XVII.
E.M. Photos, J.R. Busemeyer, *Quantum Cognition*, in *Annual Review of Psychology*, v. 73, 2022.
G.P. Pierini, *The Legal Framework for Psychological Operations and Influence Operations Under International Law, the Law Applicable to Armed Conflict and International Criminal Law*, in *Rassegna della giustizia militare*, 2020, www.giustiziamilitare.difesa.it.
A. Pillet, *Le Droit International Public. Ses éléments constitutifs, son domaine, on objet*, in *Revue Général de Droit International Public*, 1894.
A. Pin, *Libertà di coscienza e intelligenza artificiale*, in *Coscienza e libertà*, n. 67, 2024.
G. Pitruzzella, O. Pollicino, *Disinformation and Hate Speech. A European Constitutional Perspective*, Egea, Milano, 2020.
P. Pomerantsev, *This Is Not Propaganda: Adventures in the War Against Reality*, PublicAffairs, New York, 2019.
A. Ponsonby, *Falsehood in War-Time*, George Allen & Unwin, London, 1928.
K. Popper, *Tutta la vita è risolvere problemi*, Bompiani Editore, Milano, 2001.
P. Pradier-Fodéré, *Traité de droit international public Européen & Américain suivant les progrès de la science et de la pratique contemporaines*, Paris, 1885.
E. Prati, *È possibile quantizzare le relazioni internazionali?*, in Id. (a cura di), *Quantum Diplomacy*, Centro Studi Americani, Roma, 2022.
E. Prati, *Introduzione*, in Id. (a cura di), *Quantum Diplomacy*, Centro Studi Americani, Roma, 2022.
E. Prati, *Tecnologie quantistiche e relazioni internazionali*, in Id. (a cura di), *Quantum Diplomacy*, Centro Studi Americani, Roma, 2022.
I. Pujol, Q. Dinh, *The battle for the mind: understanding and addressing cognitive warfare and its enabling technologies*, IE CGC, 2024.
A. Qadir, *Quantum economics*, in Pakistan Economic and Social Review, v. 16, n. 3/4, 1978.
P. Qiu, S. Zhou, E. Ferrara, *Information suppression in large language models: Auditing, quantifying, and characterizing censorship in DeepSeek*, in *Information Sciences*, 2026.
Rand Corporation, *The Emerging Domain of Cognitive Warfare*, RAND Corporation, Santa Monica, 2021.
A. Rapisardi-Mirabelli, *Storia dei trattati e delle relazioni internazionali*, Milano, 1940.
M. Raska, *Hybrid Warfare with Chinese Characteristics*, RSIS Commentary, 2015.
W. Rech, *Enemies of Mankind. Vattel's Theory of Collective Security*, Leiden, 2013.
Redazione, *Come l'IA neuromorfica e i modelli fondazionali stanno ridefinendo il panorama delle minacce alla cybersecurity*, in *ICT Security Magazine*, 2025.
G.U. Rescigno, *Forme di Stato e forme di governo*, in *Enc. Giur.*, Roma, Treccani, 1989.

E. Resta, *Le regole della fiducia*, Roma-Bari, Laterza, 2009 e Id., *Il diritto fraterno*, Laterza, Roma-Bari, 2005.
G. Resta, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. Trim. Dir. Pubbl.*, n. 4, 2022.
G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. Trim. Dir. Pubbl.*, 4, 2022.
T. Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, New York, 2020.
T. Rid, *Cyber War Will Not Take Place*, Oxford University Press, Oxford, 2013.
T. Rid, *Misure attive. Storia segreta della disinformazione*, trad. it., Luiss University Press, Roma, 2022.
E.F. Risko, S.J. Gilbert, *Cognitive offloading*, in *Trends in Cognitive Sciences*, v. 20, n. 9, 2016.
R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, in *Communications of the ACM*, v. 21, n. 2, 1978.
S. Rodotà, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012
S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997.
G. Rolin-Jaequemyns, *Note sur la théorie du droit d'intervention, a propos d'une lettre de M. le professeur Arntz*, in *Revue de droit international et de législation comparée*, 1876.
S. Romano, *L'ordinamento giuridico*, Sansoni, Firenze, 1977.
S. Romanosky, Z. Goldman, *Understanding Cyber Collateral Damage*, in *Procedia Computer Science*, v. 95, 2016.
J. Roozenbeek, C.S. Traberg, S. van der Linden, *Technique-based Inoculation against Real-world Misinformation*, in *Royal Society Open Science*, v. 9, n. 5, 2022.
J. Roozenbeek, S. van der Linden, B. Goldberg, S. Rathje, S. Lewandowsky, *Psychological Inoculation Improves Resilience against Misinformation on Social Media*, in *Science Advances*, v. 8, n. 34, 2022.
J. Roozenbeek, S. van der Linden, *How to Combat Health Misinformation: A Psychological Approach*, in *American Journal of Health Promotion*, v. 36, n. 3, 2022.
H. Rosa, *Accelerazione e alienazione*, Einaudi, Torino, 2015.
C. Rudschies, I. Schneider, *The Long and Widing Road to Bans for Artificial Intelligence: From Public Pressure and Regulatory Initiatives to the EU AI Act*, in *Digital Society*, n. 4, 2025.
F. Rugge, *Il «contesto intransigente». Appunti sulla storia di un postulato*, in Id. (a cura di), *Il trasferimento internazionale dei modelli istituzionali*, Bologna, 2012.
G.E. Rusconi, *Dove va la Germania. La sfida della nuova destra populista*, Il Mulino, Bologna, 2019.

H.A. Sale, *Monitoring Facebook*, in *Harvard Business Law Review*, v.12, n. 2, 2022

T. Santamato, *L'IA cambia la cybersicurezza*, in La Sicilia, 1° settembre 2025.

G. Santomartino, *Conoscere e contrastare il jihadismo*, Panda, Trento, 2020

G. Santomartino, *Storia del pensiero sulla guerra e la pace dalla Bibbia al Jihadismo*, Panda, Trento, 2022.

S. Sassi, *Disinformazione contro Costituzionalismo*, Editoriale Scientifica, Napoli, 2021.

S. Sassi, *Il ruolo della disinformazione nelle moderne strategie di guerra*, in E.A. Imparato, G. Giorgini Pignatiello (a cura di), *La libertà di espressione nel diritto comparato tra stato di diritto e stati di emergenza*, Giappichelli, Torino, 2024.

S. Sassi, A Sterpa (a cura di), *Minacce Ibride alla sicurezza nazionale. Disinformazione e migrazioni*, Editoriale Scientifica, Napoli, 2025.

S. Sassi, A Sterpa., *La Corte costituzionale della Romania difende la democrazia liberale dalla disinformazione. Prime note sulla sentenza n. 32 del 6 dicembre 2024*, in *federalismi.it*, n. 4, 2025.

C.R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton, 2017.

W. Schaeuble, *Erinnerungen. Mein Leben in der Politik*, Klett-Cotta, Stuttgart, 2024.

T.C. Schelling, *Arms and Influence*, Yale University Press, New Haven, 1966.

U. Schliesky, *Die wehrhafte Demokratie des Grundgesetzes*, in: J. Isensee, P. Kirchhof (a cura di), *Handbuch des Staatsrechts*, Müller Verlag, Erlangen, 2014.

S. Schmid, D. Lambach, C. Diehl, C. Reuter, *Arms Race or Innovation Race? Geopolitical AI Development*, in *Geopolitics 2025*.

C. Schmitt, *Il nomos della terra nel diritto internazionale dello «jus publicum europaeum» (1974)*, Milano, 1991.

M.N. Schmitt (a cura di), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017.

B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, Wiley, New York, 2000.

G. Sciannella, *Intelligenza artificiale, politica e democrazia*, in *DPCE online*, n. 1, 2022.

D. Shah, S. Jain, T. Bhatt, C. De Armas, A. Karbasi, *Bridging Nodes and Narrative Flows: Identifying Intervention Targets for Disinformation on Telegram*, in arXiv preprint, 2024.

C. Shannon, *A Mathematical Theory of Communication*, in *Bell System Technical Journal*, v. 27, n. 3–4, 1948.

N. Shapira, C. Wendler, A. Yen, G. Sarti, K. Pal, O. Floody, A. Belfki, A. Loftus, A.R. Jannali, N. Prakash, J. Cui, G. Rogers, J. Brinkmann, C.

Rager, A. Zur, M. Ripa, A. Sankaranarayanan, D. Atkinson, R. Gandikota, J. Fiotto-Kaufman, E.J. Hwang, H. Orgad, P.S. Sahil, N. Taglicht, T. Shabtay, A. Ambus, N. Alon, S. Oron, A. Gordon-Tapiero, Y. Kaplan, V. Shwartz, T.R. Shaham, C. Riedl, R. Mirsky, M. Sap, D. Manheim, T. Ullman, D. Bau, *Agents of Chaos*, 2021.

M.R. Shoaib, Z. Wang, M. Taleby Ahvanooey, J. Zhao, *Deepfake, Misinformation, and Disinformation in the Era of Frontier AI, Generative AI, and Large AI Models*, in *International Conference on Computer Applications*, 2023.

B. Simma, D.-E. Khan, G. Nolte, G. Paulus, *The Charter of the United Nations – A Commentary*, v. 1, Oxford, 2012.

A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1, 2019.

A. Simoncini., *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in internet*, Milano, 2017.

A. Simoncini, E Longo., *Digital Constitutionalism and Fundamental Rights: Reconfiguring Liberty and Power*, in G. De Gregorio, O. Pollicino, P. Valke (a cura di), *The Oxford Handbook of Digital Constitutionalism*, Oxford University Press, Oxford, 2026.

G. Simpson, *Great Powers and Outlaw States: Unequal Sovereigns in the International Legal Order*, Cambridge, 2004.

P.W. Singer, E.T. Brooking, *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, 2018.

Small Wars Journal, *Cognitive Warfare Without a Map: Why Current Targeting Logic Fails*, www.smallwarsjournal.com, 2026.

A. Smith, *The Theory of Moral Sentiments*, London, 1761.

Q. Song, W. Wang, W. Fu, Y. Sun, D. Wang, Z. Gao, *Research on quantum cognition in autonomous driving*, in *Scientific Reports*, v. 12, n. 300, 2022.

A. Soro, *Persone in Rete. I dati tra poteri e diritti*, Fazi, Roma, 2018.

V. Sorrentino, *Il segreto e la menzogna in politica: Hannah Arendt*, in Studium, n. 6, 1995.

A. Stazi, *Legal big data: prospettive applicative in ottica comparatistica*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, il Mulino, Bologna, 2020.

A. Sterpa, *Commento all'art. 126 Cost.*, in F. Clementi, L. Cuocolo, F. Rosa, G. Vigevani (a cura di), *La Costituzione italiana. Commento articolo per articolo*, il Mulino, Bologna, v. 2, 2021.

A. Sterpa, I. De Vivo, C. Capasso, *L'ordine giuridico dell'algoritmo: la funzione regolatrice del diritto e la funzione ordinatrice dell'algoritmo*, in *Nuovi autoritarismi e democrazie. Diritto, istituzioni, società*, n. 2, 2023.

A. Sterpa, *Il "saluto romano" tra divieto di ricostituzione del partito fascista e difesa dei valori costituzionali* in *Rivista giuridica delle forze armate e di polizia*, Jovene, n. 2, 2024.

A. Sterpa, *L'ordine giuridico dell'algoritmo: un nuovo ordinamento giuridico* in A. Sterpa (a cura di), *L'ordine giuridico dell'algoritmo*, Editoriale Scientifica, Napoli, 2024.

A. Sterpa, *La difesa della democrazia dalle minacce ibride. Teoria della comunità, dell'autorità, del potere e delle migrazioni: elementi per un'analisi strategica della "guerra tiepida"*, Editoriale Scientifica, Napoli, 2025.

A. Sterpa, *La libertà di comunicazione digitale, il potere e il costituzionalismo*, in M.E. Bucalo, M. Caporale, A. Sterpa (a cura di) *Diritto pubblico di internet*, Editoriale Scientifica, Napoli, 2024.

A. Sterpa, *Quando le élite falliscono nelle società libere* in Id. (a cura di), *Il fallimento delle élite*, Giubilei Regnani, Cesena, 2025.

A. Sterpa, C. Capasso, *Empty squares, empty billboards, empty dashboards, and semi-empty ballots: the "political" european elections in the global election year*, T. incerruti, F. savastano (a cura di), *the european parliament elections in 2024*, Giappichelli, Torino, 2024.

B. Stiegler, *Taking Care of Youth and the Generations*, Stanford University Press, Stanford, 2010.

J. Styczynski, N.E. Beach-Westmoreland, *When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure*, Booz Allen Hamilton, 2016.

C. R. Sunstein, *#Repubblic. La democrazia nell'epoca dei social media*, Il Mulino, Bologna, 2017.

N. Süsa, *The Historical Interpretation of the Origin of the Capitulations in the Ottoman Empire*, Baltimore, 1930.

E. Șușnea, I.-C. Buță, *Artificial intelligence in hybrid warfare: A literature review and classification*, in *Proceedings of the 16th International Scientific Conference "Strategies XXI"*, 2021.

C.R. Sustein, *Liars. Falsehood and Free Speech in Age of Deception*, OUP, Oxford, 2021.

E.C. Tandoc Jr., Z.W. Lim, R. Ling, *Defining «Fake News»: A Typology of Scholarly Definitions*, in *Digital Journalism*, v. 6, n. 2, 2018.

N.N. Taleb, *Antifragile. Things That Gain from Disorder*, Random House, New York, 2012.

N.N. Taleb., *Il Cigno nero. Come l'improbabile governa la nostra vita*, Il Saggiatore, Milano, 2008.

R. Tarchi, *Democrazia e istituzioni di garanzia*, in *Rivista AIC,* n. 3, 2018.

B.C. Taylor, H. Bean (a cura di), *The handbook of communication and security*, Routledge, London, 2019.

S. Tchakhotine, *Le viol des foules par la propagande politique (1939)*, Gallimard, Paris, 1952.

R. Thangamani, *Securing the Future: Quantum Computing in Cybersecurity*, in R. Thangamani, M. Vimaladevi, G.K. Kamalam, K.M. Subramanian (a cura

di), *Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategies*, Springer Nature, Singapore, 2025.

M. Thiel, *The "Militant Democracy" Principle in Modern Democracies*, Routledge, London, 2016.

P. Thiel, *Il momento straussiano*, Liberilibri, Macerata, 2025.

S. Tiribelli, *Identità personale e algoritmi*, Carocci, Roma, 2023.

T. Todorov, *I nemici intimi della democrazia*, Garzanti, Milano, 2012.

L. Torchia, *Lo Stato digitale. Una introduzione*, il Mulino, Bologna, 2023.

B. Török, *The Fight against Disinformation in the Council of Europe, and the Relevant Case Law of the European Court of Human Rights*, in R.J. Krotoszynski Jr., A. Koltay, C. Garden (a cura di), *Disinformation, Misinformation, and Democracy: Legal Approaches in Comparative Context*, Cambridge University Press, Cambridge, 2025.

C.S. Traberg, J. Roozenbeek, S. van der Linden, *Psychological Inoculation against Misinformation: Current Evidence and Future Directions*, in *The Annals of the American Academy of Political and Social Science*, v. 700, n. 1, 2022.

A. Tversky, D. Kahneman, *Extensional Versus Intuitive Reasoning: The Conjunction Fallacy in Probability Judgment*, in *Psychological Review*, v. 90, n. 4, 1983.

S. Tyulkina, *Militant Democracy. Undemocratic Political Parties and Beyond*, Routledge, London, 2015.

M.i. Ul Haq, N. Ul Hassan, D.q. Rizvi, Umama, *Nano-scale architectures for quantum AI robotics: A review of emerging trends in neuromorphic chip design, advanced medical diagnostics, and cybernetic enhancements*, in Spectrum of Engineering Sciences, v. 9, 2016.

M. Valentini, *Sicurezza della Repubblica e democrazia costituzionale*, Editoriale Napoli, Scientifica, 2017.

A. Valeriani, *Twitter factor*, Laterza, Roma-Bari, 2011.

S. van der Linden, *Foolproof: Why Misinformation Infects Our Minds and How to Build Immunity*, W.W. Norton & Company, New York, 2023.

P. Vareta, H. Muzenda, T. Nyamupaguma, Y. Dube, B. Ndlovu, *The Rise of Quantum Computing and Its Impact on Cybersecurity*, in *The Indonesian Journal of Computer Science*, v. 8, n. 1, 2025.

M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act: Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, in *Computer Law Review International*, v. 22, n. 4, 2021.

G. Vernetti, *Il nuovo grande gioco. Dal Giappone all'Ucraina. Viaggio lungo la frontiera fra libertà e autoritarismo*, Solferino, Milano, 2025.

N. Viceconte, *Segreto di Stato*, in C. Bassu, G. Pistorio, A. Sterpa (a cura di), *Diritto pubblico della sicurezza*, Editoriale Scientifica, Napoli, 2023.

U. Villani-Lubelli, *L'ascesa di Alternative für Deutschland. Origine e conseguenze politiche e istituzionali*, in L. Rapone (a cura di), *Le destre europee nel XXI secolo. Eredità e mutamenti*, Carocci, Roma, 2026, (in corso di stampa).

U. Villani-Lubelli, *La Repubblica Federale tedesca e la difesa della democrazia (wehrhafte Demokratie) tra l'ascesa dell'estrema destra e crisi dei partiti tradizionali*, in *Nuovi Autoritarismi e Democrazia: Diritto, Istituzioni e Società*, v. 7, n. 1, 2025.

U. Villani-Lubelli, *Nationalism Against Europeanisation: The Challenge of Far-Right Populism for European Democracy. A Comparison of Italy and Gerany*, in C. Liermann Traniello, M. Scotto, J. Stefanlli (a cura di), *Stati Uniti d'Europa: Auspicio, incubo, utopia?*, Villa Vigoni Editore, Loveno di Menaggio, 2020.

E. Volokh, *When Are Lies Constitutionally Protected?*, 2022, www.knightcolumbia.org.

C. von Clausewitz, *Della guerra (*1832), Mondadori, Milano, 2009.

C. von Martens, *Le guide diplomatique. Précis des droits et des fonctions des agents diplomatiques et consulaires suivi d'un Trait. des Actes et Offices divers qui sont du ressort de la Diplomatie, accompagné de pièces et documents proposés comme exemples*, Leipzig, 1866.

T. von Schmalz, *Das europäische Völker-Recht*, Berlin (1817), Frankfurt am Main, 1970.

S. Vosoughi, D. Roy, S. Aral, *The Spread of True and False News Online*, in *Science*, v. 359, n. 6380, 2018.

M. Wacket, *German authorities to get more powers against foreign hackers, draft law shows*, Reuters, 27 febbraio 2026, www.reuters.com.

O.J. Waddup, J.m. Yearsley, P. Blasiak, E.M. Pothos, *Temporal Bell inequalities in cognition*, in *Psychonomic Bulletin & Review*, v. 30, 2023.

O. Wæver, *Securitization and Desecuritization*, Centre for Peace and Conflict Research, Copenhagen, 1993.

Z. Wang, J.R. Busemeyer, H. Atmanspacher, E.M. Pothos, *The Potential of Using Quantum Theory to Build Models of Cognition*, in *Topics in Cognitive Science*, v. 5, n. 4, 2013.

C. Wardle, *Understanding Information Disorder*, First Draft, New York, 2019.

C. Wardle, H. Derakhshan, *Information disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe, 2017.

J. Watling, N. Reynolds, *Ukraine at War: Paving the Road from Survival to Victory*, Royal United Services Institute, London, 2023.

M. Weber, *Economia e società* (1922), Edizioni di Comunità, Milano, v. 1, 1961.

M. Weber, *La scienza come professione. La politica come professione (1919)*, Einaudi, Torino, 2004.

S. Wenwei, M. Weiwei, Z. Jiachen, L. Xiaohong, M. Dong, *Opportunities and Challenges of Brain-on-a-Chip Interfaces*, in *Cyborg and Bionic Systems*, v. 6, 2025.

H. Wheaton, *Elements of International Law with a sketch of the History of the Science*, Philadelphia, 1836.

L.C. White, E.M. Pothos, J.R. Busemeyer, *Insights from quantum cognitive models for organizational decision making*, in *Journal of Applied Research in Memory and Cognition*, v. 4, n. 3, 2015.

J. Qc Wright, *Cyber and International Law in the 21st Century*, Discorso al Chatham House, 23 maggio 2018, www.gov.uk.

J.M. Yearsley, J.R. Busemeyer, *Quantum cognition and decision theories: A tutorial*, in Journal of Mathematical Psychology, v. 74, 2016.

J.M. Yearsley, E.M. Pothos, *Challenging the classical notion of time in cognition: a quantum perspective*, in *Proceedings of the Royal Society B*, v. 281, n. 1781, 2014.

D.C. Youvan, *Quantum-Inspired Cognition: A Unified Model of Learning, Thinking, and Memory in Biological and Artificial Intelligence*, 2025.

V.I. Yukalov, *Evolutionary processes in quantum decision theory*, in *Entropy*, v. 22, n. 6, 2020.

G. Zagrebelsky, *Diritti per forza*, Einaudi, Torino, 2017.

V. Zeno Zencovich, *Big data e epistemologia giuridica*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, il Mulino, 2020.

D. Zolo, *Chi dice umanità. Guerra, diritto e ordine globale*, Torino, 2000.

S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019,

S. Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, New York, 2019.

Finito di stampare nel mese di maggio 2026
dalla *Vulcanica srl* - Nola (Na)

ISBN 979-12-235-0697-4

euro 30,00