

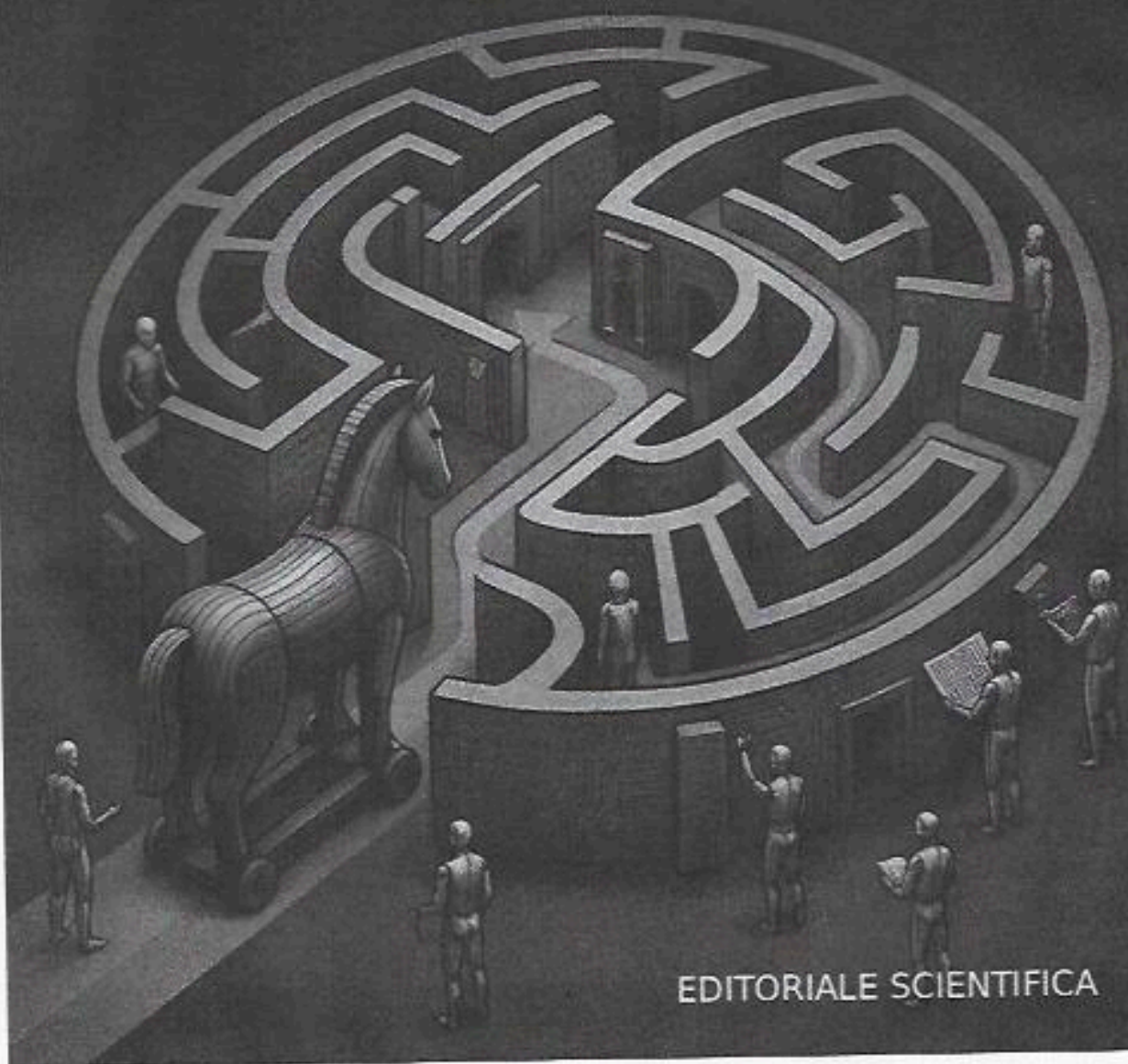
# GUERRA COGNITIVA E SICUREZZA NAZIONALE

## Profili giuridici e istituzionali

a cura di

**Roberto Sgalla**

**Alessandro Sterpa**



EDITORIALE SCIENTIFICA

GUERRA COGNITIVA E SICUREZZA NAZIONALE  
PROFILI GIURIDICI E ISTITUZIONALI

ES

# GUERRA COGNITIVA E SICUREZZA NAZIONALE

*Profili giuridici e istituzionali*

a cura di  
ROBERTO SGALLA e ALESSANDRO STERPA

EDITORIALE SCIENTIFICA



UNIVERSITÀ  
della TUSCIA

DIPARTIMENTO DI  
ECONOMIA, INGEGNERIA,  
SOCIETÀ E IMPRESA



CENTRO STUDI  
AMERICANI

*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.*



algo-freedom society

[www.algofreedomociety.it](http://www.algofreedomociety.it)

*Proprietà letteraria riservata*

© Copyright 2026 Editoriale Scientifica s.r.l.  
Via San Biagio dei Librai, 39 – 80138 Napoli  
[www.editorialescientifica.it](http://www.editorialescientifica.it) [info@editorialescientifica.com](mailto:info@editorialescientifica.com)

ISBN 979-12-235-0697-4

# INDICE

|                                                                                                                                                         |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <i>Introduzione a cura di Roberto Sgalla e Alessandro Sterpa</i>                                                                                        | 7   |
| <i>Il dominio cognitivo e la minaccia ibrida di Vittorio Rizzi</i>                                                                                      | 9   |
| <i>Minaccia ibrida e offensività multidominio: la cybersicurezza a tutela della democrazia di Bruno Frattasi</i>                                        | 21  |
| <i>La Costituzione e la "nuova guerra": Stato e individuo nella guerra cognitiva di Alessandro Sterpa</i>                                               | 29  |
| <i>Tra autorità e libertà: la minaccia nell'ecosistema digitale di Victor Maximilian Hartl</i>                                                          | 53  |
| <i>Forma di Stato e guerre cognitive: la difesa delle democrazie liberali nell'era delle minacce ibride di Antonio Teti</i>                             | 67  |
| <i>Elementi di riflessione per una lettura normativa della guerra cognitiva di Claudia Capasso</i>                                                      | 79  |
| <i>From Battlefields to Browsers: Neuroscienze e AI nella Guerra Socio-Cognitiva di Arije Antinori</i>                                                  | 97  |
| <i>Oltre il campo di battaglia: la weaponizzazione del cyberspazio e la protezione dei civili nel diritto internazionale umanitario di A. Calabrese</i> | 117 |
| <i>Dal codice nascosto al codice migrante: evoluzione della crittografia non convenzionale di Michele Empler</i>                                        | 141 |
| <i>I dati personali come infrastruttura della guerra cognitiva. Proposte per una risposta istituzionale di Andrea Gatti</i>                             | 159 |
| <i>Dalla diplomazia dei gabinetti alla guerra cognitiva: diritto internazionale, opinione pubblica e trasformazione del conflitto di Eliana Augusti</i> | 179 |
| <i>La sicurezza nazionale nella Repubblica Federale tedesca: strategie di difesa e tenuta istituzionale di Ubaldo Villani Lubelli</i>                   | 201 |
| <i>La sfida della disinformazione nell'ecosistema digitale europeo di Silvia Sassi</i>                                                                  | 221 |



## Prospettive operative

|                                                                                                                                                                                                            |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <i>La dimensione cognitiva della guerra ibrida</i> di Andrea Manciulli                                                                                                                                     | 233 |
| <i>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</i> di Michele Empler | 245 |
| <i>La mente quale obiettivo strategico: la difesa della dimensione cognitiva attraverso lo sviluppo del pensiero critico</i> di Massimo Panizzi                                                            | 271 |
| <i>Conflitti e confini immateriali. Violenza ibrida, propaganda e governo del caos</i> di Vincenzo D'Anna                                                                                                  | 283 |
| <i>Dalla disinformazione al sabotaggio nell'era digitale: guerra cognitiva, IA agente e sovranità del dato</i> di Pierguido Iezzi                                                                          | 301 |
| <i>Imprese e istituzioni nella guerra ibrida: difendere la reputazione come infrastruttura critica</i> di Gianluca Giansante                                                                               | 313 |
| <i>Quantum Cognitive Warfare</i> di Fabrizio De Longis                                                                                                                                                     | 325 |
| <i>Minacce ibride alla sicurezza nazionale. Disinformazione e migrazioni</i> di Laura Lega                                                                                                                 | 353 |
| Bibliografia                                                                                                                                                                                               | 369 |

## LA SFIDA DELLA DISINFORMAZIONE NELL'ECOSISTEMA DIGITALE EUROPEO

Silvia Sassi\*

SOMMARIO: 1. Introduzione. – 2. La natura sistemica della disinformazione e la sua dimensione tecnologica. – 3. Disinformazione e guerra ibrida. – 4. Il modello normativo europeo e le sue criticità. – 5. Alcune conclusioni.

### 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<sup>1</sup>. 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<sup>2</sup>, 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.

<sup>1</sup> 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. PRIRUZZELLA, 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, *Lies. 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 University 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. MCINTYBE, *On Disinformation. How to Fight for Truth and Protect Democracy*, MIT Press, Cambridge-MA, 2023.

<sup>2</sup> 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. CARUTTA DI TORITTO, *Principi costituzionali e intelligenza artificiale*, ora in Id., *Lecture di diritto costituzionale*, Giappichelli, Torino, 2020; A. D'ALOMA, *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<sup>3</sup>. In tale contesto, la disinformazione assume una portata sistemica, tale da essere qualificata, in taluni casi e da alcuni ordinamenti giuridici<sup>4</sup>, 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<sup>5</sup>. Come evidenziato di recente dalla dottrina<sup>6</sup>, 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"<sup>7</sup>. 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.

<sup>3</sup> Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaello Cortina, 2017; S. ZUBOV, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, Luiss, 2019; A. SIMONCINI, *L'algoritmo costituzionale: 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.

<sup>4</sup> 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.internetgovernance.org](http://www.internetgovernance.org).

<sup>5</sup> A. BUCCARIO, *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. MAITIS, F.G. HOFFMAN, nel loro articolo dal titolo *Future Warfare: The Rise of Hybrid Wars*, in *US Naval Institute*, 132(11), 2005, pp. 1 ss.

<sup>6</sup> 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.

<sup>7</sup> Al riguardo v. l'ultimo rapporto NATO: J.M. BLATNY, S. SONDERGAARD, *Cognitive Warfare*, 2025.



sticati; dall'altro, l'obbligo di preservare i diritti fondamentali, *in primis* la libertà di espressione<sup>8</sup>. Il presente contributo intende analizzare tale tensione, esaminando la configurazione giuridica della disinformazione in particolare nell'ordinamento europeo<sup>9</sup>, 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<sup>10</sup>. 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»<sup>11</sup>, per porre in evidenza due dimensioni essenziali:

<sup>8</sup> Cfr. F. NÚÑEZ, *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.

<sup>9</sup> Su alcuni dei differenti approcci nazionali alla lotta alla disinformazione cfr.: J. CHARNY, *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. KROTUSZYNSKI, 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>.

<sup>10</sup> 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.

<sup>11</sup> 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<sup>12</sup>. Al riguardo l'Unione europea ha più volte ribadito che la disinformazione, in quanto tale, non può essere considerata illegale, ma legale e dannosa<sup>13</sup>. 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<sup>14</sup>.

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.

<sup>12</sup> Tra i primi che misero l'accento su queste differenti disfunzioni nella informazione: C. WARDLE, H. DERAKSHIAN, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe report DGI(2017)09, 2017. Di recente v. B. TÓBÓK, *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.

<sup>13</sup> 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.

<sup>14</sup> 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<sup>13</sup>. 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.*

<sup>13</sup> 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<sup>16</sup>.

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<sup>17</sup>. 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

<sup>16</sup> 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.

<sup>17</sup> Interessante il recente rapporto a cura di W. BROWN, J. KOEZOVA, 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<sup>18</sup>, che trova i suoi pilastri principali nel Digital Services Act (DSA) e nell'AI Act<sup>19</sup>.

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<sup>20</sup>.

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<sup>21</sup>. Anche in

<sup>18</sup> 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. FLORELLI, 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.

<sup>19</sup> 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.F. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. Inf.*, 2022 e D.U. GALETTA, *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *federalismi.it*, 5, 2023.

<sup>20</sup> 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. LANNOTTI, *Libertà di espressione e valori democratici alla prova dei social media: il DSA e un nuovo caso TikTok europeo*, in *federalismi.it*, 2, 2025.

<sup>21</sup> 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. RUDOLPH, L. SCHNEIDER, *The Long and Winding 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<sup>22</sup>. Nel loro complesso, tali strumenti delineano un modello di "costituzionalismo digitale"<sup>23</sup>, 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<sup>24</sup>. 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.

<sup>22</sup> L'esempio più significativo dell'IA sulla disinformazione è il *deepfake*: su questo tema cfr.: M.R. SHOAB, 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. NUBUL-LAH, B. SUTHEYL, *Deepfake Disinformation*, 6 *Digital L. Rev.* 321, 2024.

<sup>23</sup> Sul costituzionalismo digitale v. per tutti: T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. Inf.*, 2020.

<sup>24</sup> V. ZENO ZENCONICH, *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.<sup>25</sup>

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<sup>26</sup>: quella di garantire le condizioni di un dibattito pubblico libero e informato in un ambiente tecnologico che tende, strutturalmente, a comprometterle<sup>27</sup>.

<sup>25</sup> 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. POLICINO, E. APA, M. BASSINI, (a cura di), *op. cit.*

<sup>26</sup> V. T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, cit. Per un abbinamento costituzionalismo e disinformazione cfr. S. SASSI, *Disinformazione contro Costituzionalismo*, cit.

<sup>27</sup> 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.