JURA

Temi e problemi
del diritto

STUDI

discipline civilistiche
discipline penalistiche - Criminalia
discipline pubblicistiche
filosofia del diritto
storia del diritto

TESTI

CLASSICI

collana diretta da

Italo Birocchi, Marcello Clarich,
Aurelio Gentili, Fausto Giunta,
Mario Jori, Vito Velluzzi

La nozione di contenuto illecito online

Fattispecie e responsabilità penale nella prospettiva europea

a cura di
Kolis Summerer, Matteo L. Mattheudakis, Gian Marco Caletti

con la collaborazione di
Paolo Beccari

Edizioni ETS

www.edizioniets.com

Il volume è stato pubblicato con il finanziamento del Trust & Safety Research Award di Google.

EDIZIONI ETS
Palazzo Roncioni - Lungarno Mediceo, 16, I-56127 Pisa
info@edizioniets.com
www.edizioniets.com

Distribuzione
Messaggerie Libri SPA
Sede legale: via G. Verdi 8 - 20090 Assago (MI)

Promozione
PDE PROMOZIONE SRL
via Zago 2/2 - 40128 Bologna

ISBN cartaceo 978-884677392-0

INDICE

PREFAZIONE

Il presente volume trae origine dal progetto di ricerca dal titolo *Leveling the Field. Clarifying the Notion of Illegal Content under the EU's Digital Services Act - CliC*, condotto presso la Libera Università di Bolzano e presso l'Università di Bologna.

Il progetto è stato finanziato nel 2023 da *Google* nell'ambito del programma *Trust & Safety Research Award,* dedicato al sostegno di ricercatori impegnati a promuovere, mediante la tecnologia, un impatto positivo sulla società. Il programma, attraverso finanziamenti non vincolanti, favorisce ricerche volte a migliorare la fiducia, la sicurezza, la privacy e la protezione in tutto l'ecosistema digitale, accogliendo proposte provenienti da una vasta gamma di discipline: dall'informatica al diritto, dalle scienze sociali alla psicologia, dalle politiche pubbliche all'interazione uomo-macchina.

Abbiamo colto questa preziosa occasione per porci un obiettivo ambizioso: contribuire alla chiarificazione concettuale e sistematica della nozione di contenuto illecito nel diritto dell'Unione europea, con particolare riguardo al *Digital Services Act* (Regolamento UE 2022/2065). La nostra ricerca approfondisce lo studio dei principali fenomeni criminosi contro la persona che vengono realizzati online, proponendosi di rileggere le fattispecie collegate con una vocazione anche interdisciplinare e di respiro internazionale.

In tale cornice si sono collocati due momenti di confronto scientifico di importante rilievo: il Convegno nazionale dal titolo *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea*, svoltosi a Bologna il 29 e 30 novembre 2024, dal quale prende avvio e titolo il presente volume, e il Simposio internazionale dal titolo *The Notion of Illegal Content in the EU Digital Age*, tenutosi a Merano (BZ) il 18 e 19 settembre 2025, le cui suggestioni confluiranno in una pubblicazione internazionale.

La competenza delle relatrici e dei relatori coinvolti nel dibattito e la ricchezza dei loro contributi ci ha consentito di delineare fondamenta solide, articolate e non prive di spunti problematici intorno al punto di partenza del nostro progetto, volto all'implementazione delle disposizioni della nuova disciplina sui servizi digitali, secondo una prospettiva squisitamente penalistica.

Nell'offrire agli studiosi, agli operatori e a tutti gli interessati questo primo lavoro di lettura e inquadramento delle fattispecie nell'ordinamento italiano, desideriamo esprimere un sincero ringraziamento a tutte le autrici e a tutti gli autori che vi hanno contribuito con i loro scritti, nonché alle colleghe e ai colleghi stranieri che hanno sin qui partecipato con entusiasmo alle nostre iniziative, arricchendo il dialogo scientifico con le loro prospettive internazionali.

Un doveroso ringraziamento va, inoltre, a *Google* per l'opportunità di questa ricerca e il sostegno al progetto e a Edizioni ETS per la paziente cura editoriale e la preziosa collaborazione nella pubblicazione dell'opera.

Meritano, infine, il nostro sentito ringraziamento i componenti del gruppo di ricerca, il Dott. Gian Marco Caletti e il Dott. Paolo Beccari, per l'importante contributo scientifico e organizzativo prestato nell'ambito del progetto e nelle fasi di lavorazione del volume.

Bolzano-Bologna, 13 novembre 2025

I coordinatori del progetto di ricerca
Kolis Summerer e Matteo L. Mattheudakis

INTRODUZIONE

Con il nuovo Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e recante modifica della direttiva 2000/31/CE (c.d. *Digital Services Act* o *DSA*), in vigore dal 25 agosto 2023 e pienamente operativo dal 17 febbraio 2024, l'Unione europea ha riformato profondamente il proprio quadro normativo dei servizi digitali, con l'obiettivo di garantire una maggiore protezione dei consumatori, della privacy degli utenti e della libertà di espressione online.

Il legislatore di Bruxelles, a poco più di vent'anni dall'originaria disciplina europea sul commercio elettronico, ha inteso "chiudere un cerchio", predisponendo un nuovo e articolato regime di responsabilità per i gestori di piattaforme di intermediazione digitale, nella consapevolezza di quanto il ruolo di quest'ultimi fosse ormai «sempre più distante dalla conformazione normativa che per prima la direttiva 2000/31 aveva delineato», basata sul presupposto di «una neutralità operativa in funzione di un'ipotetica equidistanza tra fornitori di contenuti e utenti»[1], sul modello del "buon Samaritano" statunitense[2].

Da tempo, infatti, il marcato attivismo nella c.d. «*content moderation*»[3] da parte degli *Internet Service Providers*, svolto nell'ambito delle proprie piattaforme e segno di un'era di «capitalismo della sorveglianza»[4], non rendeva più ragione del binomio consolidatosi tra neutralità e irresponsabilità di tali prestatori per contenuti illeciti diffusi da terzi[5].

[1] L'osservazione è di O. POLLICINO, *Tutela del Pluralismo nell'era digitale, ruolo e responsabilità degli Internet Service Provider*, in «Percorsi costituzionali», 1(2014), p. 454.

[2] Si allude alla celebre *Section 230* del *Communications Decency Act* del 1996, che dalla fine dello scorso Millennio postulavala distinzione tra creatore del contenuto e *Internet Service Providers*, garantendo a quest'ultimo una sostanziale immunità dalla giurisdizione civile e penale anche nel caso di intervento operato sul contenuto in buona fede per limitarne la diffusione (e, dunque, alla stregua del "buon Samaritano" di evangelica memoria). Cfr. *47 U.S. Code* § 230 (c) (1): «*TREATMENT OF PUBLISHER OR SPEAKER. – No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*». In argomento, J. KOSSEFF, *The Twenty-Six Words That Created the Internet*, Cornell University Press, New York, 2019.

[3] Sul termine, *ex multis*, F. WILMAN, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*, Edward Elgar Publishing, Cheltenham, 2020, p. 246 ss.

[4] Il termine, come noto, è coniato da S. ZUBOFF, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, in «Journal of Information Technology», 30 (2015), p. 75 ss., ed EAD., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019.

[5] Lo rileva M. MANETTI, *Libertà di pensiero e anonimato in Rete*, in «Diritto dell'informazione e dell'informatica», 2 (2014), p. 139.

Così, il Regolamento europeo ha predisposto una serie di obblighi di compliance in materia di trasparenza e *reporting*, valutazione preventiva dei rischi (c.d. *risk assessment*) e ricerca di soluzioni per la loro mitigazione, accesso ai dati per autorità e ricercatori (c.d. *disclosure*), gestione delle segnalazioni degli utenti, blocco e rimozione di contenuti illeciti e altri ancora, collegando l'inottemperanza di ciascuno a significative sanzioni pecuniarie.

Il ruolo cruciale delle procedure di compliance, fondato su un approccio *risk-based* e sul criterio dell'autoregolamentazione della piattaforma, ha gettato le basi per un'inedita forma di responsabilità nell'alveo della c.d. *secondary liability* degli *Internet Service providers*[6], che presenta significative ricadute sulla libertà di espressione online, a motivo di «un apparato sanzionatorio severo, ma nebuloso nella sua configurazione»[7].

A destare particolari insidie è stato proprio il presupposto di tale apparato, costituito dalla nozione di «contenuto illegale» di cui all'art. 3, lett. h *DSA*.

Se il *Digital Services Act* muove dal lineare principio per cui «ciò che è illegale offline dovrebbe esserlo anche online» («*what is illegal offline should be illegal online*»), la nuova disciplina europea appare piuttosto generale e carente nella sua definizione, descrivendo il contenuto illegale come «qualsiasi informazione che, di per sé o in relazione a un'attività, compresa la vendita di prodotti o la prestazione di servizi, non sia conforme al diritto dell'Unione o al diritto di uno Stato membro che sia conforme al diritto dell'Unione, indipendentemente dall'oggetto o dalla natura di tale legge». Si tratta di un concetto a dir poco ambiguo, che non può ritenersi dipanato neppure dal riferimento, nelle premesse al Regolamento europeo, a fenomeni specifici quali pedopornografia e incitamento all'odio[8].

Se infatti, da un lato, il diritto penale dell'Unione europea appare ancora "in costruzione"[9], è pur vero, dall'altro, che le legislazioni nazionali appaiono spesso lacunose e non sempre allineate, restituendo un quadro tutt'altro che univoco[10]. Ciò,

[6] In tema, G.B. Dinwoodie (a cura di), *Secondary Liability of Internet Service Providers*, Springer, Berlin, 2017.

[7] Così, con riferimento al *DSA*, F. Sarzana di Sant'Ippolito, *Le sanzioni nel* Digital Markets Act, in L. Bolognini, E. Pelino, M. Scialdone (a cura di), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Giuffrè Francis Lefebvre, Milano, 2023, p. 400.

[8] Rilevano la "confusione definitoria" A. Turillazzi, M. Taddeo, L. Floridi, F. Casolari, *The Digital Services Act: an analysis of its ethical, legal, and social implications*, in «Law, Innovation and Technology», 15/1 (2023), p. 94. Molto critico anche V. Zeno-Zencovich, *The EU regulation of speech. A critical view*, in «Media Laws - Rivista di diritto dei media», 1 (2023), p. 13, il quale, dopo aver apostrofato le normative europee contro i discorsi d'odio come una «macedonia» che spazia dal terrorismo alla pornografia minorile, rileva la confusione tra «*illegal*» e «*harmful*» nell'ambito del nuovo Regolamento, con serie ricadute sulla libertà di espressione.

[9] Sul tema, M. Bergström, V. Mitsilegas (a cura di), *EU Law in the Digital Age. Swedish Studies in European Law*, Hart Publishing, Oxford, 2025; J. Öberg, *The Normative Foundations for EU Criminal Justice. Powers, Limits and Justifications*, Hart Publishing, Oxford, 2024; A. Klip (a cura di), *Substantive Criminal Law of the European Union*, Maklu, Antwerpen, 2011.

[10] Viene alla mente la domanda di U. Sieber, M. Nolde, *Sperrverfügungen im Internet. Nationale Rechtsdursetzung im globalen Cyberspace?*, Duncker & Humblot, Berlin, 2008. Sulla necessità di armonizzare le sanzioni

peraltro, nonostante i più recenti e significativi tentativi del legislatore eurounitario di uniformare la tutela delle vittime di taluni fenomeni criminosi, come da ultimo avvenuto con la Direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica. Se tale normativa ha avuto il pregio di soffermarsi su alcune fattispecie assai rilevanti, concentrandovi nuovi obblighi di criminalizzazione per gli Stati membri, questi ultimi appaiono ancora lontani dalla loro effettiva implementazione.

Nella disomogeneità tra ordinamenti viene in gioco un catalogo amplissimo e potenzialmente infinito di ipotesi, a cominciare da quelle più classiche, con ben più di qualche cortocircuito normativo. La diffamazione, per esempio, costituisce reato in alcuni Paesi europei (tra cui l'Italia), ma non in altri (come Romania, Estonia, Cipro, Irlanda), dove da tempo configura un semplice illecito civile: in linea teorica, quindi, non è del tutto certo se ad essa debba farsi riferimento nel solco del "contenuto illecito" dell'Unione europea.

Inoltre, il dibattito su alcuni fenomeni criminali non è sviluppato in modo uniforme negli Stati membri, anche in quelli più avanzati, rispetto al contesto anglo-americano: per esempio, in ambito europeo alcuni ordinamenti non prevedono ancora un reato specifico sulla diffusione di immagini intime[11] e si è ben lontani da forme univoche di non punibilità nello scambio di materiale sessualmente esplicito tra minori d'età o, ancora, da una nozione condivisa di odio digitale[12].

Specularmente, anche la nozione di contenuto legale è interamente rimessa – con approccio pilatesco – nelle mani degli Stati membri: il *Considerando* 39 del Regolamento prevede, invero, la facoltà, in capo «alle competenti autorità giudiziarie o amministrative nazionali di emettere, sulla base del diritto dell'Unione o nazionale applicabile, un ordine di ripristino dei contenuti, qualora tali contenuti fossero conformi alle condizioni generali del prestatore di servizi intermediari, ma siano stati erroneamente considerati illegali da tale prestatore e siano stati rimossi».

Così, nell'arco di due decenni i prestatori di servizi digitali – per dirla con una perifrasi sufficientemente eloquente – sono divenuti «da responsabili per niente, responsabili per tutto»[13], indotti alla pronta cancellazione di qualsivoglia contenuto (presumibilmente) illecito o lecito, spesso anche attraverso il ricorso alle proprie *policies* private, pur di ottemperare a un meccanismo di responsabilità fuori dal perimetro della tipicità.

penali nell'ambito dell'Unione europea, H. SATZGER (a cura di), *Harmonisierung strafrechtlicher Sanktionen in der Europäischen Union*, Nomos, Baden-Baden, 2020.

[11] Sulle scelte di criminalizzazione dell'*intimate image abuse*, v. G.M. CALETTI, K. SUMMERER (a cura di), *Criminalizing Intimate Image Abuse: A Comparative Perspective*, Oxford University Press, Oxford-New York, 2024.

[12] Sul punto, v. A. NICITA, *Nell'età dell'odio. Sfera pubblica, intolleranza e democrazia*, il Mulino, Bologna, pp. 81-82, ove rileva, anche nell'alveo del Consiglio d'Europa, difformità tra la nozione di *hate speech* del 1997 e del 2022.

[13] P. BECCARI, Quis custodiet ipsos custodes*? La responsabilità delle piattaforme digitali per gli illeciti penali degli utenti. Modelli a confronto dal "*Good Samaritan*" statunitense al* Digital Services Act, in «Diritto penale contemporaneo - Rivista trimestrale», 3 (2025), § 6 (in corso di pubblicazione).

Appare, quindi, assolutamente necessario "livellare il campo", individuando definizioni condivise nello scenario europeo intorno ai contenuti illegali e penalmente rilevanti, superando la disarmonia delle molteplici legislazioni nazionali e cercando di riempire di significato la nozione delineata dal *DSA*. Tale sforzo non può che scaturire, in prima battuta, dalle singole esperienze nazionali, chiamate a rileggere le proprie fattispecie e a scioglierne i nodi esegetici, con particolare attenzione alle condotte che colpiscono le fasce più vulnerabili (tra cui donne e minori).

Nell'ambizioso obiettivo di individuare un vocabolario condiviso e un denominatore comune tra gli Stati membri dell'Unione, il presente volume si propone di offrire un'ampia visuale sulle principali fattispecie contro la persona nell'ordinamento italiano, muovendo da alcuni dei fenomeni più rilevanti tra quelli menzionati dal Regolamento europeo.

Nell'intento di offrire una trattazione lineare e analitica, l'opera si suddivide in tre parti.

Una prima sezione è dedicata ai profili giuridici dello spazio digitale e ai fondamenti teorici e normativi della responsabilità degli *Internet Service Providers*. Vengono affrontati in chiave regolatoria e penalistica i temi della cybersicurezza (anche in seguito alla recente legge n. 90/2024) e del paradigma delineato dal *Digital Services Act* nella gestione dei contenuti illeciti online, al quale lo sguardo può dirsi rivolto in prospettiva diacronica – nel confronto con la più risalente esperienza statunitense – e sincronica – nell'accostamento all'altrettanto recente *AI Act* europeo. Un particolare approfondimento è, inoltre, riservato alla complessa definizione di "contenuto illegale" nel diritto dell'Unione europea, anche a fronte del labile confine tra questa e la nozione di "contenuto dannoso".

Il lettore viene, così, introdotto alla seconda sezione, che esplora le nuove prospettive di offesa alla persona in ambito digitale, analizzando l'impatto delle c.d. *ICT* sulla tipologia di condotte lesive, prestando attenzione alle nuove modalità di aggressione, alla tutela della dignità e della riservatezza nell'ambiente virtuale e alle capacità del diritto penale e della giurisprudenza di fronteggiare tali fenomeni.

In particolare, un primo insieme di offese concerne i contenuti illeciti sessualmente espliciti e le molestie digitali, che portano alla luce le criticità interpretative e le sfide poste all'intervento penale. Vengono analizzati i profili giuridici della produzione e diffusione di materiale pedo-pornografico e materiali sessualmente espliciti raffiguranti adulti, le implicazioni del *sexting* e dei *deepfakes*, nonché il rilievo dei più recenti obblighi di incriminazione di matrice europea. La riflessione si estende, inoltre, ai fenomeni di cyberstalking e cyberbullismo, evidenziando la necessità di adattare le fattispecie tradizionali alla realtà digitale, e alle molestie sessuali in rete, che sollecitano una rinnovata attenzione alla tutela della libertà sessuale nella sua dimensione «incorporea»[14].

[14] In ripresa di B. PANATTONI, *Violazioni "incorporee" della sfera sessuale. Possibili evoluzioni ed insidie nell'ambito dei reati sessualmente connotati*, in «Archivio penale», 3 (2022), p. 1 ss.

Un secondo gruppo di fattispecie riguarda, invece, i c.d. discorsi offensivi, con particolare riguardo alla tutela della reputazione, al contrasto all'*hate speech* e ai fenomeni di disinformazione. L'analisi si incentra sulle difficoltà applicative delle tradizionali categorie penali alle offese online, ponendo l'accento sugli strumenti di regolazione previsti dal *Digital Services Act*. In tale contesto, la prospettiva si sposta inevitabilmente dal piano individuale a quello superindividuale, giacché la distorsione della parola è alla base della disinformazione e della manipolazione del consenso politico. Al diritto penale è affidato (anche attraverso i poteri privati delle piattaforme) il compito delicatissimo di trovare un punto di equilibrio tra repressione degli illeciti e garanzie di libertà e pluralismo nello spazio digitale[15].

Infine, la terza e ultima sezione del volume è dedicata alle vittime di violenza online e alle possibili strategie per la loro efficace protezione, nella prospettiva di un intervento multidimensionale e integrato, volto a garantire supporto, sicurezza e riconoscimento alle persone offese. Accanto ai tradizionali strumenti di prevenzione e repressione, la riflessione si estende anche al ruolo della giustizia riparativa come via complementare di ricomposizione del danno e di ricostruzione del legame sociale nello spazio virtuale, che coinvolge e responsabilizza sia la comunità di utenti sia i gestori di servizi e piattaforme.

Il quadro dei contributi così delineato intende avviare la costruzione di uno "standard comune" sul piano linguistico-ermeneutico e operativo, ancorché nazionale, in relazione ai contenuti potenzialmente illegali, contribuendo alla loro maggiore conoscibilità per incrementare, da un lato, la sicurezza degli utenti online e, dall'altro, la conformità da parte dei gestori di servizi e piattaforme agli obblighi previsti dal nuovo *Digital Services Act*.

Se è vero che il *Digital Services Act*, nella regolamentazione dello spazio digitale, può ancora definirsi «un punto di partenza piuttosto che di arrivo»[16], è pur vero che i tempi per la sua piena implementazione appaiono più che maturi, a cominciare dalle sue definizioni più basilari.

Paolo Beccari, Gian Marco Caletti,
Matteo L. Mattheudakis, Kolis Summerer

[15] Sul tema, C. Caruso, *La libertà di espressione in azione: contributo a una teoria costituzionale del discorso pubblico*, Bologna University Press, Bologna, 2013; A. Galluccio, *Punire la parola pericolosa? Pubblica istigazione, "discorso d'odio" e libertà di espressione nell'era di internet*, Giuffrè Francis Lefebvre, Milano, 2020; J. Horder, *Criminal Fraud and Election Disinformation: Law and Politics*, Oxford University Press, Oxford-New York, 2022.

[16] D. Keller, *The European Union's New DSA and the Rest of the World*, in J. van Hoboken, J.P. Quintais, N. Appelman, R. Fahy, I. Buri, M. Straub (a cura di), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, Verfassungsbooks, Berlin, 2023, p. 237, che lo ritiene esattamente «*a starting point, rather than an end point*».

SEZIONE 1

PROFILI GIURIDICI DELLO SPAZIO DIGITALE: SICUREZZA, RESPONSABILITÀ E CONTENUTI ILLECITI

PRIME RIFLESSIONI A MARGINE DELLA LEGGE N. 90/2024. CYBERCRIME E TUTELA PENALE DELLA CYBERSECURITY: UN'OCCASIONE PERSA?

Roberto Flor

SOMMARIO: 1. Introduzione. – 2. Cybersecurity e tutela penale. – 3. Semantica tecnica e componenti strutturali della definizione di cybersecurity.

1. *Introduzione*

Con la legge 28 giugno 2024, n. 90 ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici") il legislatore penale ha inteso apportare modifiche al sistema codicistico dei reati informatici.

Al di là della rilevanza mediatica di tale intervento, elevato alla stregua di un "giro di vite" contro il cybercrime, il suo impatto, sul piano del diritto penale sostanziale, appare davvero limitato ad un generale inasprimento della risposta sanzionatoria e a taluni "correttivi", fra cui, per citare solo alcuni esempi, l'introduzione di una nuova ipotesi di reato (art. 629, comma 3), nel tentativo di rispondere alla diffusione (soprattutto) di *cyber-attacks* "*ransomware*", di cui si dovranno attendere le prime applicazioni giurisprudenziali per vagliarne effettività ed efficacia, e l'abrogazione, in particolare, dell'art. 615-*quinquies* c.p. che, in verità, viene collocato fra i reati contro il patrimonio (*ex* art. 635-*quater*.1) con la previsione di due nuove circostanze aggravanti. Oppure si pensi al reato di truffa di cui all'art. 640 c.p., che viene arricchito da un ulteriore comma (2-*ter*), se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione. La l. n. 132/2025 appare rilevante, in questo contesto, in quanto lo sviluppo di sistemi e di modelli di intelligenza artificiale avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati. Le disposizioni in essa contenute, inoltre, sono volte a valorizzare l'intelligenza artificiale anche come risorsa per il rafforzamento della cybersicurezza nazionale.

Proprio al fine di garantire il rispetto dei diritti e dei princìpi espressi da tale atto normativo deve essere assicurata, quale precondizione essenziale, la cybersicurezza durante tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici

controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza.

Fra il resto la medesima legge ha introdotto alcune aggravanti speciali per "l'aver commesso il fatto mediante l'impiego di sistemi di i.a." e inserito, nel lungo elenco di circostanze previste all'art. 61, c. 1, c.p., l'aggravante comune di cui al n. 11-*decies*, che si applica ai casi in cui il fatto sia stato commesso «mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato».

Con il presente lavoro, alla luce dell'entrata in vigore della legge n. 90/2024, si intendono proporre, nei limiti consentiti dagli obiettivi perseguiti con questo volume, alcune riflessioni relative all'esigenza di tutela penale di beni giuridici di nuova o nuovissima generazione espressione altresì di innovative forme di manifestazione dei diritti fondamentali, quali la riservatezza informatica e la sicurezza informatica, tenendo ben presente che le proteiformi definizioni di "cybersecurity" dovrebbero incontrare, in un comune denominatore, le esigenze preventive e proattive rispetto alla stessa diffusione di contenuti illeciti, che troverebbe nelle piattaforme o nei servizi digitali dei vettori di amplificazione della loro viralità propagativa.

2. *Cybersecurity e tutela penale*

La c.d. cybersecurity, dunque, non può rappresentare solo una questione, o peggio un ostacolo, di ordine tecnico. Al contrario, la sua rilevanza nella costellazione sempre più variegata dell'ecosistema digitale la eleva ad una innovativa espressione dei diritti fondamentali e se non ad un diritto fondamentale. Questo approccio è confermato anche nella letteratura straniera, che sempre più spesso fa riferimento a «*Human-Centric Approach to Cybersecurity*»[1], oppure a «*Cybersecurity as a human rights*»[2] o, ancora, ponendosi la seguente questione, almeno nel panorama europeo: «*New right to cybersecurity?*»[3].

In effetti, mentre si assiste ad una generale condivisione sull'importanza della cybersecurity, non vi è consenso unanime relativamente all'approccio "metodologico", "contenutistico" e "definitorio" a tale concetto, almeno sul piano del diritto penale sostanziale.

[1] Deibert, *Toward a Human-Centric Approach to Cybersecurity*, Cambridge University Press, 2018.

[2] Shackelford, *Should Cybersecurity Be a Human Right? Exploring the 'Shared Responsibility' of Cyber Peace*, in «Stanford Journal of International Law» (2019), pp. 17-55.

[3] Chiara, *Towards a right to cybersecurity in EU law? The challenges ahead*, in «Computer Law & Security Review» (2024), p. 53, in cui l'Autore concentra l'analisi su *"three legal challenges brought about by a theoretical framework for development of a new right to cybersecurity. They regard: i) the need for a new right to cybersecurity against the background of the existing fundamental right to security (Art. 6 EU Charter of Fundamental Rights, CFR); ii) the actual content of this new right; and, iii) how such a new right could be implemented*".

Non è raro imbattersi, in letteratura, in argomentazioni che sovrappongono piano diversi, confondendo la cybersecurity nel contesto della sicurezza nazionale (se non internazionale) – ossia del perimetro di sicurezza cibernetica nazionale al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale – la cybersecurity nel contesto pubblico e la cybersecurity nel settore privato, ovvero *cyberscurity* intesa quale risultato di un processo organizzativo rispetto alle componenti strutturali del concetto stesso di cybersecurity.

La legge n. 90/2024 contiene, infatti, da un lato misure di rafforzamento della *cybersicurezza* nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario e, dall'altro lato, interventi nell'ambito dei reati informatici.

Si tratta di una legge che, per il vero, si inserisce in un contesto europeo in cui l'Unione europea stessa lavora su vari fronti per promuovere la resilienza informatica, ivi compresa la resilienza operativa digitale per il settore finanziario (si pensi solo, a titolo esemplificativo, al regolamento UE/2022/2554).

Dopo la legge n. 547/1993 (prima normativa in materia di cybercrime) e la legge n. 48/2008 (di attuazione della Convenzione del Consiglio d'Europa sulla criminalità informatica – Convenzione Cybercrime) non si è assistito ad ulteriori interventi di carattere sistematico, e tanto meno risponde a simile esigenza la legge n. 90.

La legislazione penale italiana *in subiecta materia*, infatti, è stata sin dall'origine caratterizzata da un insieme di norme incriminatrici eterogenee, frutto di interventi spesso settoriali o frammentari imposti, da un lato, dalla necessità di colmare alcune lacune emerse nella prassi applicativa, dall'altro lato di dare attuazione alle fonti internazionali ed europee.

Si pensi che per più di 30 anni l'art. 615-*ter* c.p., fattispecie fulcro nel micro-sistema dei reati informatici, non ha subito modifiche, tanto che si sono susseguite diverse tesi riguardanti il suo oggetto giuridico. È stato sostenuto, inizialmente, che la fattispecie tutelasse la privacy, intesa non più solo nel significato riduttivo di «*the right to be let alone*», il domicilio informatico, ovvero configurasse un reato plurioffensivo, a tutela anche dell'integrità del sistema, dei programmi, dei dati e delle informazioni. Il nostro legislatore poi, nel 2008, non ha ritenuto necessario modificare la formulazione originaria dell'art. 615-*ter* c.p., confermando pertanto le scelte di politica criminale degli anni '90.

Oggi, anche dopo il limitato intervento del legislatore del 2024 (vedi *infra*), l'individuazione dell'oggetto giuridico tutelato deve avvenire attraverso l'interpretazione sistematica e teleologica di questa fattispecie da porre in relazione ad altri reati, tra cui quelli *ex* artt. 615-*quater*, 617-*quater*, 617-*quinquies* e 617-*sexies* c.p.

Nell'era dell'interconnessione, della comunicazione globale e dell'infosfera, nonché dell'accessibilità e della fruibilità delle risorse attraverso la rete e qualsiasi strumento di

comunicazione anche mobile, lo "spazio informatico" è rapidamente passato da una dimensione privata o singola ad una "dimensione pubblica". In altri termini all'interesse del singolo si affianca quello super-individuale o di natura collettiva a che l'accesso a tali spazi, ai sistemi e ai dati informatici ed alla stessa rete avvenga per finalità lecite e in modo tale da essere regolare per la sicurezza degli utenti, pur mantenendosi quale «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost.» e strumentale per l'esercizio degli stessi diritti fondamentali dell'individuo.

Per cui, da un lato, è innegabile che una componente di tale "area riservata" riguardi la facoltà, il potere, il diritto del titolare di gestire in modo autonomo le utilità e le risorse del sistema informatico, nonché i contenuti delle comunicazioni informatiche (o telematiche), indipendentemente dalla loro natura; dall'altro lato, appare indispensabile un bilanciamento con le esigenze connesse alla "sicurezza informatica". Sia quest'ultima che la "riservatezza informatica", dunque, contribuiscono a delineare un livello anticipato e preventivo di protezione rispetto al momento dell'effettiva lesione dell'integrità delle informazioni, dei programmi o dei sistemi informatici, nonché alla presa di cognizione dei contenuti dei dati ivi archiviati o trattati, anche di natura riservata o segreta. Simile prospettiva di tutela, che valorizza i profili funzionali della sicurezza informatica, è direttamente rafforzata da dati normativi, espliciti ed autonomi. In primis, l'art. 615-*ter* c.p. offre protezione penale solo ai sistemi protetti da "misure di sicurezza". Le diverse tesi interpretative sul "ruolo" di tale elemento costitutivo convergono su almeno una argomentazione comune e insuperabile: la legge penale non definisce la natura delle misure protettive e non richiede che esse siano efficaci e idonee. A tali misure, dunque, il legislatore sembra aver ragionevolmente affidato il compito di manifestare lo *ius excludendi alios* del titolare dello spazio informatico. In secondo luogo, l'art. 615-*ter*, comma 2, n. 3, c.p. prevede un aumento della pena e la procedibilità d'ufficio se dal fatto derivi la «distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti». La legge n. 90/2024 ha apportato un sensibile inasprimento sanzionatorio per le ipotesi aggravate di cui al comma 2, prevedendo la pena della reclusione da 2 a 10 anni inserendo, proprio nell'ipotesi di cui al n. 3, dopo le parole: «ovvero la distruzione o il danneggiamento» le seguenti: «ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare».

Questa locuzione, da un lato e sul piano sistematico, pare voler rafforzare la già stretta connessione fra riservatezza, integrità e sicurezza informatiche, offese o messe in pericolo dalle condotte previste dall'art. 615-*ter* c.p. Dall'altro lato, il legislatore è caduto nel medesimo errore del legislatore del 2013 quando, questo ultimo, con la legge n. 119/2013 (di conversione con modificazioni del d.l. n. 93/2013) ha introdotto nell'art. 640-*ter* c.p. un nuovo comma, che sanziona ancora oggi la frode informatica commessa mediante sostituzione (furto o indebito utilizzo) dell'identità digitale in danno di uno o più soggetti. L'espressione "furto" di identità digitale sembra richiamare (impropria-

mente) le condotte di sottrazione e impossessamento previste dall'art. 624 c.p., che sono tecnicamente riferite ad un oggetto fisico-materiale, espresso dal termine "cosa".

Riproporre a più di 10 anni di distanza l'espressione "sottrazione […]" riferita ai dati sembra confermare un difetto di comprensione della "regola tecnologica", essendo i dati, per loro stessa natura, insuscettibili di sottrazione ed impossessamento.

La rapidità dell'evoluzione tecnologica ha sempre rappresentato una sfida per il diritto e, in particolare, per la legislazione e la giurisprudenza penale. Proprio la comprensione della regola tecnologica costituisce e probabilmente costituirà un fattore determinante, in quanto deve entrare nelle scelte di politica criminale, come la tecnologia entra e entrerà sempre più frequentemente fra gli strumenti investigativi e decisori, gli elementi costitutivi della fattispecie incriminatrice, le note modali di realizzazione della condotta, nonché quale oggetto di tutela se non di espressione essenziale dell'oggettività giuridica, anche quale spazio immateriale e a-territoriale attraverso cui persone, enti ed istituzioni prestano le loro attività ed i loro servizi e garantiscono la regolarità dei rapporti giuridici. La comprensione della regola tecnologica dovrebbe guidare altresì l'interpretazione della fattispecie legale, nel limite dei possibili significati penalmente rilevanti del testo, per evitare "acrobazie" ermeneutiche espressione di approcci decisamente "*vintage*", nascosti in argomentazioni solo apparentemente di stampo evolutivo ma, di fatto, risultato persino di applicazioni analogiche *in malam partem* dettate da una serie di fattori contingenti, fra cui la preoccupazione di lasciare vuoti di tutela penale. Il rischio da evitare è quello "scollamento" fra il contesto tecnologico-sociale, le scelte del legislatore e l'interpretazione delle singole disposizioni.

Deve aggiungersi che, per quanto attiene ai "fatti" tipizzati dai delitti di danneggiamento informatico, anche dopo l'intervento del legislatore del 2024, la dimensione del bene giuridico tutelato non sembra potersi ridurre al patrimonio del titolare dei sistemi o dei dati, che rimane sullo sfondo. Essa è invece estesa all'integrità e alla disponibilità dei dati e dei sistemi informatici e telematici se non persino, per quanto riguarda le incriminazioni di cui agli artt. 635-*ter* e 635-*quinquies* c.p. – strutturati come delitti di attentato – l'ordine pubblico. L'elemento comune e l'area di intersezione fra dimensione individuale e dimensione collettiva del bene tutelato, è costituita dall'interesse a non subire indebite interferenze nella sfera di rispetto e disponibilità di "spazi informatici", indipendentemente dalla qualità (natura) o dalla quantità di dati e informazioni o dalla natura o dimensione dello spazio informatico di pertinenza di uno o più soggetti "titolari", ovvero dal potere di determinare, in sé, il "destino" di tali aree informatiche in cui si manifesta la personalità umana. Il rafforzamento della tutela penale della riservatezza e sicurezza informatiche era comunque già assicurata sia dalla fattispecie ostacolo di cui all'art. 615-*quater* c.p. – che sanziona condotte prodromiche all'accesso abusivo ad un sistema informatico o telematico tramite una decisa anticipazione della punibilità – sia dalla norma di cui all'art. 615-*quinquies* c.p. (ora confluita sostanzialmente nel nuovo art. 635-*quater*.1) sia, infine, dalle citate disposizioni di cui agli artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p. Con riferimento a queste ultime è facile notare come la

stessa innovazione tecnologica abbia contribuito ad ampliare il raggio di tutela della segretezza della comunicazione, costituzionalmente garantito dall'art. 15 Cost., andando oltre la segretezza del contenuto della comunicazione e attraendo nella sua orbita i dati esterni alle comunicazioni.

A prescindere dalle funzioni che si vogliono attribuire alla tutela penale della sicurezza informatica – positiva e negativa – comunque orientate ad assicurare la tutela dell'interesse alla riservatezza informatica ed alla generale correttezza dello svolgimento dei rapporti giuridici, essa deve trovare un bilanciamento con l'esigenza di garantire la libertà di circolazione dei dati e delle informazioni, nonché con la loro libera accessibilità e fruibilità. Tale bilanciamento risulta essere più complesso per la crescente vulnerabilità dei sistemi informatici, dei dati e delle informazioni in essi archiviati, dovuta a forme di aggressione sia "tradizionali" che "tecnologiche" che si evolvono con lo stesso sviluppo tecnologico.

L'esigenza di assicurare tutela penale della sicurezza informatica non corrisponde ad una necessità costruita artificialmente, ma esprimerebbe il bisogno «di assicurare una condizione condivisa nella società dell'informazione».

3. *Semantica tecnica e componenti strutturali della definizione di cybersecurity*

Appare ora necessaria una ulteriore precisazione, di carattere non solo terminologico. A fenomeni "in costante movimento", come quelli riconducibili al settore della *cyber-criminality*, dovrebbero corrispondere, da un lato, settori dell'ordinamento ad elevato coefficiente di adattamento e, dall'altro lato, un diritto giudiziale flessibile. In campi nuovi o "sperimentali" queste caratterizzazioni del sistema giuridico potrebbero, al contempo, trasmettere un senso di instabilità e di irritazione. Ma proprio la specificità di tali campi o settori necessita del ricorso ad una semantica tecnica che possa riempire termini "tradizionali", comprensibili al giurista ed all'opinione pubblica, con contenuti adattabili al nuovo contesto tecnologico, attenendosi quanto più fedelmente possibile sia al testo redatto dal legislatore, sia ai significati correnti di un termine attribuiti dalla realtà o, meglio, dalla regola tecnologica. Nell'ambito delle ICTs la concezione dello "spazio", inteso quale "area" fruibile dall'utente per il trattamento di dati e informazioni, si basa sull'immaterialità dell'ambiente, che non sempre può essere delimitato entro confini fisici (*server*, singolo sistema o *device*, *smartphone* ecc.) o territoriali. Esso può assumere una duplice dimensione. La prima può essere definita "globale" o "pubblica" e viene tendenzialmente utilizzata per descrivere Internet o, meglio, il *World Wide Web*, ossia ambiti "aperti" a tutti gli utenti. La seconda, invece, è di carattere "individuale" o "privato" e identifica un'area riservata ad uno o più soggetti legittimati ad accedervi attraverso diverse modalità di autenticazione.

Il concetto di cybersecurity (inteso sia riferito alla sicurezza nazionale – nell'ambito della quale si assiste ad una estensione ad un ampio numero di "operatori" di un com-

plesso insieme di obblighi, con penetranti poteri preventivi, prescrittivi e sanzionatori delle Autorità governative e indipendenti – sia in quello relativo al settore pubblico o privato) non può che essere concepito come un *comprehensive concept* e, in linea con questo approccio "integrato", che comprende l'*information security*, dunque, esso esprime anche – e forse in modo preminente – l'interesse alla protezione contro le minacce alla riservatezza, all'integrità, alla disponibilità ed all'affidabilità di dati e informazioni, nonché dei *computers*, di ogni *device* o di ogni rete o sistema attraverso cui tali dati e tali informazioni vengono trattati.

Cybersecurity che, in tal senso, da un lato si distingue dalla nozione di *cybersafety*, la quale sembra includere i rischi connessi agli *informational contents* dei dati e delle informazioni trattati nel *cyberspace*, con ripercussioni dirette e indirette sull'uomo; dall'altro lato, può essere intesa quale processo proattivo e reattivo volto proprio alla protezione ideale dell'interesse degli uomini e delle organizzazioni ad essere liberi da minacce, in specie da quelle alla *CIA-Triad* – la triade *Confidentiality, Integrity* e *Availability* – che costituisce, al tempo stesso, il fulcro, la *core area* della *information security* o cybersecurity e il modello guida della sua governance, a cui può collegarsi l'esigenza di protezione dell'affidabilità di sistemi informatici, reti, dati e informazioni ivi contenuti o tramite di essi trattati.

In estrema sintesi, la nozione di cybersecurity potrebbe essere edificata su almeno tre livelli, tutti meritevoli di protezione, pur tenendo presente le esigenze afferenti alla "sicurezza nazionale": 1. infrastrutturale (*devices, hardware, software* e reti); 2. informazionale (ossia riguardante il patrimonio informativo della persona o dell'ente, non necessariamente di carattere personale); 3. personale "in senso stretto" (che riguarda la *data protection*, ossia la tutela dei dati personali).

Queste riflessioni, però, non possono che partire dalla obiettiva rilevanza di un approccio proattivo e reattivo nella tutela penale della *CIA-Triad*, in uno scenario evanescente ed estremamente mutevole in cui è forse davvero giunto il momento, riprendendo le parole di Rodotà, «di pensare ad un sistema di diritti per il più grande pubblico che l'umanità abbia mai conosciuto».

Questa ricostruzione dogmatica, che giunge all'indomani della legge n. 90/2024, tramite la quale il legislatore penale sarebbe potuto intervenire in modo sistematico sul sistema dei reati informatici, pur valorizzando la tutela di beni collettivi, lungi dal voler limitarsi a contribuire a delimitare la "tipicità" delle fattispecie incriminatrici, vuole offrire un contributo alla elaborazione di un concetto "sostanziale" e "prepositivo" di cybersecurity, capace di assurgere, nella prospettiva di riforma o di adeguamento del sistema penale sostanziale e processuale, a parametro razionale di orientamento delle scelte anche di politica criminale, nella consapevolezza di un necessario e costante dialogo fra discipline, in quanto la scienza penale, in generale, «è fatta da diversi attori che usano oggi molti linguaggi, tra i quali ci sono anche la dogmatica classica e quella moderna, ma sempre più forti sono gli apporti della comparazione e di saperi extragiuridici». La scienza e il sapere tecnologico dovrebbero influenzare il diritto, in un'ottica

di interazione reciproca per la comprensione dei diversi linguaggi. Oggi è proprio la complessità dei linguaggi tecnico-scientifici a mettere il legislatore ed il giudice in una condizione di inferiorità cognitiva, che nel peggiore dei casi si traduce in un approccio casistico culturalmente arretrato rispetto al livello di progresso tecnologico raggiunto. È condivisibile la conclusione a cui giunge una parte della dottrina nell'affrontare, più in generale, il problema dei rapporti tra scienza e diritto e delle controversie tecnico-scientifiche nel diritto e nel processo penale, ossia che si tratti di un «paradosso al quale oggi non ci si può sottrarre». Si tratta di «saperlo gestire, guardandosi dal duplice pericolo che la scienza espropri il diritto, e che il diritto ignori o rinneghi la scienza. Impresa realizzabile in linea di astratto principio, ma difficile nei fatti».

Lo stesso adeguamento, nella prospettiva di una interpretazione evolutiva degli elementi strutturali della fattispecie incriminatrice, a nuove manifestazioni fenomeniche del contesto tecnologico è soluzione percorribile e maggiormente efficace, in molti casi, rispetto ad un approccio interventistico del legislatore penale che potrebbe scontare evidenti criticità di fronte alla rapidità del progresso tecnico. Ma ciò può valere solo in presenza di fattispecie già in astratto suscettibili di plurime chiavi di lettura sotto il profilo dell'oggettività giuridica/offensività.

LA RESPONSABILITÀ PENALE DELL'*INTERNET SERVICE PROVIDER* DOPO IL *DIGITAL SERVICES ACT*

Sofia Braschi

SOMMARIO: 1. Introduzione. – 2. I contenuti essenziali del *Digital Services Act* e della relativa disciplina di attuazione. – 3. La responsabilità penale dell'*hosting provider* nel quadro normativo attuale. – 4. Conclusioni.

1. *Introduzione*

Che la disciplina della comunicazione digitale abbia assunto una posizione di primo piano all'interno della politica dell'Unione è cosa difficile da negare: ove non bastasse il dato relativo alla centralità che il tema riveste all'interno del dibattito pubblico internazionale, per una conferma di questa affermazione è sufficiente guardare al numero delle iniziative legislative presentate al riguardo dalla Commissione[1]. A fronte di un simile quadro, di giorno in giorno sempre più articolato, il presente contributo si propone di approfondire il Regolamento (UE) 2022/2065, c.d. "Regolamento sui servizi digitali" o "*Digital Services Act*" (di seguito DSA), riflettendo in particolare sull'impatto che esso è destinato a dispiegare sulla responsabilità penale dell'*internet service provider* per gli illeciti commessi dagli utenti.

Nella prospettiva in esame, s'inizierà riassumendo i contenuti più significativi della normativa italiana e sovranazionale, di cui occorre tenere conto allorché si tratta di individuare lo statuto di responsabilità dei suddetti operatori; terminata questa operazione, si cercherà di comprendere se e come le novità introdotte dal DSA siano in grado di impattare sui criteri finora utilizzati per imputare al *provider* i reati commessi dagli utenti. L'indagine sarà infine completata da alcune brevi annotazioni relative al ruolo del Regolamento nell'ambito più generale delle politiche dell'Unione che mirano ad assicurare la legalità dell'ambiente digitale.

Prima di procedere in questo senso, sono peraltro opportune alcune precisazioni, volte a meglio individuare l'oggetto delle nostre riflessioni. Occorre invero puntualizzare che, nel contesto attuale, non è più possibile parlare genericamente di responsabilità penale dell'*internet service provider*, dal momento che lo statuto di questi operatori viene oggi individuato da un complesso reticolato normativo, che va a delineare doveri di

[1] Per una panoramica si suggerisce di consultare il seguente sito: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_it.

collaborazione differenziati in ragione delle caratteristiche dell'attività svolta dai singoli prestatori e della tipologia di contenuti illeciti che l'ordinamento intende contrastare.

Per chiarire il significato di questa affermazione, conviene brevemente rammentare che gli *internet service provider* hanno trovato la loro prima regolamentazione all'interno della Direttiva 2000/31/CE, c.d. "Direttiva sul commercio elettronico" o "Direttiva *e-commerce*": muovendo dal principio della neutralità della rete, questo atto ha dettato i principali obblighi dei fornitori di servizi di intermediazione, contenendo altresì delle clausole di esenzione da responsabilità, capaci di riverberare sul piano penale[2]. Senonché, con l'evolversi del mercato digitale, l'avvertita inadeguatezza della suddetta normativa ha fatto sì che alle disposizioni contenute nella Direttiva 2000/31/CE si venissero ad affiancare discipline di settore comprensive di norme capaci di integrare o addirittura derogare ai generali criteri di imputazione ricavabili dalla Direttiva (si pensi, nella prospettiva in esame, al Regolamento (EU) 2016/679 sulla protezione dei dati personali, alla Direttiva 2019/790/EU in tema di *copyright* e al Regolamento (UE) 2021/784 concernente il contrasto della diffusione di contenuti terroristici online). Senza volerci dilungare sulla questione[3], occorre però annotare che il nuovo Regolamento sui servizi digitali, nel disciplinare i doveri degli *internet service provider*, non ha abrogato nella sua interezza la Direttiva sul commercio elettronico, che rimane quindi tutt'ora in vigore, e ha fatto salve le previsioni via via introdotte dagli atti sopra richiamati (art. 2 co. 3 e 4). Non solo: come si avrà modo di evidenziare, il DSA ha differenziato la posizione dei diversi prestatori di servizi *internet* in relazione anche alla natura e alla dimensione dell'attività svolta, aggiungendo, in particolare, alla tradizionale distinzione fra *mere conduit*, *caching* e *hosting provider* le nozioni di piattaforme online e piattaforme online di dimensioni molto grandi, motori di ricerca e motori di ricerca di dimensioni molto grandi[4].

La conseguenza di una simile evoluzione è che, nella realtà attuale, non è più possibile parlare genericamente di responsabilità del *provider*: la posizione di questi operatori viene oggi individuata da una complessa normativa, che si compone di previsioni generali, essenzialmente fornite dal Regolamento (UE) 2022/2065 e differenziate in relazione alla natura dei diversi operatori, e di regole speciali previste dalle singole normative di settore. Se una simile situazione configura un avanzamento rispetto alla Direttiva *e-commerce*, nella misura in cui consente di modulare la responsabilità e i doveri di collaborazione in relazione alle caratteristiche dei diversi soggetti attivi nel mercato digitale e alla diversa gravità dei fenomeni oggetto di regolazione, è anche vero

[2] Per maggiori informazioni sui contenuti della Direttiva sul commercio elettronico vd. L. D'AGOSTINO, *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di* compliance, in «Diritto penale contemporaneo – Rivista trimestrale», 4 (2021), pp. 288-290.

[3] Sulle tappe essenziali dell'evoluzione della normativa relativa alla responsabilità dei *provider* sia consentito rinviare a S. BRASCHI, Social media *e responsabilità penale dell'*Internet Service Provider, in «Medialaws», 3 (2020), pp. 158-163.

[4] Per completezza, conviene inoltre segnalare che regole speciali sono previste per le piattaforme di *e-commerce*: vd., ad esempio, l'art. 6 co. 3 del Regolamento.

però che l'estrema complessità della disciplina pone non pochi problemi di interpretazione, potendo fra l'altro impattare negativamente sulla capacità degli operatori di conformare la propria attività alle richieste dell'ordinamento.

Fatta questa precisazione, a fronte dell'impossibilità di un esame esaustivo, nelle pagine che seguono ci concentreremo sulla responsabilità di un particolare soggetto, l'*hosting provider*, per cercare di indagare le conseguenze derivanti dalla mancata rimozione dei contenuti illeciti prodotti dagli utenti, che non sono destinatari di regole speciali stabilite da provvedimenti di settore.

2. *I contenuti essenziali del* Digital Services Act *e della relativa disciplina di attuazione*

Per un corretto inquadramento del problema, è indispensabile incominciare riepilogando i contenuti essenziali della normativa che oggi concorre a delineare lo statuto di responsabilità penale dell'*hosting provider*.

Al riguardo, è bene preliminarmente precisare che all'approvazione del DSA, entrato in vigore nel febbraio 2024, ha fatto seguito un ulteriore Regolamento di attuazione, che disciplina i poteri sanzionatori della Commissione europea nei confronti delle piattaforme di dimensioni molto grandi[5]. Soprattutto, spostandoci sul versante nazionale, occorre ricordare che il nostro legislatore ha attuato il Regolamento sui servizi digitali mediante due diversi provvedimenti: il d.l. 15 settembre 2023, n. 123 – il c.d. "decreto Caivano" – conv. in l. 13 novembre 2023, n. 159, che all'art. 15 ha individuato nell'Agenzia per le Comunicazioni (AGCOM) il Coordinatore dei Servizi Digitali e ne ha disciplinato i poteri sanzionatori nei confronti delle piattaforme digitali, e il d.lgs. 25 marzo 2024, n. 50, che, fra l'altro, all'art. 3 ha abrogato gli artt. 14-17 del d.lgs. 9 aprile 2003, n. 70, di attuazione della Direttiva *e-commerce*, sostituiti dagli artt. 4-6 del Regolamento che occorre adesso esaminare.

Passando dunque ad analizzare le disposizioni più rilevanti del DSA, si può anzitutto affermare che, nel definire la posizione degli *internet service provider*, tale atto si muove lungo due direttrici essenziali, che possiamo schematicamente compendiare nelle nozioni di *liability* e *accountability*.

Con riferimento al primo profilo, il Regolamento si pone in una linea di sostanziale continuità con la precedente Direttiva sul commercio elettronico. Invero, oltre a ribadire l'assenza di un generale dovere di controllo preventivo (art. 8), il DSA riproduce la tradizionale distinzione tra servizi di accesso e memorizzazione, stabilendo per ciascuno di essi delle regole di esenzione da responsabilità per le attività illecite commesse

[5] Si fa riferimento al Regolamento di esecuzione (UE) 2023/1201 della Commissione del 21 giugno 2023, relativo alle modalità dettagliate di attuazione da parte della Commissione di determinate procedure a norma del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio («regolamento sui servizi digitali»).

dagli utenti (artt. 4-6). Ai nostri fini conviene soprattutto ricordare il contenuto dell'art. 6, in base al quale l'*hosting provider* non è responsabile delle informazioni memorizzate, sempre che esso (*i*) non sia effettivamente a conoscenza delle attività o dei contenuti illegali e (*ii*) non appena venga a conoscenza di tali attività o contenuti, agisca immediatamente per la loro rimozione. Rispetto alla Direttiva *e-commerce*, conviene poi evidenziare che il Regolamento precisa che le esenzioni da responsabilità non dovrebbero trovare applicazione laddove il prestatore di servizi intermediari «svolga un ruolo attivo atto a conferirgli il controllo o la conoscenza di tali informazioni»[6].

Le principali innovazioni introdotte dalla normativa europea si situano però sul piano dell'*accountability*[7]: invero, il Regolamento contiene numerose previsioni volte a stabilire doveri di *due diligence*, che presentano un'intensità crescente in relazione alla natura economica e all'ampiezza del servizio offerto dall'operatore. Limitandoci ad alcune brevi annotazioni, si può anzitutto osservare che i suddetti doveri attengono alle attività di controllo e moderazione dei contenuti, alla trasparenza ovvero alla valutazione e gestione del rischio; hanno un diverso ambito di applicazione, potendo interessare tutti gli intermediari digitali (artt. 16-28), solamente le piattaforme online, individuate negli *hosting provider* che offrono «un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico»[8] (artt. 29-32), nonché, infine, solamente le piattaforme e i motori di ricerca di dimensioni molto grandi (artt. 33-43)[9].

In questa cornice generale, per lo svolgimento delle nostre riflessioni è utile soprattutto riportare il contenuto dell'art. 16: invero, al co. 1 tale disposizione prevede che i fornitori di servizi di memorizzazione debbano predisporre meccanismi di segnalazione e rimozione volti a facilitare segnalazioni sufficientemente precise; al co. 3 chiarisce che le suddette segnalazioni «permettono di acquisire una conoscenza o consapevolezza effettiva ai fini dell'articolo 6 […] qualora consentano a un prestatore diligente di servizi di memorizzazione di informazioni di individuare l'illegalità della pertinente

[6] Vd. il *Considerando* n. 18, il quale recepisce la figura dell'*hosting provider* attivo elaborata dalla Corte di Giustizia dell'Unione Europea. Sulle incertezze inerenti all'affermazione riportata nel testo, C. De Menech, *Mercato digitale e danno da prodotti*, in «juscivile», (2024), pp. 514-515; con riferimento alla responsabilità penale, si può peraltro ritenere che la previsione sollevi problematiche minori dal momento che, come si chiarirà, il principale ostacolo alla punibilità del *provider* origina dall'atipicità della condotta ascrivibile a questo operatore.

[7] Così M. Husovec, *Principles of the Digital Services Act*, Oxford University Press, London, 2023, p. 22.

[8] Art. 3 lett. i); per completezza, occorre precisare che fuoriescono dalla suddetta nozione i casi in cui l'attività di memorizzazione e diffusione configuri «una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale». Il senso di questa precisazione viene illustrato nel *Considerando* n. 13, in cui si chiarisce che, ad esempio, non dovrebbero essere considerati piattaforme i quotidiani online che contengano una sezione per i commenti degli utenti, «ove sia evidente che [la sezione] è accessoria al servizio principale rappresentato dalla pubblicazione di notizie sotto la responsabilità editoriale dell'editore»; la medesima conclusione vale per i servizi di *cloud computing* e di memorizzazione di informazioni di siti *web*.

[9] Nella dottrina italiana, per una panoramica dei doveri di *due diligence* fissati dal Regolamento, E. Longo, *Libertà di informazione e lotta alla disinformazione nel* Digital Services Act, in «Giornale di diritto amministrativo», (2023), pp. 741-744; in quella straniera, Husovec, *Principles of the Digital Services Act*, cit., pp. 22-30.

attività o informazione senza un esame giuridico dettagliato»[10]. In altri termini, come si vede, il DSA istituzionalizza i meccanismi di *notice and action* che si erano andati affermando a partire dalla prima decade degli anni Duemila, e che erano già stati oggetto di previsione in atti di *soft law*, come il codice di autoregolamentazione promosso dalla Commissione europea[11]; chiarisce che la ricezione di una segnalazione sufficientemente precisa è in grado di determinare l'acquisizione di quella "conoscenza effettiva" alla cui maturazione consegue la perdita della esenzione da responsabilità prevista per la memorizzazione dei materiali illeciti.

Dopo avere così brevemente sintetizzato i contenuti del Regolamento, è opportuno articolare adesso due brevi osservazioni. La prima attiene al tema della *liability*: al riguardo, è bene precisare che, al pari della Direttiva sul commercio elettronico, il DSA ha scelto di non armonizzare le regole inerenti ai presupposti di configurazione della responsabilità degli *internet service provider*, limitandosi a tracciare delle aree di esenzione da responsabilità. La conseguenza di una simile impostazione è che, da un lato tale atto normativo non può essere utilizzato per fondare una responsabilità penale[12], dall'altro la mancata applicazione delle clausole di esenzione sopra riportate non può determinare automaticamente la configurazione di una responsabilità in capo al *provider*[13]. Detto diversamente, l'operatore *internet* risponde delle violazioni commesse dagli utenti solamente in quanto siano integrati i presupposti di punibilità che sono fissati dal diritto nazionale e non trovino applicazione le cause di esenzione da responsabilità previste dal Regolamento.

La seconda considerazione riguarda invece i doveri di *due diligence*, in relazione ai quali è opportuno annotare che il DSA impone agli Stati membri di introdurre norme

[10] Sul significato di questa disposizione WILMAN, *Article 16*, in F. WILMAN, S.L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, Oxford University Press, London, 2023, pp. 139-140, §§ 20-22, il quale peraltro precisa che la norma non dovrebbe trovare applicazione nei casi in cui il *provider* riceve una segnalazione sufficientemente precisa, senza però che sia utilizzato il meccanismo di *notice and action* delineato dal Regolamento.

[11] Si allude al *Code of conduct countering illegal hate speech online*, promosso nel 2016 in collaborazione con alcune piattaforme digitali; non si può peraltro non ricordare che queste procedure erano già state rese obbligatorie in alcuni paesi, come la Germania, mediante la c.d. "Legge per il miglioramento dell'applicazione del diritto nei *social network*" (*Netzwerkdurchsetzungsgesetz*). Per approfondimenti sulle origini delle procedure di *notice and action* (o *notice and take down*) e alcuni riferimenti comparati B. PANATTONI, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di* notice and take down, in «Sistema penale», 5 (2018), pp. 256-259; per maggiori dettagli sul meccanismo di *notice and action* delineato dal DSA, invece, WILMAN, *Article 16*, cit., pp. 135-139, §§ 8-19.

[12] Così chiaramente si esprime il *Considerando* n. 17, laddove prevede che le norme che disciplinano le esenzioni da responsabilità «non dovrebbero essere intese come una base per stabilire quando un prestatore può essere ritenuto responsabile, circostanza che deve essere determinata in base alle norme applicabili del diritto dell'Unione o nazionale». Nel senso riportato nel testo vd. anche F. WILMAN, *Chapter II. Liability of Providers of Intermediary Services*, in F. WILMAN, S.L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, cit., p. 50, § 4.

[13] Sottolinea questo aspetto HUSOVEC, *Principles of the Digital Services Act*, cit., p. 117, osservando criticamente che tanto la Corte di Giustizia dell'Unione Europea, quanto la giurisprudenza nazionale tendono a far coincidere i presupposti per la configurazione della responsabilità dei *provider* con la mancata applicazione delle clausole di esenzione da responsabilità.

volte ad applicare sanzioni «effettive, proporzionate e dissuasive», finalizzate ad assicurare il rispetto delle relative prescrizioni (art. 52). A ciò ha provveduto il nostro legislatore con il già citato d.l. n. 123 del 2023, che all'art. 15 ha stabilito che l'AGCOM, in quanto Coordinatore dei Servizi Digitali, assicura il rispetto degli obblighi fissati dal Regolamento, comminando, in caso di loro violazione, «sanzioni amministrative pecuniarie fino ad un massimo del 6% del fatturato annuo mondiale»[14]. In altri termini, come si vede, il DSA ha inteso assicurare il rispetto dei doveri di *due diligence* mediante la previsione di specifiche sanzioni; tale osservazione, se da un lato consente di affermare che le su richiamate prescrizioni non operano solamente sul piano della responsabilità sociale, dall'altro lascia aperta la questione relativa alla loro possibile intersezione con le regole che disciplinano la responsabilità penale per gli illeciti commessi dagli utenti[15]. È sul suo esame che ci dobbiamo quindi concentrare.

3. *La responsabilità penale dell'*hosting provider *nel quadro normativo attuale*

Procedendo con ordine, conviene incominciare ricordando brevemente le conclusioni alle quali erano pervenute la dottrina e la giurisprudenza precedenti all'approvazione del Regolamento sui servizi digitali, per poi verificare se e in che misura le novità introdotte da questo provvedimento siano in grado di impattare sulla responsabilità penale dell'*hosting provider*.

Sintetizzando, posto che in occasione della ricezione della Direttiva 2000/31/CE il legislatore non aveva seguito la strada, pur percorsa da altri ordinamenti[16], di introdurre un'apposita incriminazione, per affermare la punibilità di tali ultimi operatori la dottrina aveva ritenuto indispensabile applicare le fattispecie e i criteri di imputazione presenti all'interno del codice penale. In maniera coerente con questa impostazione aveva anzitutto indagato la possibilità di configurare una responsabilità concorsuale per il reato commesso dall'utente; a tal riguardo, però, salvi i casi di positiva partecipazione alla realizzazione del contenuto, l'opinione prevalente si era espressa nel senso di negare la plausibilità di una simile soluzione, facendo leva su tre principali considerazioni[17]. In primo

[14] Si tratta dell'art. 15 co. 4, così come modificato dalla l. n. 159 del 2023, di conversione del d.l. n. 123 del 2023, che espressamente richiama la violazione degli obblighi previsti dagli artt. 9-18, 20-24, 26, 27, 28, 30 e 45 del DSA.

[15] Sul rapporto fra *liability* e *accountability* cfr. HUSOVEC, *Principles of the Digital Services Act*, cit., pp. 181-184, il quale sostiene la netta separazione fra doveri degli utenti e doveri degli operatori *internet*, evidenziando fra l'altro come il Parlamento Europeo avesse premuto per legare le esenzioni da responsabilità dei *provider* al rispetto dei doveri di *due diligence*, soluzione infine esclusa dalla Commissione; M. TIERNAN, G. SLUITER, *The European Union's Digital Services Act and secondary criminal liability for online platform providers. A missed opportunity for fair criminal accountability?*, (2025), p. 2 del testo reperibile al seguente *link*: https://ssrn.com/abstract=5104485, i quali invece ritengono che i doveri di *due diligence* aumenteranno la conoscenza dei contenuti illeciti da parte degli operatori, con conseguenze destinate a riverberare anche sulla responsabilità penale.

[16] Sul punto vd. D. PETRINI, *La responsabilità penale per i reati via* Internet, Jovene, Napoli, 2004, pp. 201-207.

[17] Così, in particolare, S. SEMINARA, Internet *(diritto penale)*, in *Enc. dir.*, Annali VII, Giuffrè, Milano, 2014, p. 597; in un'analoga prospettiva PETRINI, *La responsabilità penale per i reati via* Internet, cit., p. 178; A. INGRASSIA,

luogo, si era evidenziato come il carattere istantaneo dei reati incentrati su condotte di comunicazione impedisse di affermare una responsabilità basata sul solo mantenimento in rete di contenuti già pubblicati dagli utenti, trattandosi di una condotta successiva alla consumazione del reato principale; a tale annotazione si era, inoltre, aggiunto che non era possibile affermare l'esistenza in capo al *provider* di una posizione di garanzia in grado di fondare una responsabilità a titolo di reato omissivo improprio. Tanto più che – e qua veniamo alla terza considerazione – trattandosi di un concorso tramite condotte neutre, di responsabilità penale si sarebbe potuto parlare solamente ove si fosse accertata la sussistenza di un dolo intenzionale. Sulla scorta di simili osservazioni, la dottrina maggioritaria aveva dunque negato la possibilità di configurare una responsabilità accessoria in capo all'*hosting provider* che non avesse rimosso i contenuti illeciti pubblicati dagli utenti, argomentando piuttosto in favore della contestazione di fattispecie come l'art. 388 o 650 c.p., laddove la mancata attivazione dell'operatore seguisse a una richiesta qualificata da parte dell'autorità giudiziaria o di una pubblica amministrazione.

Come noto, però, una ricostruzione in parte differente era stata infine adottata dalla giurisprudenza di legittimità. Più in particolare, la Corte di Cassazione da un lato aveva escluso la possibilità di configurare una posizione di garanzia in capo al *provider*[18], dall'altro lato aveva però affermato la punibilità dell'amministratore del *blog* per la mancata rimozione dei contenuti illeciti che fossero stati segnalati dagli utenti. A fondamento di una simile soluzione aveva portato ora la configurabilità di una responsabilità concorsuale per il mantenimento in rete del materiale antigiuridico oggetto di pubblicazione, ora la suscettibilità di tale ultima condotta di integrare un autonomo illecito penale[19].

Così brevemente ricostruita la situazione antecedente all'approvazione del Regolamento, si tratta adesso di verificare se le sue innovazioni possano determinare un mutamento delle conclusioni precedentemente raggiunte. Nella prospettiva in esame, conviene anzitutto ribadire che le norme relative alle esenzioni da punibilità non sono di per sé in grado di fondare una responsabilità penale: ne consegue che dalla modifica della previsione concernente i doveri dell'*hosting provider* (art. 16), che come visto lega l'acquisizione della "conoscenza effettiva" dell'illiceità del contenuto richiesta dall'art. 6 alla mera ricezione di una segnalazione sufficientemente precisa, non discende automaticamente la punibilità di tale ultimo operatore. Ancora una volta, si tratta cioè di accertare che la condotta del *provider* integri tutti i presupposti per la configurazione di una responsabilità penale.

Responsabilità penale degli internet service provider*: attualità e prospettive*, in «Diritto penale e processo», (2017), p. 1626; D'Agostino, *Disinformazione e responsabilità delle piattaforme*, cit., pp. 297-298. In favore di una più ampia configurazione di responsabilità in capo al *provider* vd., fra gli altri, con diverse sfumature, L. Picotti, *Diritto penale e tecnologie informatiche. Una visione d'insieme*, in *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, UTET, Torino, 2019, p. 89; R. Bartoli, *Brevi considerazioni sulla responsabilità penale dell'*Internet Service Provider, in «Diritto penale e processo», (2013), p. 606.

[18] Cass., sez. III, 3 febbraio 2014, n. 5107.

[19] Cfr. Cass., sez. V, 27 dicembre 2016, n. 54946; Id., sez. V, 20 marzo 2019, n. 12546 e Id., sez. V, 1° dicembre 2022, n. 45680.

Ciò premesso, si potrebbe argomentare che, alla luce dell'introduzione di più pregnanti doveri di *due diligence* in capo ai prestatori di servizi della società dell'informazione, questi possano essere ritenuti titolari di una posizione di garanzia, in grado di legittimare l'applicazione dell'art. 40 cpv. Senonché, anche ammettendo una simile soluzione[20], resta l'obiezione per cui la mancata rimozione del materiale illecito configura una condotta successiva alla consumazione del reato, come tale incapace di assumere rilevanza penale a titolo di concorso nel reato principale. Per superare questa *impasse*, si potrebbe allora argomentare che il *provider* sia l'autore di un'autonoma violazione; una simile affermazione, certamente non condivisibile in relazione al semplice fornitore di servizi di memorizzazione, potrebbe apparire invece più plausibile con riferimento al gestore della piattaforma digitale, alla luce della scelta del legislatore europeo di caratterizzare l'attività svolta da questo operatore anche tramite il concetto di "ulteriore diffusione" al pubblico del materiale oggetto di pubblicazione. Detto diversamente, si potrebbe sostenere che, nel caso della mancata rimozione del contenuto illecito caricato dall'utente, sia possibile chiamare la piattaforma a rispondere come autore di un autonomo reato, identico a quello commesso dal produttore del contenuto, e fondato sulla nuova diffusione del materiale antigiuridico[21]; benché astrattamente plausibile, una simile impostazione non pare però del tutto convincente.

Soffermandoci brevemente sul punto, occorre anzitutto precisare che, anche una volta ammesso che il mantenimento nella rete del materiale antigiuridico possa configurare una condotta di "diffusione" suscettibile di integrare un'autonoma violazione, resta in piedi la necessità di accertare l'elemento soggettivo del reato; né una simile operazione appare agevole, ove solo si consideri che, in linea tendenziale, il produttore del contenuto è un utente privo di legami con la piattaforma e che, per questa ragione, assai difficilmente tale ultimo soggetto ha un interesse verso il mantenimento o la circolazione della singola pubblicazione[22]. Ciò puntualizzato, si può poi osservare che dalla configurazione di una responsabilità penale in capo a colui che non abbia provveduto a eliminare il contenuto oggetto di segnalazione discende la possibilità di chiamare a rispondere del reato pure l'ente di appartenenza dell'operatore. Senonché, anche trascurando le disparità derivanti dal fatto che solo alcuni degli illeciti che formano oggetto dell'obbligo di

[20] In termini negativi S. SEMINARA, *La diffamazione e le responsabilità penali sul* web, in *Informazione e media nell'era digitale*, a cura di A. Avanzini, G. Matucci, L. Musselli, Giuffrè, Milano, 2023[2] (I ed. Giuffrè, Milano, 2019), p. 146, secondo il quale «l'opzione in favore di prescrizioni di tipo organizzativo orienta verso forme di responsabilità prevalentemente civile e, d'altra parte, l'imposizione di standard tecnologici non può convertirsi in una posizione di garanzia penalmente rilevante in assenza di apposite fattispecie punitive».

[21] Questa la strada percorsa da Cass., sez. V, 20 marzo 2019, n. 12546, cit., sull'assunto che la mancata tempestiva rimozione del commento diffamatorio "equivalga" alla consapevole condivisione del contenuto.

[22] Sotto il profilo in esame, risalta la differenza con la stampa più tradizionale e trova giustificazione la tradizionale esclusione della possibilità di applicare l'art. 57 c.p. ai *social media*: così ad esempio Cass., sez. V, 24 febbraio 2021, n. 7220. Sul legame fra piattaforme e utenti, e sui rischi di *overblocking* derivanti dalla responsabilizzazione dei *provider*, E. ROSATI, G. SARTOR, *Social networks e responsabilità del provider*, in *EUI working papers, LAW*, (2012), 5, p. 8.

rimozione ricadono entro l'ambito di applicazione del d.lgs. 8 giugno 2001, n. 231[23], non può negarsi che una simile soluzione presenta il rischio di determinare una violazione del divieto di *bis in idem*: come visto, infatti, il rispetto dei doveri di *due diligence* forma oggi oggetto di un obbligo giuridico, la cui violazione è sanzionata dall'AGCOM con sanzioni capaci di arrivare fino al 6% del fatturato annuo dell'operatore[24]. D'altra parte, chiudendo sul punto, ci dobbiamo domandare se l'idea della configurazione di una responsabilità di natura concorsuale sia davvero persuasiva: a ben vedere, infatti, l'illecito ascrivibile alla piattaforma risiede in un difetto di organizzazione, più che nella volontà di contribuire alla diffusione del materiale pubblicato dall'utente.

In definitiva, alla luce delle considerazioni che precedono sembra possibile affermare che le novità introdotte dal Regolamento sui servizi digitali non giustificano una revisione delle posizioni maturate prima della sua approvazione: anche nel quadro normativo attuale è più corretto ritenere che non sia generalmente possibile chiamare il *provider* a rispondere della mera mancata rimozione del materiale antigiuridico prodotto dall'utente. La medesima conclusione vale anche per la piattaforma digitale: tutti questi soggetti potranno peraltro essere sanzionati in via amministrativa laddove non diano attuazione ai doveri stabiliti dal DSA, volti ad assicurare la legalità della comunicazione online.

4. *Conclusioni*

A completamento di questa analisi, siano consentite alcune brevi considerazioni relative al significato del DSA nell'ambito più generale delle politiche dell'Unione concernenti la disciplina dell'ambiente digitale.

Al riguardo, occorre anzitutto evidenziare che, come già rilevato in sede introduttiva, il provvedimento oggetto delle nostre riflessioni fa parte di un più ampio pacchetto di misure – di cui il Regolamento "fratello" (UE) 2022/1925 (c.d. "Regolamento sui mercati digitali" o "*Digital Market Act*") è solo un'ulteriore esemplificazione – che sono volte a disciplinare il mondo della rete e a ripensare il ruolo degli operatori attivi sul mercato digitale: un simile sforzo di regolamentazione, che pure non ha mancato di sollevare critiche legate all'assenza di un corrispondente impegno nello sviluppo e nella promozione delle infrastrutture tecnologiche, va salutato con favore, nella misura

[23] In particolare, ricadono entro l'ambito di applicazione del d.lgs. n. 231 del 2001 i delitti con finalità di terrorismo (art. 25-*ter*), quelli in materia di pedopornografia (art. 25-*quinquies*), i delitti in tema di violazione del diritto d'autore (art. 25-*novies*), l'art. 604-*bis* c.p. e le fattispecie aggravate ai sensi dell'art. 604-*ter* c.p. (art. 25-*terdecies*): ne risulta che rimarrebbe, ad esempio, fuori il reato di diffusione illecita di immagini o video sessualmente espliciti (art. 612-*ter* c.p.), pur rientrando la pornografia non consensuale nella nozione di "contenuto illecito" avuto in mente dal legislatore europeo (vd. *Considerando* n. 80).

[24] Un analogo concorso di misure sanzionatorie oggi caratterizza, ad esempio, il settore dei reati finanziari, non a caso individuato come problematico sotto il profilo del divieto di *bis in idem*: così S. SEMINARA, *Il divieto di* bis in idem*: un istituto inquieto*, in «Diritto penale e processo», (2022), p. 1396, al quale si rimanda anche per ampi approfondimenti sul suddetto principio, alla luce della giurisprudenza nazionale e sovranazionale.

in cui rivela l'acquisita consapevolezza della centralità che *internet* assume nell'odierna vita sociale, con una particolare attenzione ai possibili effetti distorsivi sul piano della libertà di informazione e comunicazione.

Fatta questa preliminare osservazione, occorre peraltro riconoscere che il Regolamento solleva alcune perplessità. Limitandoci a quelle maggiormente attinenti al campo della nostra riflessione, si può anzitutto ribadire la singolarità della scelta del legislatore europeo di non disciplinare i presupposti della responsabilità degli *internet service provider*: una simile impostazione, benché apprezzabile dal punto di vista del rispetto delle prerogative del legislatore nazionale, appare invece poco convincente, allorché si consideri il rischio di pregiudicare gli obiettivi di armonizzazione che sono alla base della stessa adozione del Regolamento[25].

Parimenti, alcune perplessità solleva il dato per cui il DSA si preoccupa di regolare i doveri dei prestatori di servizi della società dell'informazione di rimozione dei contenuti illeciti, senza peraltro definire il significato di tale ultima nozione. Invero, per determinare l'antigiuridicità del materiale oggetto di pubblicazione è necessario riferirsi alle scelte di incriminazione effettuate dal legislatore nazionale: senonché, ancora una volta, risulta evidente come una simile impostazione sia in grado di riverberare sull'ampiezza degli obblighi di attivazione, inevitabilmente destinati a variare in relazione all'ambito di applicazione delle fattispecie penali vigenti all'interno dei diversi paesi. D'altra parte, alla luce di tale annotazione non sorprende che, poco dopo l'entrata in vigore del Regolamento, l'Unione abbia altresì approvato una Direttiva, la Direttiva (UE) 2024/1385, contenente numerose previsioni volte ad armonizzare le fattispecie incriminatrici delle principali forme di violenza di genere online: una simile iniziativa, se da un lato va apprezzata nella misura in cui permette una più efficace attuazione del DSA, dall'altro suggerisce di meditare sulla capacità di tale provvedimento di determinare una surrettizia estensione delle competenze penali dell'Unione[26].

In definitiva, anche sotto il profilo in esame, trova conferma l'importanza che la comunicazione digitale assume nel quadro più ampio del diritto eurounitario; di qui l'opportunità di dedicare al tema ulteriori spazi di riflessione.

[25] Nei limiti di quello che conosciamo, è significativa, sotto il profilo in esame, l'indagine recentemente avviata in Francia nei confronti dell'amministratore della piattaforma Telegram, accusato, fra l'altro, di concorso nei reati di pedopornografia commessi dagli utenti: sul punto, per alcune sommarie informazioni, P. Dufourq, *Decifrare il recente procedimento giudiziario a carico del fondatore del servizio di messaggistica TELEGRAM*, in «Giurisprudenza penale», (2 settembre 2024), pp. 1-3 e 5-7.

[26] Invero, benché la base legale della Direttiva 2024/1385 sia stata individuata nell'art. 83 par. 1 TFUE, interpretato estensivamente in modo da ricomprendere anche i reati soltanto facilitati dal ricorso alla tecnologia digitale, è difficile negare che l'intervento legislativo risponda pure alla necessità di assicurare l'implementazione del DSA, più volte richiamato dalla stessa Commissione nel corso dell'*iter* che ha portato all'approvazione della Direttiva. In generale, sulla competenza penale accessoria dell'Unione e sulla tendenza del legislatore europeo a non fare ad essa espresso riferimento, A. Bernardi, *La competenza penale accessoria dell'Unione Europea: problemi e prospettive*, in «Diritto penale contemporaneo – Rivista trimestrale», (2012), 1, pp. 49-57.

LA RESPONSABILITÀ DELLE PIATTAFORME PER I CRIMINI ONLINE NELL'ORDINAMENTO STATUNITENSE: IL CASO DELLE "PIATTAFORME ILLECITE"

Beatrice Panattoni

1. *Il regime d'immunità delle piattaforme nell'ordinamento statunitense: la Section 230 del* Communications Decency Act

Nel rinnovo semantico che segue un cambiamento sociale, la prima e inevitabile tendenza è quella di estendere e riproporre concetti e categorie note per descrivere le manifestazioni prodotte da quel cambiamento. Si utilizzano così parole e termini pensati per contesti e dinamiche sociali differenti, perché ci si trova sprovvisti dei riferimenti adatti a cogliere la trasformatività. Questo è ciò che è accaduto quando, nell'ordinamento statunitense, il legislatore ha deciso di regolare l'attività dei gestori delle piattaforme online.

Prima dell'avvento di Internet, la circolazione delle informazioni era il prodotto dello scambio tra attori precisi: l'editore (il *publisher*), il distributore (il *distributor*) e il fruitore, lettore o utente finale. Il referente concettuale era dunque quello del mondo dell'editoria, in cui un agente professionalmente competente pubblicava contenuti, selezionati e raccolti da fonti qualificate, i quali venivano poi distribuiti da altri operatori, come ad esempio potevano essere le librerie, e messi così a disposizione del grande pubblico. Di conseguenza, tradizionalmente, la responsabilità per i contenuti di terze parti si è sempre legata al criterio del "controllo editoriale" sui contenuti, senza il quale il soggetto che li pubblica o distribuisce non può ritenersi responsabile per gli stessi[1].

Nella "preistoria" della rivoluzione digitale, ossia nel periodo dei primi anni '90 del secolo scorso, quando Internet aveva solo pochi anni di vita, la giurisprudenza statunitense ricondusse a questo schema concettuale i primi casi di materiali offensivi circolanti in rete[2].

[1] Cfr. E. GOLDMAN, *An Overview of the United States' Section 230 Internet Immunity*, in *Oxford Handbook of Online Intermediary Liability*, a cura di G. Frosio, Oxford University Press, Oxford, 2020, p. 155.

[2] Per una ricostruzione del *case law* in materia di rimanda a J. KOSSEFF, *The Twenty-Six Words That Created the Internet*, Cornell University Press, New York, 2019.

Con la nascita dei nuovi servizi di comunicazione e scambio di contenuti in rete, le corti americane, e poi anche il legislatore, non si interrogarono sulle novità che hanno caratterizzato fin da subito il contesto dei servizi digitali, ma iniziarono a legare le forme di responsabilità di tali operatori al criterio del controllo editoriale. Di conseguenza, si generò quello che è stato definito il "dilemma del moderatore"[3], ossia il dubbio, per gli intermediari, di implementare pratiche di moderazione dei contenuti per far sì che la propria piattaforma non divenisse veicolo di materiali offensivi, scelta che si associava però al rischio di andare incontro a forme di responsabilità proprio in virtù dell'implementazione di quelle stesse pratiche, che li potevano rendere, secondo lo schema tipicamente utilizzato nel contesto della responsabilità per contenuti terzi, "editori" dei contenuti ospitati.

Tale "dilemma" ha portato così all'eliminazione da parte degli intermediari di ogni forma di controllo sui contenuti ospitati sui propri siti: circostanza che ha agevolato la fortuna dei modelli economici di questo settore d'attività, in cui la scelta di estromettere un controllo editoriale sui contenuti non era operata solamente per tutelarsi da possibili forme di responsabilità, ma consentiva al servizio digitale una maggior resa economica. Il modello economico che sta dietro a tali attività, infatti, non solo non si fonda su un controllo editoriale, ma lo vede come un ostacolo alla profittabilità del servizio. In altri termini, il modello di *business* dei siti di scambio di contenuti online "*user-generated*", ossia generati direttamente dai propri utenti, si è fin dall'inizio fondato sulla libera circolazione di materiali, senza alcuna mediazione "editoriale" da parte del gestore del sito[4].

Venendo ora al piano normativo, la fonte di riferimento che disciplina la materia nell'ordinamento statunitense è la Section 230 del *Communication Decency Act*, introdotta nel 1996, la quale ha ritagliato un regime di immunità per i *provider* da possibili addebiti di responsabilità per i contenuti caricati e diffusi dai propri utenti. Nello specifico, la *subsection* (c) – *Protection for "Good Samaritan" blocking and screening of offensive material* – è composta da due previsioni: ciò che interessa ai nostri fini è la *subsection* (c)(1) – *Treatment of publisher or speaker* – secondo cui nessun fornitore o utente di un servizio informatico interattivo potrà essere considerato quale editore (*publisher*) o autore (*speaker*) di qualsivoglia informazione fornita da un terzo soggetto[5].

[3] Su questo cfr. E. Golman, *Sex Trafficking Exceptions to Section 230*, in «Santa Clara U. Legal Studies Research Paper», 13, (2017), diponibile al sito: <https://ssrn.com/abstract=3038632>, che mantiene una posizione volta a salvaguardare il regime d'immunità per evitare di ricadere nel dilemma del moderatore, mentre, per posizioni che auspicano una riforma del regime d'immunità, cfr. D. Citron, B. Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, in «Fordham Law Review», 86 (2017), p. 401 ss.

[4] Per una lettura della responsabilità delle piattaforme nell'ordinamento statunitense usando le lenti del diritto dell'economia cfr. K.E. Spier, R.V. Loo, *Foundations for Platform Liability*, in «Harvard Public Law Working Paper», 24-16 (2024), disposibile al sito: <https://ssrn.com/abstract=5015344>.

[5] 47 U.S.C. § 230(c)(1). Traduzione dell'autrice. Si riporta di seguito il testo originale: «*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*».

Tale previsione, che distanzia i *provider* dalla figura dei *publisher*, ha permesso alla giurisprudenza americana di qualificarli quali meri intermediari passivi in relazione ai contenuti veicolati, lasciandoli liberi di mantenere online i contenuti caricati e fatti circolare dai propri utenti, senza per ciò incorrere in alcun tipo di responsabilità.

Per quanto il regime d'immunità sia piuttosto esteso, non facendo distinzioni in relazione ai diversi tipi di operatori che possono rientrare nell'ampio insieme di *provider* di servizi d'interazione, o ai diversi contenuti illeciti che possono circolare online, non si tratta tuttavia di una immunità senza confini. Alla *subsection* (e) sono fissati alcuni paletti. Si tratta di un elenco di cinque casi che fuoriescono dall'area di operatività del regime di impunità. Nello specifico, il *legal shield* offerto dalla Section 230 non può essere invocato nell'ambito di cause giudiziarie riguardanti: (1) il diritto penale federale; (2) il diritto della proprietà intellettuale; (3) le leggi degli Stati federali "in linea" (*consistent*) con la Section 230; (4) determinate leggi in materia di *privacy* nelle comunicazioni elettroniche; (5) talune leggi degli Stati federali in materia di *sex trafficking*, mentre, fatta eccezione per questi corpi normativi, il diritto penale degli Stati federali non rientra nella lista delle eccezioni.

Salvo per l'ultima di queste eccezioni, quello riportato è il testo originario della Section 230, per come introdotto alla fine degli anni '90, il quale è dunque rimasto immutato fino ad oggi. L'unico intervento riformatore che si registra concerne, infatti, l'introduzione dell'eccezione numero cinque, la cui storia è particolarmente interessante per quanto riguarda i profili penali della responsabilità dei *provider.* Prima di ripercorrere le ragioni che hanno portato all'introduzione di questa eccezione, e di esaminarne più nel dettaglio i contenuti, si ritiene utile tratteggiare brevemente il contesto da cui è scaturita la scelta di modificare in tale direzione il testo della Section 230.

2. *L'emersione dei c.d. "*Bad Samaritans*": le "piattaforme illecite"*

Il regime d'immunità per i *provider* nell'ordinamento statunitense nacque con un intento ben preciso. Lo scudo da forme di responsabilità "editoriali" rispondeva alla necessità di tutelare e incentivare gli sforzi che tali operatori implementavano autonomamente nel filtrare i contenuti ospitati sui propri servizi, avendo essi stessi un interesse diretto a che la propria piattaforma fosse sicura e libera da materiali offensivi. In particolare, ciò che preoccupava alla fine degli anni '90 era il rischio che politiche troppo restrittive finissero per frenare il filtro e la rimozione che i *provider* avevano fin da subito iniziato ad eseguire della circolazione di una specifica categoria di materiali illeciti, ossia quelli di pornografia minorile.

Da questa circostanza emerse l'etichetta del "buon Samaritano" (*Good Samaritan*), che andava a indicare quegli operatori privati che, nell'auto-regolazione della propria attività economica, filtravano contenuti offensivi, e che, per questo, dovevano essere tutelati da uno scudo normativo che li proteggesse da forme di responsabilità per quegli stessi contenuti.

Senonché, come si è detto, questa dinamica iniziale ha segnato la fortuna dei servizi digitali, che hanno potuto proliferare e svilupparsi nelle forme del capitalismo dell'informazione che oggi conosciamo. Dalla fine degli anni '90 il contesto delle piattaforme online si è infatti fortemente ampliato e diversificato: la rete ha iniziato a popolarsi di operatori di diverse dimensioni, che offrono servizi di diversa natura, e, non meno rilevante, affianco alle piattaforme che svolgono attività lecite hanno iniziato a nascere spazi online appositamente dedicati allo scambio di materiali illeciti.

Oltre ai c.d. *Good Samaritans*, la rete ha cominciato a popolarsi anche di *Bad Samaritans*[6], ovverosia gestori di servizi digitali che, attraverso comportamenti attivi od omissivi, contribuiscono, a vario titolo, alla diffusione e veicolazione di materiali illeciti sui propri siti, di frequente ricavando anche un profitto dalle attività in questione.

Può trattarsi di gestori che aprono piattaforme su cui essi stessi caricano autonomamente materiali offensivi, rendendosi così direttamente responsabili per i reati integrati dalla pubblicazione e diffusione di tali materiali, oppure di soggetti che offrono piattaforme su cui gli utenti possono liberamente caricare contenuti offensivi. Si tratta, per vero, di una casistica che concerne più facilmente i siti che popolano il c.d. *dark web*, ossia quella parte "nascosta" di Internet, a cui si può accedere attraverso specifici *browser* (il più famoso è TOR), e in cui proliferano attività illecite online ospitate in siti che non sono indicizzati e che sono quindi più complessi da intercettare[7]. Tuttavia, si possono avere siti di tale fattezza anche nel c.d. *deep web*, ossia quella parte di Internet non nascosta, ma "sommersa", che rimane liberamente accessibile a chiunque, ma che non risulta tra i primi risultati indicizzati sui motori di ricerca[8].

È stata l'emersione di tali spazi online, che potremmo definire con l'etichetta di "piattaforme illecite", a destare l'interesse del legislatore statunitense, il quale si è tuttavia concentrato sul contrasto a una specifica categoria di contenuti offensivi, ossia quelli sessualmente connotati.

Il primo e unico intervento modificativo della Section 230, che esamineremo a breve, trasse infatti origine da un contesto preciso d'attività in rete, legato alle vicende di un caso concreto, che suscitò un deciso interesse mediatico: il c.d. caso *Backpage.*

Si trattava di un grande operatore di servizi di annunci online, attraverso cui gli utenti potevano pubblicare avvisi di diverso tipo e che, tra i contenuti veicolati, permetteva la pubblicazione di annunci pubblicitari di servizi a sfondo sessuale riguardanti anche

[6] Così D. Citron, *How to fix Section 230*, in «Boston University Law Review», 103 (2023), p. 724, che descrive I "*Bad Samaritans*" come quei «*sites that deliberately solicited privacy violations (…), sites that purposefully enhanced the visibility of illegality while ensuring that perpetrators could not be identified*».

[7] Sul punto cfr. S. Braschi, Social media *e responsabilità penale dell'Internet Service Provider*, in «Rivista di diritto dei media», 3, (2020), p. 16 ss. nonché già D. Petrini, *La responsabilità penale per i reati via Internet*, Jovene, Napoli, 2004, p. 151 ss.

[8] Alcune studiose americane hanno effettuato un'indagine sui siti che monetizzano gli annunci pubblicitari associati a materiali di pornografia non consensuale, al cui caricamento gli stessi gestori sollecitano. Cfr. D. Citron, *The fight for privacy: protecting dignity, identity, and love in the digital age*, Norton & Company, New York, 2022, p. 72 ss.

minori, o connessi a forme di traffico d'esseri umani a scopo sessuale (*sex trafficking*)[9]. L'"effettiva conoscenza" (*actual knowledge*) della piattaforma di tali contenuti si poteva evincere dalle *policies* interne di moderazione, che prevedevano un contributo attivo dei gestori nell'*editing* delle inserzioni in questione. Attraverso, prima, un *software* automatico, poi l'opera di un moderatore, gli avvisi contenenti *"flagged words"*, ossia parole chiave che potevano rendere manifesta l'illiceità dei servizi offerti (come "*lolita*, *teenage*, *rape*, *young*, *little girl*, *teen*, *fresh*, *innocent*, *school girl*"), venivano rivisti così da mantenere l'accessibilità dei materiali sulla piattaforma.

Il caso diede origine a numerose vicende giudiziarie, sia civili che penali. Soffermandosi su queste ultime, il primo processo venne istruito in California, all'interno dunque del sistema di corti di diritto statale, non federale, su iniziativa del procuratore generale dello Stato, che chiedeva la condanna dei gestori del sito (persone fisiche) per concorso nel reato di sfruttamento della prostituzione (*Pimping, California Penal Code § 266h*)[10]. La vicenda si concluse con l'assoluzione dei gestori in virtù dell'operatività del regime di immunità della Section 230. I gestori della piattaforma non furono ritenuti responsabili per concorso nel reato di sfruttamento della prostituzione, inclusa la prostituzione minorile, dal momento che l'eccezione della *subsection* (e)(1) prevedeva l'esclusione del regime d'immunità solamente rispetto ai procedimenti di diritto penale federale, mentre l'ambito del diritto penale statale rimaneva ricompreso nell'operatività della Section 230.

3. *Il bipolarismo regolatorio tra protezionismo del* free speech *e contrasto dei contenuti sessualmente connotati: la legge FOSTA*

In risposta al caso *Backpage* il legislatore statunitense intervenne, nel 2018, sulle eccezioni in grado di sollevare lo scudo d'immunità della Section 230.

Nonostante il diritto penale federale facesse già eccezione all'immunità prevista dalla Section 230, non si registravano casi in cui la previsione era stata fatta valere dai procuratori statunitensi. La scelta di delimitare l'eccezione al solo diritto penale federale si è rivelata infatti poco efficace, anche in considerazione della struttura del sistema di giustizia americano: lasciando fuori il diritto penale statale ci si preclude la

[9] In una lettera inviata alla piattaforma quarantacinque procuratori statali scrissero di aver rintracciato più di cinquanta casi in tre anni di sfruttamento sessuale di minori realizzati attraverso la pubblicazione di annunci sul sito Backpage. Così KOSSEFF, *The Twenty-Six Words*, cit., p. 301.

[10] People v. Ferrer, No. 16FE019224 (Cal. Super. Ct. 2016). Dove viene specificato che non vi sia un contributo materiale nella messa a disposizione delle informazioni tale da poter qualificare il provider quale *content provider*: «*Here, the People acknowledge that advertisements are placed by third parties and Backpage's edits "would not change the users' intent." Nor is there an allegation that Defendant(s) set up the website to require offensive content to be supplied, as in Roommates, Bollaert or Dirty World. As such, there is no material contribution to the offensive content in the advertisements, and the allegations reference traditional publisher functions*». Più diffusamente su questo si veda il prossimo paragrafo.

possibilità di legare forme di responsabilità dei *provider* a un ventaglio molto più ampio di fattispecie penali, disciplinate nei codici dei diversi Stati federali, e, al contempo, impedisce la possibilità di usufruire di un bacino di risorse operative considerevolmente maggiore nell'apparato dell'amministrazione della giustizia americana.

Il Congresso statunitense arrivò così ad approvare il primo atto modificativo della Section 230 dalla sua entrata in vigore. Nel 2018 fu ampliata la lista delle eccezioni di cui alla *subsection* (e) per ricomprendere le previsioni di diritto penale statale riguardanti il contrasto al *sex trafficking*[11].

La nuova *subsection* (e)(5) prevede ora che il gestore di un servizio digitale non possa invocare l'immunità in: (A)-(B) procedimenti civili e penali, secondo il diritto penale statale, riguardanti i reati previsti in materia di schiavitù e traffico di persone (18 U.S.C. Chapter 77 - *Peonage, slavery, and trafficking in persons*); (C) procedimenti penali, secondo il diritto penale statale, riguardanti il reato federale di facilitazione della prostituzione realizzato tramite servizi digitali (18 U.S.C. § 2421A - *Promotion or facilitation of prostitution and reckless disregard of sex trafficking*[12]), laddove la promozione o l'agevolazione della prostituzione sia illegale nella giurisdizione in cui l'imputato ha realizzato la condotta. Quest'ultimo reato è stato introdotto con la stessa legge che ha modificato la Section 230 (c.d. legge FOSTA[13]) e il collegamento con la vicenda *Beckpage* risulta evidente.

[11] L'approvazione di questa nuova eccezione determinò l'istruzione di nuovi processi penali nei confronti dei gestori del sito di Backpage (prima sequestrato e poi reso inattivo), sia a livello statale che a livello federale. Mentre uno degli imputati si è dichiarato colpevole a titolo di concorso nel reato di facilitazione della prostituzione, il processo federale nei confronti degli altri imputati si è recentemente concluso con la condanna di questi allo stesso titolo. Si vedano i processi nelle corti statali della California e del Texas (dove il CEO del sito, si è dichiarato colpevole del reato di facilitazione alla prostituzione), così come nella corte federale dell'Arizona (United States v. Lacey et al., No. CR-18-00422-001-PHX-SPL (D. Ariz. Oct. 18, 2018), attualmente è in corso di pubblicazione la sentenza che conferma la condanna degli altri soggetti responsabili della gestione della piattaforma.

[12] La fattispecie punisce, con multa e/o reclusione massima di 10 anni, chiunque, (…), possiede, gestisce od opera un servizio informatico interattivo (come definito nell'articolo 230(f) del CDA), o cospira o cerca di farlo, con il fine di promuovere o agevolare la prostituzione di un'altra persona. La pena si aggrava (multa e/o reclusione massima di 25 anni) quando la promozione o agevolazione della prostituzione coinvolge 5 o più persone, nonché nel caso in cui il soggetto agisca con imprudenza ('*reckless disregard*') del fatto che la sua condotta contribuisca alla tratta di persone a scopi sessuali. Si riporta il testo in lingua originale: «*(a) In General. - Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, owns, manages, or operates an interactive computer service (…), or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person shall be fined under this title, imprisoned for not more than 10 years, or both. (b) Aggravated Violation. - Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, owns, manages, or operates an interactive computer service (…), or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person and: (1) promotes or facilitates the prostitution of 5 or more persons; or (2) acts in reckless disregard of the fact that such conduct contributed to sex trafficking, in violation of [2] 1591(a), shall be fined under this title, imprisoned for not more than 25 years, or both*».

[13] Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), Pub. L. No. 115-164, § 4, 132 Stat. 1253 (2018).

Assieme all'introduzione di questa nuova eccezione, la legge FOSTA ha ampliato i reati federali in materia di *sex trafficking*, incriminando le condotte di chiunque assista, supporti o faciliti "*knowingly*"[14] pratiche di *sex trafficking* (18 U.S.C. § 1591)[15].

Dato emblematico è che, dall'approvazione della legge FOSTA alla data di uno dei più recenti commenti in letteratura[16], non si registrano procedimenti penali aperti dai procuratori degli Stati americani contro piattaforme ricorrendo all'eccezione della *subsection* (e)(5), ad esclusione dei casi menzionati riguardanti la vicenda *Backpage*, i cui capi d'accusa non comprendono però il reato di cui al § 2421A. Anche in quest'ultima vicenda, infatti, la nuova legge non ha avuto l'effetto deterrente e preventivo desiderato, se si considera che, una volta messo fuori servizio il sito, nuove versioni dello stesso (OneBackpage.com o Backpage.ly) sono emerse con *server* in Polonia, in cui si legge il *disclaimer*, «*FOSTA-SESTA—No operator of this site reviews content or otherwise screens the content of this site*»[17].

In effetti, la nuova eccezione e i reati introdotti dalla legge FOSTA hanno sollevato numerose critiche, in particolare a causa dell'utilizzo di espressioni non sufficientemente determinate (come quella di "*knowingly assisting*"[18]) e in generale per la scelta

[14] L'introduzione dello standard della *knowledge* affianco alle condotte di partecipazione intende rispondere ad esigenze di contenimento dell'intervento punitivo, dal momento che aggiunge un elemento che l'accusa deve provare per accertare la responsabilità dell'imputato. I gradi della *mens rea* nel diritto penale statunitense (*Purpose, Knowledge, Recklessness, and Negligence (PKRN) mens rea*) si possono trovare definiti nella section 2.02 del Model Penal Code. Tra i più recenti contributi, che evidenziano i limiti del *MPC's grading system* si veda G. ANTILL, *Fitting the Model Penal Code into a Reasons- Responsiveness Picture of Culpability*, in *Yale Law Journal*, 2022, 131(4), p. 1346 ss. Nel diritto penale americano il requisito della *knowledge* comporta la necessità di provare uno *state of mind* vicino al grado della certezza («*a person acts knowingly with respect to a material element of an offense when: (i) if the element involves the nature of his conduct or the attendant circumstances, he is aware that his conduct is of that nature or that such circumstances exist; and (ii) if the element involves a result of his conduct, he is aware that it is practically certain that his conduct will cause such a result*», Model Penal Code § 2.02(2)(b)). Si richiede quindi che il soggetto sia «*praticamente certo*» del risultato della sua condotta, cfr. G.P. FLETCHER, *Rethinking Criminal Law*, Oxfrord University Press, Oxford, 2000, p. 446, o, più precisamente, che sia «*aware of a high probability of its existence, unless he actually believes that it does not exist*».

[15] In lingua originale: «*knowingly assisting, supporting, or facilitating*».

[16] CITRON, *How to fix*, cit., p. 737 ss.

[17] *Ibidem*.

[18] Il requisito della *knowledge* è stato interpretato in modo molto estensivo, contribuendo all'ambiguità dei suoi contorni. Cfr. W. LAFAVE, J.D. OHLIN'S *Criminal Law*, 7th, Hornbook Series, St. Paul, 2023, p. 325, dove si riporta che «*the word "knowledge" has (…) sometimes been given a broader definition. Cases have held that one has knowledge of a given fact when he has the means for obtaining such knowledge, when he has notice of facts which would put one on inquiry as to the existence of that fact, when he has information sufficient to generate a reasonable belief as to that fact, or when the circumstances are such that a reasonable man would believe that such a fact existed*». Considerato che la consapevole facilitazione di pratiche illecite deve fare i conti con la circolazione di numerosi contenuti, alle volte non sempre manifestatamente illeciti, questo può comportare una difficile applicazione della norma, così come forti reazioni difensive per l'incertezza circa l'interpretazione che le corti possano dare del requisito. Cfr. M. MCKNELLY, *Untangling Sesta/Fosta: How The Internet's "Knowledge" Threatens Anti-Sex Trafficking Law*, in «Berkeley Technology Law Journal» 34/4 (2019), p. 1254 ss., la quale evidenzia come «*In enacting FOSTA, Congress did not explain what might constitute ICS knowledge. Nor did FOSTA explain what an ICS's knowledge looks like in the context of monitoring user content*».

di incriminazione operata. La diretta criminalizzazione delle condotte di possedere, gestire od operare servizi digitali con il fine di facilitare la prostituzione o pratiche di traffico di esseri umani a scopo sessuale tramite piattaforme online (con pene molto gravi), così come l'estensione dei comportamenti penalmente rilevanti a quelli della "consapevole assistenza, supporto o facilitazione", hanno condotto i gestori dei servizi digitali a porre in essere "aggressive" pratiche di moderazione dei contenuti ospitati, per dar prova della loro mancata conoscenza di eventuali materiali che potessero qualificarsi quali *forced prostitution* o *sex trafficking*.

Il caso FOSTA ha resuscitato così il dilemma del moderatore, che stava alla base dell'introduzione della Section 230 alla fine degli anni '90[19]. I meccanismi d'attribuzione della responsabilità penale fondati su politiche di incriminazione di comportamenti direttamente connessi alla gestione dei contenuti legano infatti l'accertamento della responsabilità alle politiche di moderazione dei contenuti prescelte ed attuate dal gestore del servizio. Tale meccanismo induce quindi le piattaforme a dover scegliere tra due alternative: (i) moderare tutti i contenuti con l'accettazione di un determinato livello di rischio, potendo però scivolare in forme di "moderazione aggressiva"; (ii) astenersi da qualsiasi moderazione (fino ad arrivare, in alcuni casi, alla completa sospensione di certi servizi), in modo da dimostrare l'assenza di conoscenza dei contenuti illeciti, soprattutto quando l'oggetto dello standard di prova della *knowledge* potrebbe problematicamente riferirsi a una *knowledge* circa la generale realizzazione di attività illecite sulle proprie piattaforme[20].

A seguito degli effetti connessi all'introduzione della legge FOSTA, si è sottolineato come le pratiche di *over-removal* di contenuti sessuali possano tradursi in una rimozione di qualsiasi contenuto relativo alla sfera sessuale, senza che ciò abbia nulla a che fare con pratiche di *sex trafficking*, con gravi ripercussioni sulla manifestazione della libertà sessuale online, e incidendo soprattutto su determinate categorie di contenuti espressivi, come i contenuti *queer*[21].

Inoltre, è stato denunciato come un atteggiamento fortemente difensivo da parte delle piattaforme, volto a limitare o bloccare qualsiasi tipo di attività anche solo connessa o indirettamente collegata a pratiche di prostituzione, possa limitare la possibilità per i *sex workers* di organizzare in sicurezza pratiche di prostituzione, laddove lecita, attraverso piattaforme digitali di comunicazione e offerta online, così come di utilizzare servizi di messaggistica e comunicazione digitale per esprimersi liberamente o cercare supporto attraverso la rete[22].

[19] Così E. GOLDMAN, *The Complicated Story Of Fosta And Section 230*, in «First Amendment Law Review», 17 (2019), p. 288.

[20] In letteratura si suggerisce di interpretare il requisite della *knowledge* non in termini generali, ma quale «*actual knowledge of specific sex trafficking on the website and yet continue to encourage the behavior*», così KOSSEFF, *The Twenty-Six Words*, cit., p. 272.

[21] Ossia contenuti con cui si manifesta la comunità LGBTQ+. Cfr. A.E. WALDMAN, *Disorderly Content*, in «Washington Law Review», 97 (2022), p. 907 ss., disponibile al sito <https://ssrn.com/abstract=3906001>.

[22] CITRON, *How to fix*, cit., p. 737 ss.

Il FOSTA attesta quindi come la scelta di una politica punitiva che scelga di estendere forme di responsabilità penale degli intermediari attraverso l'introduzione di nuove fattispecie incriminatrici abbia un impatto diretto sulle politiche aziendali di moderazione dei contenuti circolanti online su larga scala. L'*over-removal* è stata la risposta generalizzata al timore di incorrere in responsabilità penale dell'intera categoria, senza distinzioni tra piccole e grandi piattaforme, o tra piattaforme lecite e illecite.

Oltre alle ripercussioni sulle strategie di moderazione, il FOSTA ha messo in luce come i paradigmi d'attribuzione della responsabilità penale in capo alle piattaforme per i contenuti caricati e veicolati dai propri utenti evidenzino ulteriori problematiche. L'addebito di responsabilità delle piattaforme, secondo l'eccezione inserita nella Section 230, risente infatti di un principale ostacolo, riguardante l'elemento soggettivo.

Come dimostra un recente caso, si è stabilito che la responsabilità per i reati di *sex trafficking* non possa accertarsi se non si dimostri che la piattaforma, anche se generalmente a conoscenza che il proprio servizio sia utilizzato abusivamente dai propri utenti (in questo caso, soggetti che adescavano minori e li forzavano, attraverso minacce, a realizzare atti sessuali online), sia effettivamente a conoscenza dello specifico reato realizzato a danno della vittima[23]. Affinché il regime del FOSTA operi, è quindi necessario accertare che la piattaforma abbia «*specific and identifiable instances*» dei reati di *sex trafficking* contestati.

Riscontrare la colpevolezza dei gestori della piattaforma in questi termini diventa quindi particolarmente complesso, soprattutto in caso di piattaforme di medie o grandi dimensioni, in cui la conoscenza specifica e diretta circa un singolo contenuto illecito talvolta non sussiste, talaltra è difficilmente accertabile.

La riforma attuata con il FOSTA evidenzia quindi come il perseguimento dell'obiettivo di erodere lo schermo delle immunità attraverso il solo ampliamento delle forme di responsabilità penale e la previsione di nuovi reati rappresenti una strategia di politica criminale discutibile. Concentrarsi esclusivamente sulla rimozione delle tutele, senza accompagnare questa scelta con una regolamentazione strutturata del settore, rischia di produrre effetti distorsivi e controproducenti.

Se dunque l'obiettivo di politica criminale è condivisibile, il metodo adottato per perseguirlo appare inadeguato. Invece di promuovere la creazione un sistema normativo chiaro ed equilibrato, si è percorsa una strada che aumenta la pressione sugli operatori senza fornire linee guida precise, generando incertezza e potenzialmente ostacolando lo sviluppo del settore in questione.

[23] Si veda M.H. & J.H. v. Omegle.com, LLC, 2022 WL 93575 (M.D. Fla. January 10, 2022), caso in cui una minore di undici anni incontrò un predatore sulla piattaforma Omegle, il quale, dicendo di conoscere il suo luogo di abitazione e minacciando di *hackerare* i dispositivi elettronici della sua famiglia, la costrinse a spogliarsi di fronte alla videocamera. Il tribunale ha ritenuto che la richiesta di risarcimento avanzata dai genitori della vittima non soddisfacesse l'eccezione del FOSTA alla sezione 230, dal momento che non erano riusciti a dimostrare che Omegle.com fosse effettivamente a conoscenza dell'abuso sessuale e che traesse vantaggio da tale attività. Il tribunale ha inoltre affermato che l'eccezione FOSTA alla sezione 230 richiede una *actual knowledge* del *sex trafficking*, non solo una *constructive knowledge*.

Un ulteriore elemento che si raccoglie dalla ricostruzione delle fonti dell'ordinamento statunitense riguarda il bipolarismo delle politiche legislative in materia di contenuti illeciti in rete e responsabilità degli intermediari.

Si può tratteggiare, infatti, una evidente tensione tra il forte protezionismo in relazione al *free speech* e l'altrettanto marcato paternalismo in relazione ai contenuti sessualmente connotati. Da un lato, rimangono salde le politiche volte a tutelare la libera circolazione di contenuti in rete, che si traducono in una decisa salvaguardia del regime d'immunità di cui alla Section 230 per la generalità dei contenuti circolanti online, che ancora oggi diversi studiosi ritengono irrinunciabile[24], per evitare il *chilling effect* sulla vita in rete che sarebbe generato da politiche di segno contrario. Dall'altro lato, invece, si contrappone un forte paternalismo in relazione a contenuti sessualmente connotati.

A partire dalla legge FOSTA, si registra, infatti, un rafforzamento di questa linea politico criminale, se si considera anche uno degli ultimi interventi in materia, ossia l'introduzione del c.d. *Take it down act*, approvato dal Congresso il 28 aprile 2025[25], il quale, senza incidere sulla Section 230, che rimane quindi immutata, da un lato, incrimina, inserendo una nuova *subsection* (h) alla Section 47 U.S.C. 223, la diffusione non consensuale di materiali sessualmente connotati («*intimate visual depiction*»)[26], sia che si tratti di materiale "autentico" sia che riguardi materiale "falsificato digitalmente"[27], e, dall'altro lato, impone alle piattaforme l'obbligo di rimuovere il prima possibile le «*intimate visual depiction*» della cui pubblicazione sui propri servizi ricevono una valida notifica da un soggetto identificabile.

Si rileva, dunque, come un tale bipolarismo nelle politiche di contrasto ai contenuti illeciti in rete potrebbe generare un forte squilibrio regolatorio tra contenuti sessualmente connotati e tutti gli altri contenuti, per cui il dilemma del moderatore sarebbe destinato a polarizzarsi: tutto ciò che è anche solo connesso alla sfera sessuale potrebbe essere bloccato, mentre tutto il resto può essere lasciato liberamente online.

[24] Questa la posizione di KOSSEFF, *The Twenty-Six Words*, cit., p. 325 ss.

[25] Law No: 119-12 del 19 maggio 2025, *Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act* (c.d. Take it down Act).

[26] La definizione del termine deve rintracciarsi al 15 U.S.C. 6851(5), secondo cui «*intimate visual depiction*» ricomprende: (A) la rappresentazione visiva di: «*(i) the uncovered genitals, pubic area, anus, or post-pubescent female nipple of an identifiable individual; or (ii) the display or transfer of bodily sexual fluids- (I) on to any part of the body of an identifiable individual; (II) from the body of an identifiable individual; or (III) an identifiable individual engaging in sexually explicit conduct*», e (B) le suddette rappresentazioni visive «*produced while the identifiable individual was in a public place only if the individual did not: (i) voluntarily display the content depicted; or (ii) consent to the sexual conduct depicted*».

[27] Il termine "falsificazione digitale", ai sensi del nuovo 47 U.S.C. 223(h)(1)(B), indica qualsiasi rappresentazione visiva intima di un individuo identificabile creata mediante l'uso di software, apprendimento automatico, intelligenza artificiale o qualsiasi altro mezzo tecnologico o generato da computer, incluso l'adattamento, la modifica, la manipolazione o l'alterazione di una rappresentazione visiva autentica, che, quando viene osservata nel suo insieme da una persona ragionevole, risulta indistinguibile da una rappresentazione visiva autentica dell'individuo.

4. *Il contrasto alle "piattaforme illecite" nella prospettiva interna*

L'esperienza statunitense contribuisce a evidenziare l'emersione di una problematica effettiva, ossia la necessità di distinguere, sul piano regolatorio e nella distribuzione di forme di responsabilità, anche penali, la categoria delle piattaforme lecite da quella delle piattaforme illecite. Distinzione che non è tuttavia stata sufficientemente colta e valorizzata nelle politiche americane, nel quadro che si è brevemente sopra tratteggiato.

Passando ora al piano di diritto interno, nonostante l'espandersi del fenomeno dei contenuti illeciti online, nell'ordinamento italiano non è stata finora introdotta alcuna fattispecie che vada ad incriminare comportamenti direttamente riferibili a gestori di piattaforme, strada che occorre continuare a percorrere sul piano legislativo, per invece rafforzare l'interesse della prassi attorno al fenomeno criminoso connesso alle c.d. piattaforme illecite, che si ritiene invece sia poco attenzionato, e, come si dirà a breve, già contrastabile con gli strumenti messi a disposizione dall'ordinamento penale.

In tal senso, l'incriminazione, in funzione marcatamente preventiva, della generica "creazione", "gestione" od "operatività" di siti, finalizzata allo scambio di contenuti illeciti, rispetto a cui si registra, peraltro, qualche proposta a livello europeo[28], va incontro a diversi rilievi critici.

Oltre al caso portato dall'esperienza comprata statunitense, un'ulteriore argomentazione che depone contro siffatte soluzioni normative si può ricavare anche dall'esperienza dell'ordinamento tedesco, che ha introdotto, al § 127 dello StGB, una fattispecie che punisce chiunque gestisca piattaforme commerciali il cui scopo è quello di facilitare o promuovere la commissione di determinati reati, espressamente richiamati dalla norma stessa[29]. Il perimetro della norma ricomprende qualsiasi piattaforma "commerciale" (ossia qualsiasi infrastruttura digitale che fornisce la possibilità di offerta e scambio tra persone, beni, servizi o contenuti), rispetto a cui rimane dubbia l'inclusione dei servizi di condivisione di contenuti che non comprendono uno scambio economico[30].

[28] Si veda l'articolo 8 della proposta di direttiva del 6 febbraio 2024 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e il materiale pedopornografico, e che sostituisce la decisione quadro 2004/68/GAI, (COM(2024) 60 *final*), che istituirebbe un obbligo di criminalizzazione della gestione di un servizio online a fini di abuso o sfruttamento sessuale dei minori. Ai sensi della norma proposta: «Gli Stati membri adottano le misure necessarie affinché l'erogazione o la gestione intenzionale di un servizio della società dell'informazione destinato a favorire o incoraggiare la commissione di uno dei reati di cui agli articoli da 3 a 7 sia punita con una pena detentiva massima di almeno un anno».

[29] Il § 127 del codice penale tedesco («*Betreiben krimineller Handelsplattformen im Internet*») punisce chi gestisce una piattaforma commerciale su Internet il cui scopo è volto a consentire o favorire la commissione di atti illeciti. Con «atti illecite» si intende: la commissione di reati espressamente richiamati nella norma (tra questi, entro un lungo elenco, figurano reati contro l'ordine pubblico, di pornografia minorile, reati in materia di terrorismo, traffico di sostanze stupefacenti e di armi, proprietà intellettuale). Per un commento alla norma cfr. T. KULHANEK, § 127, in B. VON HEINTSCHEL-HEINEGG, H. KUDLICH, *Strafgesetzbuch Kommentar*, 64 ed., 2025, Monaco, Rn. 13-18 (BeckOK StGB/Kulhanek, 64. Ed. 1.2.2025, StGB § 127); T. BÄCHER, *Zur strafrechtlichen Verantwortlichkeit des Betreibers einer Plattform im Darknet*, Duncker & Humblot, Berlin, 2024, p. 204 ss.

[30] Si è criticato l'aggettivo "commerciale", siccome si cercava di far rientrare tra i destinatari del divieto anche le piattaforme di condivisioni di contenuti, pur in assenza di uno scambio economico per tale opera di

Entro il bilanciamento tra i benefici che potrebbe avere l'introduzione di una simile fattispecie (nei termini di un'eventuale maggiore certezza dei confini tra lecito ed illecito nel settore delle attività dell'economia digitale) e i costi che ne deriverebbero (connessi al rischio di fenomeni di espansione del diritto penale per via dell'elasticità della previsione) sembrano decisamente prevalere i secondi. Va peraltro rilevato, come evidenziato dalla stessa dottrina tedesca[31], che si tratterebbe di condotte che possono integrare fattispecie di reato già previste dall'ordinamento (come, ad esempio, casi di crimine organizzato)[32], o che, comunque, potrebbero essere inquadrate quali contributi partecipativi rispetto ai reati commessi dai propri utenti, ricorrendo piuttosto al paradigma del concorso commissivo.

Una tale previsione (che definisce in modo indeterminato le condotte incriminate ed è diretta all'intera categoria dei *provider*) potrebbe avere effetti di *overcriminalisation*, con conseguente compromissione del libero fluire della circolazione di informazioni in rete.

Dunque, piuttosto che percorrere la via della incriminazione di nuovi comportamenti, il fenomeno delle piattaforme illecite potrebbe essere affrontato ricorrendo a paradigmi di responsabilità a titolo di concorso commissivo nei reati integrati dalla circolazione di materiali illeciti sui siti da questi gestiti, fuoriuscendo tali soggetti dall'ambito applicativo delle fonti che regolano il settore, prima fra tutte, il regolamento europeo sui servizi digitali 2065/2022, il quale espressamente afferma, al considerando n. 20, che: «qualora un prestatore di servizi intermediari *deliberatamente collabori* con un

condivisione. È stato infatti proposto di modificare la dicitura di "piattaforme commerciali" nel termine più generico di "piattaforme", proposta che però non è stata accolta perché avrebbe reso il fatto "senza contorni". Si vedano i documenti sulla discussione al progetto di legge (BT-Drs. 19/28175, 26) di introduzione del reato di cui al § 127 (*Empfehlungen der Ausschüsse zu Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches - Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet und des Bereitstellens entsprechender Server-Infrastrukturen*, BR-Drs. 147/1/21, 2).

[31] Si vedano, in commento alla fase di approvazione della disposizione, le dichiarazioni degli esperti, prof. Mark A. Zöller e prof. Matthias Jahn, disponibili al sito <https://www.bundestag.de/dokumente/textarchiv/2021/kw18-pa-recht-handelsplattformen-835714>.

[32] Nel caso in cui le attività di tali piattaforme siano eseguite in forma organizzata, esse potrebbero ricondursi a forme di crimine organizzato "digitale", Sul punto si veda BÄCHER, *Zur strafrechtlichen Verantwortlichkeit*, cit., p. 92 ss., che prospetta l'applicabilità in questi casi del reato di *Bildung krimineller Vereinigungen* di cui al § 129 StGB. Il concetto di crimine organizzato nella società digitale deve peraltro essere distinto tra crimine organizzato "tradizionale", che si serve delle nuove opportunità dischiuse dalla rivoluzione digitale per realizzare le più disparate attività criminali, e crimine informatico organizzato (detto anche *cyber-organized crime*), dove organizzazioni criminali sono costruite per realizzare reati informatici su larga scala. Nel contesto delle piattaforme online rileva infatti il primo di questi due insiemi. Per analisi del c.d. *cyber-organized crime*, si vedano R. FLOR, L. LUPARIA, *Criminalità organizzata e criminalità informatica ("cyber-organized-crime")*, in *Stati generali della lotta alle mafie tavolo XV – "Mafie e Europa"*, a cura di A.M. Maugeri, 2019, p. 206 ss., disponibile su <dirittopenalecontemporaneo.it>; G. MORGANTE, *L'estensione dello statuto penale della criminalità organizzata di stampo mafioso alla cybercriminalità diretta contro sistemi informatici e telematici*, in «Riv. it. inf. dir.», (2024), p. 41 ss.; S. SICURELLA, *Le mafie italiane nel cyberspazio: nuova frontiera o terreno di sperimentazione?*, in «Rivista di criminologia, vittimologia e sicurezza», (2022), p. 22 ss.; A. DI NICOLA, *Towards digital organized crime and digital sociology of organized crime*, in «Trends in Organized Crime», (2022), p. 1 ss.

destinatario dei servizi al fine di commettere attività illegali, i servizi non dovrebbero essere considerati come forniti in modo neutro e il prestatore non dovrebbe pertanto poter beneficiare delle esenzioni dalla responsabilità di cui al presente regolamento. Dovrebbe essere così, ad esempio, quando il prestatore offre il proprio servizio con lo scopo principale di agevolare attività illegali, come quando indica esplicitamente che il suo scopo è agevolare attività illegali o che i suoi servizi sono adatti a tal fine».

L'INTELLIGENZA ARTIFICIALE NELLO "SPAZIO DIGITALE": PROFILI PENALISTICI E NUOVE SFIDE REGOLATORIE

Olimpia Barresi

1. *Premessa: la linea di continuità e la "strategia regolatoria" del legislatore europeo*

La recente normativa sui servizi digitali dell'Unione europea, nota come *Digital Services Act* (DSA)[1] – che costituisce il filo conduttore di tutti gli interventi dell'incontro odierno[2] – rappresenta un cambiamento di portata significativa nella regolamentazione della rete, dal momento che introduce il principio della responsabilità delle grandi piattaforme digitali nel contrasto alla diffusione di contenuti illeciti online.

[1] Il *Digital Services Act* si inserisce nel più ampio contesto della Strategia europea per il mercato unico digitale, agendo in sinergia con il Regolamento (UE) 2022/1925 del 14 settembre 2022, noto come *Digital Markets Act* (DMA), che mira ad assicurare mercati digitali equi e contendibili. Quest'ultimo modifica le direttive (UE) 2019/1937 e (UE) 2020/1828, intervenendo su aspetti fondamentali della regolamentazione digitale. In particolare, il *Digital Services Act* stabilisce il quadro normativo che disciplina gli obblighi e le responsabilità dei fornitori di servizi intermediari nella distribuzione di beni, servizi e contenuti – inclusi quelli veicolati attraverso i mercati digitali – con l'obiettivo di garantire il corretto funzionamento del mercato interno. In questa prospettiva, il Regolamento introduce norme armonizzate finalizzate a costruire un ecosistema digitale sicuro, trasparente e affidabile. In dottrina, per uno sguardo più completo sulla nuova normativa, si rinvia a F. CASOLARI, *Il* Digital Services Act *e la costituzionalizzazione dello spazio digitale europeo*, in «Giurisprudenza italiana», 2 (2024), p. 462; G. FINOCCHIARO, *"Digital Services Act" - Responsabilità delle piattaforme. Responsabilità delle piattaforme e tutela dei consumatori*, in «Giornale di diritto amministrativo», 6 (2023), pp. 730 ss.

[2] L'evento si inserisce nell'ambito di un progetto di ricerca, finanziato da *Alphabet/Google*, con titolo "*Leveling the field. Clarifying the notion of illegal content under the EU's Digital Services Act*", attualmente in corso presso l'Università di Bologna e l'Università di Bolzano.

A far da sfondo ai diversi temi tra loro interconnessi è la nozione di "contenuto illecito" che appare, tuttavia, definita in modo sfumato dal *Digital Services Act*[3] che, difatti, a sua volta rinvia alla normativa euro-unitaria e alle diverse legislazioni nazionali degli Stati membri dell'Unione[4]. Proprio a partire dall'indeterminatezza del concetto emerge la potenziale ampiezza dei fenomeni criminosi coinvolti che, lontani da logiche di armonizzazione, sollevano rilevanti questioni interpretative, in merito all'individuazione delle condotte penalmente rilevanti poste in essere dagli utenti e suscettibili di generare obblighi a carico delle piattaforme digitali[5].

Nel contesto attuale delle politiche digitali e del recente approccio regolatorio del legislatore europeo[6], il DSA, affiancato dall'*Artificial Intelligence Act*, riveste un ruolo centrale, configurandosi come uno degli strumenti normativi di riferimento per la regolazione delle trasformazioni future; queste ultime, sospinte da un progresso tecnologico sempre più rapido e imprevedibile, segnano una netta discontinuità rispetto ai paradigmi regolatori del passato[7]. A ben vedere, parallelamente alla rapida e dirompente evoluzione tecnologica, segnata dall'emergere di strumenti sempre più sofisticati, il diritto penale è chiamato a confrontarsi con nuove sfide e interrogativi[8].

Oltre a delineare i principali fondamenti teorici e normativi della responsabilità dei *provider* e *deployer*, l'intervento odierno si propone, pertanto, di valutare se, a fronte dei nuovi rischi che si manifestano nello spazio digitale, le recenti regolamentazioni europee – le quali a un primo esame appaiono strutturate in un'ottica di complementarità – possano offrire strumenti efficaci per il contrasto di alcuni fenomeni, nel rispetto delle garanzie fondamentali. Invero, la crescente necessità di un coordinamento tra i nuovi strumenti normativi adottati a livello europeo impone una riflessione ad ampio spettro, mossa dalla consapevolezza che risulterebbe incoerente considerare ammissibili, nell'ambito del *Digital Services Act*[9], quei rischi che l'*Artificial Intelligence Act*

[3] Art. 3, lett. h, "'illegal content' *means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law*".

[4] A ben vedere, il Regolamento sui servizi digitali, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 27 ottobre 2022, sembra destinato a modificare in misura rilevante lo statuto di responsabilità degli *Internet Service Provider*.

[5] Pur riconoscendo il valore di questa nuova regolamentazione, che introduce misure volte a limitare i discorsi d'odio e, più in generale, la diffusione di contenuti illeciti, alcune voci critiche evidenziano fin da ora una sua possibile lacuna: l'incapacità di includere pienamente al proprio interno tutti i modelli di intelligenza artificiale generativa, in particolare quelli che operano su grandi volumi di dati.

[6] P. De Hert, V. Papakostantinou, *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'*, in «Technology and Regulation Journal» (2022).

[7] L'Unione Europea ha sviluppato una serie di normative per regolamentare i contenuti illeciti online, con l'obiettivo di proteggere gli utenti e garantire un ambiente digitale più sicuro. Le principali normative in questo ambito sono il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA), che affrontano, sebbene in modi diversi, la gestione dei contenuti online.

[8] Per un primo e generale quadro di insieme si rimanda a F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in «Diritto Penale e Uomo», 10 (2019), p. 4.

[9] Così come espressamente previsto dall'art. 35 del DSA.

qualifica come inaccettabili[10]. Tali considerazioni dovranno necessariamente tenere conto del fatto che, pur condividendo l'obiettivo di tutelare i diritti fondamentali con un'azione di contrappeso rispetto al predominio delle logiche potenzialmente soggette a derive tecnocratiche[11], l'*Artificial Intelligence Act* e il *Digital Services Act* rappresentano espressioni profondamente differenti dell'approccio al rischio adottato dal legislatore europeo[12].

2. *Brevi riflessioni sulla prima regolamentazione dell'intelligenza artificiale*

Il rapido sviluppo degli strumenti di intelligenza artificiale (da ora anche IA)[13] ha sollevato interrogativi giuridici, etici e sociali che hanno richiesto un intervento normativo organico a livello sovranazionale[14]. L'Unione Europea ha risposto a tale esigenza mediante l'adozione del Regolamento sull'intelligenza artificiale (*AI Act*)[15], prima normativa europea a stabilire regole armonizzate[16], che rappresenta un tassello fondamentale

[10] Pur non prevedendo un divieto esplicito per tali pratiche, il DSA ne richiede la mitigazione, riconoscendone la potenziale pericolosità. Di conseguenza, anche in assenza di un'espressa interdizione all'interno del DSA, i fornitori di servizi digitali non possono ritenersi legittimati a impiegare sistemi di intelligenza artificiale vietati dall'*AI Act* – come, ad esempio, quelli progettati per manipolare in modo significativo il comportamento degli utenti, compromettendone la libertà decisionale e causando danni rilevanti (art. 5, Reg. UE 1689/2024). Così, S. Tommasi, *Digital Services Act e Artifcial Antelligence Acttentativi di futuro da armonizzare*, in «Persona e Mercato», 2 (2023), p. 285.

[11] Sul binomio tra tecnologia e tecnocrazia, si rinvia a V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in «Discrimen», 15 maggio 2020.

[12] L'*AI Act* richiama la normativa del DSA al *Considerando 120*, dove dispone che «*Furthermore, obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation*».

[13] Per fornire un inquadramento sugli aspetti definitori, l'art. 3 del Regolamento definisce sistema di IA «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

[14] Si ricalca anche in queta scelta, il c.d. "*brutality approach*" che rispecchia la tendenza del più recente approccio dell'UE di "iper-regolamentare" le materie; così sul punto si rimanda a P. De Hert, V. Papakostantinou, *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'*, in «Technology and Regulation Journal» (2022), pp. 48 ss.

[15] Il Regolamento (UE) 2024/1689, noto come *AI Act*, rappresenta il primo quadro normativo completo a livello mondiale dedicato alla regolamentazione dei sistemi di intelligenza artificiale. È stato adottato dal Parlamento europeo e dal Consiglio il 13 giugno 2024 e pubblicato nella Gazzetta ufficiale dell'Unione europea il 12 luglio 2024. Il regolamento è entrato in vigore il 1° agosto 2024.

[16] D. Benedetti, *IA e (in)sicurezza informatica*, in *Intelligenza artificiale*, *protezione dei dati personali e regolazione*, a cura di F. Pizzetti, Giappichelli, Torino, 2018, pp. 253-255.

della strategia digitale dell'UE[17] e che si propone di coniugare l'innovazione tecnologica con la tutela dei diritti fondamentali[18].

Un aspetto centrale del Regolamento riguarda la prevenzione e il contrasto alla produzione e alla diffusione di contenuti illeciti generati da sistemi di IA. A ben vedere, l'impiego dell'intelligenza artificiale[19] rende necessario un coordinamento tra il quadro regolatorio delineato dal *Digital Services Act*[20] e quello previsto dall'*Artificial Intelligence Act*.

Il punto di partenza conduce a un primo interrogativo: quale ruolo riveste l'intelligenza artificiale in relazione ai contenuti illeciti online?

Nell'ambito dei diversi aspetti disciplinati, il Regolamento dedica particolare attenzione alla questione dei contenuti illeciti, riconducibili a un uso improprio o dannoso dell'intelligenza artificiale, e, in particolare, degli strumenti di c.d. IA generativa[21]. Dal punto di vista definitorio, il Regolamento intende per *contenuto illecito* qualsiasi *output* o comportamento generato da un sistema di intelligenza artificiale che violi la legge, i diritti fondamentali o i principi democratici sanciti dalla normativa europea. Ciò può includere: disinformazione e manipolazione (es. *deepfakes* a fini politici o diffamatori); contenuti discriminatori o razzisti generati da modelli di IA; violazioni

[17] Il Regolamento si aggiungerà, infatti, a una serie di normative (tra cui il *Data Act*, il *Data Governance Act*, il *Digital Services Act* e il *Digital Markets Act*), volte a promuovere un mercato unico dei dati, la sicurezza degli ambienti online e a favorire mercati digitali equi e innovativi, nel rispetto dei valori e dei diritti europei. C. Novelli, P. Hacker, J. Morley, J. Trondal, L. Floridi, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in «European Journal of Risk Regulation» (2024); sul punto anche P. Hacker, A. Engel, M. Mauer, *Regulating ChatGPT and other Large Generative AI Models*, (2023), pp. 2 ss.

[18] A ben vedere, l'*AI Act*, al richiamo ai principi del GDPR, fa riferimento agli "Orientamenti etici per un'AI affidabile" elaborati nel 2019 dall'*High-Level Expert Group* on Artificial Intelligence (AI HLEG) della Commissione Europea.

[19] Come dispone il *Considerando 119* «Ad esempio, i sistemi di IA possono essere utilizzati per fornire motori di ricerca online, in particolare nella misura in cui un sistema di IA, come un chatbot online, effettua ricerche, in linea di principio, su tutti i siti web, incorpora i risultati nelle sue conoscenze esistenti e si avvale delle conoscenze aggiornate per generare un unico output che combina diverse fonti di informazione».

[20] All'interno del *Digital Services Act*, i servizi digitali assumono un ruolo centrale. L'impianto normativo si articola attorno a tre principi fondamentali: responsabilità degli operatori, obblighi di diligenza e cooperazione tra autorità competenti. Come accade anche per il *Digital Markets Act*, il criterio per determinare l'ambito territoriale di applicazione non si basa sul luogo in cui ha sede il prestatore del servizio, ma su quello in cui si trova il destinatario, purché situato nell'Unione europea. Il DSA aggiorna e amplia i principi stabiliti dalla direttiva sul commercio elettronico del 2001, introducendo nuovi obblighi per i fornitori di servizi digitali, modulati in base alla tipologia del servizio e alla dimensione dell'operatore. Due principi fondamentali devono essere tenuti in equilibrio: da un lato, il principio secondo cui ciò che è illecito nel mondo offline deve esserlo anche online; dall'altro, il divieto di imporre obblighi generali di sorveglianza o di controllo dei contenuti caricati da terzi. In particolare, i fornitori di servizi di semplice trasmissione dei dati (*mere conduit*) e di memorizzazione temporanea (*caching*) restano esenti da responsabilità per le informazioni trasmesse o archiviate per conto di utenti terzi.

[21] Il nuovo quadro regolatorio sembrerebbe delineare – già a un primo sguardo – uno scenario di cooperazione fra governo, settore privato, ricerca e società civile, allo scopo di definire nuovi *standard* di sicurezza a protezione della *privacy*, dell'uguaglianza e dei diritti civili, che consentano di controllare i rischi connessi alla pervasività delle applicazioni dell'intelligenza artificiale nella vita economica, sociale e politica.

della proprietà intellettuale attraverso la generazione di opere non autorizzate; incitamento all'odio o alla violenza.

Nella sovrapposizione tra queste due normative, è proprio l'*Artificial Intelligence Act*, in coerenza con il *Digital Services Act*, che esclude espressamente ogni forma di incompatibilità (art. 2, par. 5), precisando che gli obblighi previsti per i sistemi di IA si integrano con quelli già introdotti dal DSA, incluso il relativo quadro per la gestione dei rischi destinato alle grandi piattaforme online[22].

2.1. *L'*AI Act *tra "livelli di rischio" e tutela dei diritti fondamentali*

L'approccio basato sul rischio, adottato nell'ambito della recente normativa europea, rappresenta una modalità innovativa che consente di gestire il progresso tecnologico all'interno di un quadro normativo più definito[23]. In questo contesto, l'*Artificial Intelligence Act*, al pari del *Digital Services Act*, propone una disciplina che modula obblighi e responsabilità in funzione del livello di rischio identificato[24], delineando un sistema di regolazione progressiva e proporzionale.

A ben vedere, sebbene il Regolamento non abbia effetti diretti in ambito penale, esso definisce un'area di rischio "consentito", stabilendo requisiti di conformità che consentono ai sistemi di IA di essere ritenuti adeguati alla normativa europea, a condizione che soddisfino determinate condizioni di sicurezza e protezione. Il Regolamento distingue, infatti, diversi livelli di rischio: il rischio "basso" riguarda i sistemi di IA che non presentano minacce significative per i diritti e la sicurezza dei cittadini; il rischio "medio" comprende, invece, i sistemi già regolati da normative esistenti, come il GDPR, per i quali sono richieste misure di trasparenza e responsabilità; il rischio "alto" concerne i sistemi con un impatto potenzialmente significativo e per i quali sono previsti obblighi più stringenti, inclusa la valutazione dell'impatto sui diritti fondamentali;

[22] A tal riguardo, si riporta il *Considerando 118* dell'*AI Act*, che dispone che «disciplina i sistemi di IA e i modelli di IA imponendo determinati requisiti e obblighi agli operatori del mercato pertinenti che li immettono sul mercato, li mettono in servizio o li utilizzano nell'Unione, integrando in tal modo gli obblighi per i prestatori di servizi intermediari che incorporano tali sistemi o modelli nei loro servizi disciplinati dal regolamento (UE) 2022/2065. Nella misura in cui sono integrati in piattaforme online di dimensioni molto grandi designate o motori di ricerca online di dimensioni molto grandi designati, tali sistemi o modelli sono soggetti al quadro di gestione dei rischi di cui al Regolamento (UE) 2022/2065. […] In tale quadro, le piattaforme di dimensioni molto grandi e i motori di ricerca di dimensioni molto grandi sono tenuti a valutare i potenziali rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'utilizzo dei propri servizi – compresi quelli derivanti dalle modalità di progettazione dei sistemi algoritmici impiegati nel servizio o da potenziali usi impropri – e ad adottare misure di attenuazione adeguate per la tutela dei diritti fondamentali».

[23] Così, G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in «Common Market Law Review» (2022), pp. 473 ss.

[24] Diverso l'approccio seguito dalla normativa del *Digital Services Act* che adotta un modello ibrido, combinando elementi del GDPR e dell'*AI Act*, e definisce quattro livelli di rischio per i fornitori di servizi intermediari, ai quali lascia ampia discrezionalità nell'individuare le misure più idonee a mitigare le esternalità negative delle proprie attività.

infine, il rischio "inaccettabile", che concerne i sistemi di IA utilizzati per scopi che violano gravemente i diritti fondamentali, come la sorveglianza di massa, e che risultano pertanto totalmente vietati. In tal modo, l'*AI Act* non solo stabilisce una cornice regolatoria articolata, ma mette a punto anche una metodologia dinamica per affrontare i rischi legati all'intelligenza artificiale, cercando di bilanciare innovazione e protezione dei diritti umani in un contesto normativo in continua evoluzione.

3. *Considerazioni a margine: il "doppio volto" dell'intelligenza artificiale e i "contenuti illeciti"*

Alla luce della recente normativa europea[25] e degli effetti che questa potrebbe avere sui temi trattati nel Convegno odierno, è fondamentale riflettere sul ruolo che l'intelligenza artificiale potrebbe assumere in relazione ai nuovi obblighi imposti alle piattaforme digitali[26]. A partire da una prima analisi delle disposizioni contenute nell'*AI Act*, emerge come questa normativa, rispetto al *Digital Services Act*, possa assumere un ruolo cruciale nella mitigazione delle esternalità negative derivanti dall'utilizzo dell'intelligenza artificiale. Infatti, sebbene entrambi i regolamenti condividano l'obiettivo di regolare l'uso delle tecnologie digitali, l'*AI Act* si distingue per la sua capacità di affrontare in modo più diretto i rischi associati all'impiego dell'IA, ponendo un accento maggiore sulla gestione del rischio e sui profili di responsabilità.

Quando si discute dell'IA come strumento per contrastare i contenuti illeciti o, al contrario, come potenziale generatore di contenuti controversi, è necessario operare distinzioni precise, in particolare in relazione al tipo e alla quantità di dati trattati dagli strumenti di IA. Nel circoscrivere l'ambito di riflessione, ci concentreremo principalmente sui "modelli di base"[27] di intelligenza artificiale, senza entrare nel merito dei "grandi modelli linguistici" (LLM)[28] o dei "modelli generativi di grandi dimensioni" (LGAIM), per i quali si ritiene che la normativa attuale non fornisca ancora una regolamentazione esaustiva[29].

[25] Sull'argomento, A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto una rivoluzione. Diritti fondamentali, dati personali e regolazione*, il Mulino, Bologna, 2022.

[26] G. Marchetti, *Le* fake news *e il ruolo degli Algoritmi*, in «Media Laws», 1, (2020), pp. 29 ss.; sul punto anche O. Pollicino, P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi ed opportunità*, in «Federalismi», 12, (2024), p. 14.

[27] Per un'analisi più dettagliata si rimanda a R. Bommasani, D.A. Hudson, E. Adeli, R. Altman, S. Arora, S. von Arx, M.S. Bernstein, J. Bohg, A. Bosselut, E. Brunskill, *On the opportunities and risks of foundation models*, arXiv preprint arXiv:2108.07258, 2021.

[28] D. Ganguli, D. Hernandez, L. Lovitt, A. Askell, Y. Bai, A. Chen, T. Conerly, N. Dassarma, D. Drain, N. Elhage, *Predictability and surprise in large generative models. ACM Conference on Fairness, Accountability, and Transparency*, 2022, pp. 1747-1764. Sul punto anche G. Fasano, *Le 'informazioni sintetizzate' generate dai large language models e le esigenze di tutela del diritto all'informazione: valori costituzionali e nuove regole*, in «Dirittifondamentali.it», 1 (2024), p. 108.

[29] J. Hoffmann, S. Borgeaud, A. Mensch, E. Buchatskaya, T. Cai, E. Rutherford, D. Casas, D.L. Hendricks, Welbl, A. Clark, *Training compute-optimal large language models*, arXiv preprint arXiv:2203.15556, 2022.

Per affrontare in modo adeguato queste tematiche, è innanzitutto necessario chiarire alcuni interrogativi fondamentali. Esiste un concetto di "spazio digitale" all'interno del Regolamento sull'intelligenza artificiale? E, in tal caso, in che modo questo concetto può incidere sulla regolamentazione complessiva e quali effetti potrebbe avere sull'intero sistema normativo? Per rispondere a tali domande è indispensabile un inquadramento preliminare delle premesse e dei principi di fondo sottesi alla normativa in questione. L'*AI Act* è stato concepito per affrontare questioni cruciali come la sicurezza, la trasparenza[30], la *governance*[31], la responsabilità[32], gli *standard* etici e la protezione della *privacy* dei dati[33]. Il termine "spazio digitale" nel contesto dell'*AI Act* potrebbe dunque riferirsi all'ecosistema digitale più ampio in cui operano i sistemi di IA, comprendendo piattaforme, infrastrutture e servizi nei quali le tecnologie di IA sono integrate e utilizzate.

La regolamentazione dell'uso dell'IA, in particolare per quanto riguarda i contenuti online, rappresenta un ambito ancora in evoluzione[34]. La rapidità con cui la tecnologia IA sta trasformando il panorama digitale solleva sfide inedite nella gestione dei contenuti illeciti online, che spaziano dalla disinformazione all'incitamento all'odio, dal crimine informatico all'abuso di minori, fino alla violazione della *privacy* e alla diffusione di materiale protetto da *copyright*. In questo contesto, l'intelligenza artificiale non solo ha rivoluzionato le modalità di interazione con i contenuti digitali, ma ha altresì generato nuove criticità legate principalmente alla produzione e alla distribuzione di contenuti illeciti[35].

Nei paragrafi successivi si cercherà di analizzare due prospettive contrapposte: da un lato, come l'intelligenza artificiale possa rappresentare una risorsa efficace nella lotta contro i contenuti illeciti, e dall'altro, come possa costituire una minaccia per l'introduzione o l'espansione di pratiche illecite nello spazio digitale.

3.1. *Il ruolo proattivo dell'IA nel riconoscimento dei contenuti illeciti*

Nel contesto della progressiva digitalizzazione e dell'ampliamento delle interazioni online, l'intelligenza artificiale assume un ruolo sempre più centrale nel rilevamento e nella gestione dei contenuti illeciti. In una prospettiva di *governance* tecnologica

[30] I sistemi di IA dovrebbero essere "spiegabili" e comprensibili e, secondo tale principio gli individui dovrebbero essere informati quando interagiscono con l'IA (ad esempio, quando comunicano con un *chatbot*).

[31] La legge crea un nuovo organismo di regolamentazione, il Consiglio europeo per l'intelligenza artificiale, per garantire un'applicazione coerente della legge sull'IA in tutti gli Stati membri.

[32] Gli sviluppatori e i distributori di sistemi di IA ad alto rischio sono tenuti a implementare misure di sicurezza e a sottoporsi a controlli e certificazioni regolari.

[33] I sistemi di IA devono rispettare le leggi vigenti in materia di protezione dei dati, compreso il Regolamento generale sulla protezione dei dati (GDPR).

[34] A livello globale, sono in atto iniziative volte a regolamentare sia l'impiego delle piattaforme digitali sia l'utilizzo dell'intelligenza artificiale nella moderazione dei contenuti. Tali interventi possono essere letti come un possibile preludio agli sviluppi normativi attesi anche in ambito europeo.

[35] Si anticipa che secondo il Regolamento si applica anche a *providers* e *deployers* di sistemi di IA stabiliti o situati in un paese terzo, in tutti i casi in cui l'*output* prodotto dal sistema venga utilizzato all'interno del territorio dell'Unione (art. 2, par. 1, lett. c).

orientata alla tutela dei diritti fondamentali, il ricorso a sistemi di IA si rivela essenziale per far fronte alle nuove sfide poste alla sicurezza informatica e alla salvaguardia dello "spazio pubblico digitale". In particolare, gli strumenti algoritmici fondati su tecniche avanzate di apprendimento automatico – e, più specificamente sul *deep learning* – si sono dimostrati capaci di individuare contenuti digitali illeciti, quali immagini violente, materiale pedopornografico o contenuti di propaganda estremista, contribuendo così a rafforzare le attività di moderazione automatizzata. L'*AI Act* si inserisce all'interno di questa traiettoria normativa, ponendosi in linea di continuità con il *Digital Services Act* (DSA) nella definizione di un sistema di obblighi graduati e proporzionati rivolti ai fornitori e agli utenti di sistemi IA, in particolare quelli operanti su piattaforme online di grandi dimensioni. Tra gli obblighi previsti, riveste particolare rilievo quello relativo alla trasparenza degli *output* generati: i soggetti interessati sono infatti tenuti a segnalare se i contenuti siano stati artificialmente generati o modificati, al fine di agevolare l'individuazione dei rischi sistemici legati alla manipolazione dell'informazione e all'alterazione del dibattito democratico.

A ben vedere, l'efficacia operativa delle soluzioni basate sull'intelligenza artificiale trova già concreta applicazione in diversi strumenti tecnologici attualmente in uso. Un esempio emblematico è rappresentato dal sistema *PhotoDNA*[36], che consente l'identificazione e il blocco di immagini precedentemente segnalate come illecite, facilitando così l'intervento tempestivo nella loro rimozione. Analogamente, le principali piattaforme di *social media* e condivisione digitale si avvalgono già di sistemi automatizzati di monitoraggio dei contenuti caricati dagli utenti, in grado di rivelare espressioni di incitamento all'odio, minacce, discriminazioni razziali o di genere, nonché fenomeni di disinformazione. In questo ambito, le tecniche di elaborazione del linguaggio naturale (*Natural Language Processing* – NLP) consentono una sorveglianza in tempo reale delle comunicazioni testuali, potenziando così i meccanismi di segnalazione automatica ai "moderatori umani". Ulteriori applicazioni di IA riguardano il rilevamento di comportamenti digitali anomali, come nel caso del *phishing* o della diffusione di *malware*, attraverso l'analisi di *pattern* comportamentali e la capacità degli algoritmi di apprendere da grandi volumi di dati. L'impiego di tali tecnologie contribuisce altresì a rendere più efficiente il sistema di segnalazione da parte degli utenti, riducendo il numero di notifiche errate e ottimizzando l'allocazione delle risorse dedicate alla moderazione dei contenuti.

Tuttavia, nella valutazione del potenziale dell'IA come strumento di moderazione, risulta imprescindibile considerare i rischi associati ai *bias* algoritmici. È ormai ampiamente riconosciuto che tali distorsioni algoritmiche possano generare effetti censori sproporzionati, producendo conseguenze discriminatorie indirette nei confronti di determinate categorie sociali, ad esempio sulla base dell'etnia o dell'orientamento

[36] Così, si rimanda al *Considerando 136* del Regolamento e alle riflessioni di N. Pica, *La tutela della libertà di informazione nel Digital Services Act tra contrasto alle "manipolazioni algoritmiche" e limiti alla* content moderation, in «Media Laws», (2025).

sessuale[37]. Tali criticità devono essere attentamente ponderate al fine di garantire che l'impiego dell'IA in ambito regolatorio sia non solo efficace, ma anche equo e rispettoso dei diritti fondamentali.

Infine, l'integrazione di sistemi IA nelle infrastrutture digitali apre scenari inediti per il monitoraggio costante delle notizie e dei flussi informativi, grazie allo sviluppo di tecnologie di *fact-checking* automatico; questi strumenti potrebbero contribuire a prevenire la diffusione di contenuti dannosi e a contenere, per quanto possibile, gli effetti lesivi che tali fenomeni possono generare sulla collettività[38].

3.2. *L'IA generatrice di contenuti illeciti*

Nel considerare la seconda prospettiva – particolarmente problematica e meritevole di approfondimento – l'intelligenza artificiale emerge come un potenziale amplificatore della diffusione di contenuti illeciti online, configurandosi non solo come strumento di rilevazione, ma anche come generatore di contenuti dannosi. Ciò comporta un incremento esponenziale dei rischi connessi alla sua applicazione, sollevando interrogativi rilevanti sull'efficacia del Regolamento sull'intelligenza artificiale nel mitigarne gli effetti nocivi[39].

La questione riguarda tre aspetti in particolare: i modelli linguistici di grandi dimensioni (LLM), la qualità e composizione dei *dataset* di addestramento e i modelli generativi c.d. su larga scala (LGAIM), inclusi gli strumenti di elaborazione del c.d. linguaggio naturale (*Natural Language Processing*, anche NLP).

In primo luogo, i modelli linguistici di grandi dimensioni si caratterizzano per la capacità di generare contenuti con elevata coerenza testuale e plausibilità semantica, attribuendo verosimiglianza a informazioni errate, fuorvianti o addirittura inventate; l'imprevedibilità dei loro *output*, unita alla difficoltà di verificarne l'origine e l'effettiva aderenza ai fatti, rappresenta un rischio concreto per la qualità dell'informazione online.

In secondo luogo, i *dataset* impiegati nell'addestramento spesso includono contenuti fittizi, decontestualizzati o distorti che compromettono la solidità epistemica degli *output*: difatti, opinioni maggioritarie possono essere presentate come verità oggettive, contribuendo così alla diffusione di disinformazione e favorendo fenomeni di manipolazione, frode e interferenza nei processi democratici.

[37] G. Vasino, *Censura "privata" e contrasto all'*hate speech *nell'era delle* Internet Platforms, in «Federalismi», (2023), p. 146.

[38] Si fa riferimento, ad esempio, al recente progetto *AI4 Trust* (*Artificial Intelligence for Trustworthy Solutions Against Disinformation*), un'iniziativa finanziata dall'Unione Europea nell'ambito del programma *Horizon Europe*, avviata il 1° gennaio 2023 e con una durata prevista di 38 mesi.

[39] Così sul punto, si rimanda all'art. 5/1/b) del Regolamento che proibisce «*the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm*».

I modelli generativi di IA su larga scala, pur offrendo possibilità inedite nella produzione creativa, possono essere impiegati per generare testi manipolativi, sofisticate *fake news*[40] e contenuti polarizzanti[41], con una rapidità e un livello di dettaglio che ne aumentano l'efficacia persuasiva[42].

Infine, una criticità specifica nell'elaborazione automatica del linguaggio naturale risiede nel fenomeno delle c.d. "allucinazioni", ovvero la generazione di risposte plausibili ma non correlate ai dati di *input* o ai fatti reali. Questo rischio è particolarmente marcato nei sistemi di domanda-risposta, dove i modelli tendono a produrre risposte anche in assenza di informazioni adeguate. Tali *output*, se diffusi senza una adeguata verifica, possono influenzare negativamente le decisioni individuali e collettive[43].

Pertanto, come si è visto, un rischio sempre più rilevante legato all'impiego dell'intelligenza artificiale riguarda la sua capacità di facilitare la produzione e la diffusione automatizzata di contenuti illeciti: tecnologie come i *deepfake*[44] o i sistemi di generazione testuale per *social media* possono essere utilizzate per veicolare disinformazione, propaganda e teorie complottiste in modo rapido, economico e difficilmente tracciabile[45]. Tali strumenti, inoltre, risultano spesso incapaci di interpretare correttamente il contesto comunicativo: l'ironia e la satira, ad esempio, possono essere classificate erroneamente

[40] Così, J.A. Goldstein, G. Sastry, M. Musser, R. Di Resta, M. Gentzel, K. Sedova, *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations*, arXiv preprint arXiv:2301.0424, 2023.

[41] Una parte della dottrina sovranaziale ribadisce la necessità di regolamentare in maniera più dettagliata la nuova generazione di modelli di I.A. Così, P. Hacker, A. Engel, M. Mauer, *Regulating ChatGPT and other Large Generative AI Models*, che ribadiscono «*Arguably, the EU is spearheading efforts to 2 effectively regulate AI systems, with specific instruments (AI Act, AI Liability Directive), software regulation (Product Liability Directive) and acts addressed toward platforms, yet covering AI (Digital Services Act; Digital Markets Act). Besides, technology-neutral laws, such as non-discrimination law, continue to apply to AI systems. As we shall see, it may be precisely their technology-agnostic features that make them better prepared to handle the specific risks of LGAIMs than the specific AI regulation that has been enacted or is in preparation*».

[42] Sul punto, P. Hacker, A. Engel, M. Mauer, *Regulating ChatGPT and other Large Generative AI Models*, cit. pp. 2 ss.

[43] È essenziale sviluppare strategie mirate per ridurre il fenomeno delle allucinazioni nei modelli linguistici, soprattutto in contesti regolatori e istituzionali, dove l'affidabilità delle informazioni è cruciale. La ricerca ha individuato sia approcci generali – come la selezione automatica di prompt di elevata qualità durante il *fine-tuning* – sia soluzioni più tecniche e mirate, tra cui il *prompt engineering*, l'integrazione con basi di conoscenza esterne (*retrieval-augmented generation*), l'adozione di funzioni di perdita orientate alla fedeltà fattuale e l'impiego di codifiche avanzate. Particolarmente promettente è il modello del *Multiagent Debate*, in cui più modelli linguistici interagiscono in modo iterativo attraverso fasi di proposta, critica e revisione delle risposte. Ispirato al principio del controinterrogatorio nel campo giuridico, questo metodo punta a generare risposte più accurate e affidabili attraverso il confronto tra punti di vista diversi. Sul tema, C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, in «Computer Law & Security Review», vol. 55, (2024).

[44] L'intelligenza artificiale può essere utilizzata per creare *deepfakes*, ossia video o immagini manipolati che sembrano reali, ma che sono completamente falsificati; la tecnologia dei *deepfakes* è ormai molto avanzata, e riconoscere un video manipolato richiede strumenti sofisticati.

[45] L'intelligenza artificiale può produrre contenuti molto convincenti e in grandi quantità, difficili da distinguere dalle informazioni autentiche, e questo può minare la fiducia pubblica nelle fonti di informazione.

come contenuti illeciti (c.d. falsi positivi), mentre contenuti dannosi possono passare inosservati (c.d. falsi negativi); a ciò si aggiunge il rischio di *bias* nei dati di addestramento che può tradursi in decisioni discriminatorie.

Parallelamente, le tecniche di elusione dei sistemi di rilevamento automatizzato – tramite linguaggi codificati o manipolazioni visive – evolvono rapidamente, riducendo l'efficacia delle attuali soluzioni basate sull'IA. In questo scenario, la supervisione umana[46] si conferma imprescindibile per garantire l'affidabilità del processo di moderazione.

La normativa europea, ad oggi, non prevede ancora un quadro organico per la disinformazione prodotta dall'IA c.d. generativa. In prospettiva, si rende forse auspicabile un aggiornamento del *Digital Services Act*, volto ad introdurre specifici obblighi per le piattaforme che integrano modelli generativi, promuovendo un'azione proattiva contro la disinformazione[47]. L'*AI Act* interviene parzialmente sul tema, imponendo obblighi di trasparenza per i contenuti sintetici (art. 50/2), inclusi testi, immagini, audio e video, attraverso marcature digitali leggibili dalle macchine; i *deepfake* devono essere chiaramente identificati come tali, salvo eccezioni per finalità artistiche o satiriche, mentre sistemi di riconoscimento emotivo o categorizzazione biometrica devono essere dichiarati esplicitamente agli utenti (art. 50/3, art. 50/4 e art. 52).

Tuttavia, per affrontare in modo efficace i rischi derivanti dai LLM è necessario un approccio integrato che coinvolga tanto il DSA quanto l'*AI Act*. Il primo introduce strumenti utili – come i *trusted fluggers* (art. 22 DSA) – ma non affronta pienamente la disinformazione lecita ma dannosa; il secondo, invece, potrebbe fornire indicazioni più incisive, promuovendo soluzioni come il *fingerprinting* dei contenuti, l'uso di *radioactive data* per la tracciabilità delle fonti e l'impiego di tecniche di *reinforcement learning from human feedback* per rafforzare l'aderenza ai fatti.

Infine, ai sensi dell'art. 52 dell'*AI Act*, ogni prestatore di servizi digitali che impiega sistemi di IA – indipendentemente dalla tipologia di servizio o dalle dimensioni della piattaforma – è soggetto a obblighi informativi specifici, in particolare quando l'IA produce rappresentazioni ingannevoli di persone senza il loro consenso[48].

[46] Difatti, come recita il *Considerando 73* demanda, inoltre, al *provider* l'individuazione di misure di sorveglianza umana (art. 14) adeguate, prima dell'immissione del sistema sul mercato o della sua messa in servizio. Queste dovranno dunque «garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo».

[47] Anche il Codice di condotta europeo sulla disinformazione del 2022 potrebbe svolgere un ruolo rilevante, sebbene la sua natura volontaria ne limiti l'efficacia.

[48] Così, S. Tommasi, *Digital Services Act e Artifcial Antelligence Acttentativi di futuro da armonizzare*, cit., che specifica "Un altro esempio di uso frequente di sistemi di IA da parte dei prestatori di servizi digitali è quello relativo alla moderazione dei contenuti. I *provider* si affidano spesso a tecniche e mezzi di ricerca automatizzati, pur nella consapevolezza di non riuscire a cogliere le peculiarità del contesto nel quale sono inserite determinate frasi, rischiando, per esempio, di bloccare contenuti erroneamente di natura offensiva", p. 282.

4. *Nuovi interrogativi: il Regolamento di fronte allo "spazio digitale"*

L'introduzione dell'*Artificial Intelligence Act* nel quadro normativo europeo solleva questioni rilevanti in relazione ai meccanismi esistenti di imputazione della responsabilità, anche alla luce delle disposizioni previste dal *Digital Services Act*.

Sebbene il Regolamento europeo preveda misure preventive e prescrizioni tecniche orientate alla mitigazione del rischio, esso non si pronuncia in modo esaustivo sulle implicazioni penalistiche, che restano affidate alle normative nazionali dei singoli Stati membri.

Ciò nonostante, la nuova normativa contribuisce a ridefinire il perimetro delle responsabilità attraverso la distinzione tra fornitori (*provider*) e utilizzatori (*deployer*) di sistemi di intelligenza artificiale, ai quali sono attribuiti obblighi differenziati e graduati in base al livello di rischio associato alla tecnologia impiegata. In un'ottica dichiaratamente *risk-based*, il Regolamento stabilisce che quanto maggiore è il potenziale impatto su diritti e libertà fondamentali, tanto più stringenti saranno i requisiti di conformità richiesti.

Particolarmente rilevante, in tale contesto, come già anticipato, è il principio di *human oversight*[49], che impone un coinvolgimento attivo sia dei *provider* sia dei *deployer* nella supervisione dei sistemi ad alto rischio; il mancato adempimento degli obblighi di vigilanza e controllo potrebbe, in taluni casi, integrare ipotesi di responsabilità penale per omissione, qualora da tale negligenza derivino conseguenze lesive per i terzi.

4.1. *Dagli aspetti definitori agli obblighi sui* provider *e* deployer

Nel quadro normativo delineato dal Regolamento sull'intelligenza artificiale si coglie l'intento del legislatore europeo di predisporre un sistema giuridico improntato a un approccio *risk-based*, volto a garantire un impiego sicuro, trasparente e conforme ai diritti fondamentali dei sistemi di intelligenza artificiale. Alla luce di tale impostazione, si cercherà pertanto di delineare le implicazioni giuridiche derivanti dall'attuazione della nuova disciplina.

Risulta centrale la figura del *provider*[50], definito come il soggetto – persona fisica o giuridica, autorità pubblica, agenzia o altro ente – che sviluppa o fa sviluppare un sistema o modello di IA a fini generali, immettendolo sul mercato sotto il proprio nome o marchio, indipendentemente dal carattere oneroso della operazione; a tale soggetto sono attribuiti obblighi stringenti, soprattutto per i sistemi classificati come

[49] L'*Artificial Intelligence Act* riconosce espressamente un ruolo centrale all'*human oversight*. A ben vedere, per alcuni *high-risk AI systems*, si dispone che l'insufficienza anche del coinvolgimento di una sola persona umana, esigendosi che «*no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons*».

[50] Introdotte dall'art. 2, le figure del fornitore e dell'utilizzatore vengono poi ulteriormente specificate dall'art. 3, che ne traccia il perimetro di operatività.

ad alto rischio (art. 16). Tra essi si annoverano: la valutazione della conformità e della classificazione del rischio; la predisposizione e conservazione della documentazione tecnica; la comunicazione trasparente agli utenti circa il funzionamento del sistema; il monitoraggio continuo del sistema dopo l'immissione sul mercato; la cooperazione lungo la filiera, nel rispetto dei diritti di proprietà intellettuale. Per i sistemi ad alto rischio – tra cui ad esempio i dispositivi medici (art. 6) – sono inoltre richiesti l'adozione di un sistema di gestione della qualità, la conservazione dei *log*, la marcatura CE e una dichiarazione UE di conformità[51]. Inoltre, ai sensi del *Considerando 84*, modifiche sostanziali al sistema o al suo utilizzo possono comportare il trasferimento della qualifica (e delle relative responsabilità) di *provider* a distributori, importatori e utilizzatori. Inoltre, ulteriore obbligo fondamentale è l'implementazione di misure efficaci di sorveglianza umana (art. 14) che garantiscano la supervisione da parte di operatori competenti, debitamente formati e dotati dell'autorità necessaria.

Accanto al *provider*, l'*AI Act* introduce la figura del *deployer*, identificato come il soggetto che utilizza un sistema di IA sotto la propria autorità per fini professionali. A ben vedere, anch'egli è destinatario di obblighi rilevanti (art. 26), tra cui: l'adozione di misure tecniche e organizzative coerenti con le istruzioni del *provider*; l'affidamento della supervisione a personale qualificato; e, in caso di rischio dei diritti fondamentali, salute o sicurezza, l'obbligo di informare tempestivamente *provider* e autorità competenti, sospendendo l'uso del sistema.

Sul piano sanzionatorio, il Regolamento prevede unicamente sanzioni amministrative e pecuniarie, da modulare secondo i criteri *ex* artt. 99-101, demandando agli ordinamenti nazionali la loro concreta determinazione.

Tra le novità più rilevanti figura l'obbligo di "etichettatura" dei contenuti generati artificialmente, con particolare riferimento ai *deepfake*, per i quali l'art. 52/3, impone l'indicazione esplicita dell'origine artificiale; se impiegati in contesti pubblici o da autorità, tali contenuti rientrano nella categoria dei sistemi ad alto rischio e sono soggetti a requisiti rafforzati di trasparenza e vigilanza.

Il Regolamento, tuttavia, ammette deroghe per finalità artistiche, satiriche o creative, prevedendo forme semplificate di "etichettatura" per contenuti inequivocabilmente fittizi. Nonostante il rigore della disciplina, permangono alcune criticità: l'obbligo di trasparenza grava esclusivamente sull'utente finale, senza un corrispondente dovere in capo ai produttori di sistemi. Inoltre, in assenza di una cornice penale specifica, l'utilizzo fraudolento di *deepfake* – per finalità di disinformazione, diffamazione o manipolazione – rischia di sfuggire ad una risposta sanzionatoria adeguata.

Ulteriore lacuna riguarda l'assenza di una regolamentazione degli strumenti di rilevazione dei *deepfake*, i quali potrebbero costituire un efficace strumento di contrasto alla manipolazione informativa. Sebbene il Regolamento riconosca il rischio che i

[51] A livello di applicazione "territoriale, il Regolamento si applica anche ai soggetti stabiliti in Paesi terzi, qualora il risultato del sistema venga utilizzato all'interno dell'Unione (art. 2, par. 1, lett. c).

sistemi di IA alimentino fenomeni di disinformazione, l'attenzione normativa appare concentrata quasi esclusivamente sui *deepfake*, trascurando altre modalità di alterazione artificiale dell'informazione[52]. Tale limite appare particolarmente significativo, alla luce del potenziale impatto di simili fenomeni sulla qualità del dibattito pubblico, sull'integrità dei processi democratici e sulla coesione sociale.

5. *Considerazioni conclusive: il diritto penale tra "vecchi paradigmi" e recenti evoluzioni*

Come già anticipato, il nuovo assetto normativo delineato dall'*AI Act* non contempla espressamente la responsabilità penale, con riferimento alla quale – in attesa di interventi legislativi di adeguamento – dovrà farsi riferimento alla disciplina esistente.

A ben vedere, il sistema delineato dal Regolamento promuove un intervento di natura "proattiva", piuttosto che "reattiva", imponendo a tutti i soggetti coinvolti, in particolare alle imprese, una serie di obblighi e attività destinate alla gestione del rischio. Tali obblighi danno vita ad un sistema articolato di responsabilità, che si sviluppa all'interno di un *framework risk-based*[53].

Il Regolamento – sebbene privo di efficacia diretta in ambito penale – stabilisce un'area di rischio accettabile, identificando requisiti che, se soddisfatti, consentono di considerare il sistema di intelligenza artificiale conforme. Pertanto, tali requisiti costituiscono gli *standard* a cui le imprese dovranno attenersi al fine di produrre e immettere i propri prodotti sul mercato. Senza dubbio, il ruolo delle procedure di compliance appare cruciale, poiché permettono una valutazione preventiva dei potenziali rischi associati all'uso di sistemi di IA, rischi che dovranno essere mantenuti all'interno dei limiti predefiniti. Una volta adottate le opportune misure cautelative, la responsabilità per eventuali danni derivanti dal mancato rispetto di tali misure sarà attribuibile all'ente stesso e altresì ai soggetti responsabili della loro attuazione[54].

In un'altra prospettiva, l'*AI Act* affronta in maniera decisa la questione del contenuto illecito, cercando di bilanciare le esigenze di innovazione tecnologica e la tutela dei

[52] Sul tema si rinvia al completo approfondimento di G. PROIETTI, *L'impianto regolatorio della società dell'informazione tra vecchi e nuovi equilibri. Il fenomeno del* deep fake, in «Media Laws», I (2024) pp. 330 ss.

[53] Sulla nozione di rischio, «la nozione di rischio che ritorna a più riprese nel Regolamento europeo si configura come intrinsecamente normativa. Non si basa cioè su una propensione effettiva, verificata esperienzialmente, alla causazione del danno, ma, a conferma di un'ottica precauzionale, sul superamento di livelli di cautela condensati in regole giuridiche», così F. CONSULICH, *Il diritto penale al tempo dell'Intelligenza artificiale. Prospettive punitive nazionali dopo l'AI Act*, in «Diritto di difesa», 17 dicembre 2024.

[54] A tal proposito, un altro aspetto di rilevante importanza potrebbe risiedere nei modelli di organizzazione e gestione (MOG) previsti dal Decreto Legislativo 231/01, i quali consentono di identificare le figure apicali responsabili del potere decisionale e di stabilire le modalità operative per intervenire in caso di commissione di reati che rientrano tra quelli "presupposto" per l'attribuzione della responsabilità amministrativa dell'ente a seguito dell'utilizzo dei sistemi di intelligenza artificiale.

diritti fondamentali. Difatti, dalla panoramica svolta, si evince come l'*AI Act* imponga un insieme di obblighi di trasparenza e conformità, rivolti ai *providers* e ai *deployers* dei sistemi di IA, la cui violazione è sanzionata esclusivamente con sanzioni amministrative pecuniarie[55]. In relazione ai contenuti illeciti online e ai relativi profili di responsabilità penale, il dibattito dovrebbe concentrarsi sulla definizione di metodi di "moderazione dei contenuti" e sull'applicazione delle regole generali di ascrizione della responsabilità, in base al rischio associato. Tuttavia, una delle principali difficoltà risiede nella individuazione dell'errore all'interno del sistema, nonché nella difficoltà di determinare il ruolo dell'operatore umano nella sorveglianza del processo decisionale automatizzato.

In prospettiva *de iure condendo*, tali riflessioni dovranno integrarsi con la recente normativa di adeguamento in materia di intelligenza artificiale – la legge 23 settembre 2025, n. 132 – che sembra dedicare ambio spazio al tema oggetto del convegno poichè, da un lato, prevede l'introduzione di autonome fattispecie incriminatrici e di circostanze aggravanti nel caso in cui i reati vengano commessi attraverso l'impiego di sistemi di IA e, dall'altro, attraverso un'ampia delega demanda al legislatore di individuare strumenti per inibire la diffusione e rimozione di contenuti generati illecitamente dall'IA[56].

Dall'altro, un'ulteriore rilevante modifica riguarda l'introduzione della nuova fattispecie di reato di cui all'art. 612-*quater* c.p., "illecita diffusione di contenuti generati o alterati mediante l'intelligenza artificiale", che punisce con la reclusione da uno a cinque anni chi cagioni un danno ingiusto a una persona cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o registrazioni vocali falsificate o alterate tramite sistemi di IA, idonee a ingenerare errore sulla loro genuinità. In considerazione del ruolo centrale attribuito alla sorveglianza, dal punto di vista penalistico potrebbe configurarsi una responsabilità del "sorvegliante umano" – sia esso *provider* o *deployer* – per la mancata adozione di misure adeguate a prevenire danni derivanti dall'operato del sistema di intelligenza artificiale. Parallelamente, potrebbe ipotizzarsi la possibilità di "addestrare" i sistemi di IA al rispetto delle leggi e delle normative applicabili, sia a livello nazionale sia sovranazionale, senza che ciò esoneri il sorvegliante umano dalla sua posizione di garanzia[57].

[55] Con riferimento al profilo sanzionatorio, va rilevato che il sistema di sanzioni previsto dal Regolamento richiama, per natura e struttura, quello già delineato dal GDPR agli articoli 83 e 84. Anche nell'ambito dell'*AI Act*, infatti, si configura un impianto sanzionatorio incisivo, che può avere un impatto significativo sul fatturato dei soggetti interessati. Le sanzioni amministrative pecuniarie variano in base alla tipologia di violazione e alla disposizione normativa trasgredita; inoltre, la competenza a irrogare tali sanzioni spetta alle autorità di controllo, cui è demandato il compito di valutare sia l'*an* che il *quantum* della sanzione, tenendo conto delle specifiche circostanze del caso. A tali autorità è riconosciuto un ampio margine di discrezionalità nell'esercizio del potere sanzionatorio.

[56] Di particolare interesse risultano le modifiche al codice penale e ad ulteriori disposizioni penali introdotte fin da subito all'art. 26. Come anticipato, da un lato sono state previste nuove circostanze aggravanti nel caso in cui il fatto sia commesso mediante l'impiego di sistemi di intelligenza artificiale (art. 61 c.p., n. 11-*novies*), applicabili a specifiche fattispecie di reato, quali, ad esempio, l'aggiotaggio, la violazione del diritto d'autore e gli attentati contro i diritti politici del cittadino.

[57] Per quanto riguarda il diritto dell'UE, la Corte di Giustizia dell'Unione Europea (CGUE) ha stabilito, in una serie di sentenze (CGUE, Causa C-54/07, Feryn; Causa C-507/18, Associazione Avvocatura per i diritti

Per quanto riguarda i paradigmi ascrittivi di imputazione della responsabilità penale, l'approccio previsto dal Regolamento europeo, sembra orientato principalmente all'opportunità di strutturare le nuove fattispecie a titolo colposo, di evento o di mera condotta. Secondo parte della dottrina sembrerebbe preferibile l'ipotesi di strutturare la nuova fattispecie sul paradigma del reato colposo di mera condotta[58], che ruota attorno al riconoscimento di responsabilità sul soggetto agente per non aver predisposto le adeguate cautele poste a presidio delle scelte rischiose e devianti dell'IA. Si tratterebbe pertanto di ricorrere ai paradigmi già presenti nel nostro ordinamento, cioè di applicare la sanzione penale alla violazione consapevole di una regola cautelare, qualora l'agente, pur conoscendone la funzione di prevenzione, scelga di disattenderla. In tal contesto, si potrebbe configurare una responsabilità per colpa cosciente o per dolo eventuale, qualora l'agente, pur consapevole della funzione di prevenzione di una regola cautelare, decida di disattenderla. Un approccio sistemico sarebbe auspicabile, evitando così di ridurre le sanzioni a semplici aggravanti accessorie e mirando piuttosto a sanzionare omissioni di controllo, programmazione negligente o impiego imprudente di sistemi autonomi.

Nel contesto delineato permane, invece, l'assenza di un riferimento alla responsabilità penale degli enti, ai sensi del d.lgs. 231/2001, un'assenza che sembrerebbe compromettere la coerenza del Regolamento con la struttura operativa degli attori del settore. In tale contesto, l'imputazione per colpa, attraverso il modello della omissione impropria e la costruzione di posizioni di garanzia, sembrerebbe comunque la via più percorribile, anche in considerazione della logica precauzionale sottesa all'*AI Act*.

In conclusione, sebbene l'*AI Act* non affronti direttamente i profili di responsabilità penale, esso rappresenta la base concettuale su cui si fondano e si fonderanno, probabilmente, le future normative. Appare comunque necessario interrogarsi su come l'ordinamento italiano si confronterà con l'entrata in vigore della normativa europea e sui primi effetti derivanti dall'adozione della prima legge nazionale in materia di intelligenza artificiale. Ne derivano nuovi interrogativi circa la possibilità che i paradigmi tradizionali di responsabilità penale resistano di fronte all'emergere di tali strumenti innovativi, o, al contrario, circa l'eventualità che sia necessario un parziale ripensamento di alcune categorie giuridiche, al fine di garantire un'implementazione efficace delle misure previste e un costante aggiornamento normativo, in risposta alle sfide poste dall'evoluzione dell'intelligenza artificiale e delle nuove tecnologie.

LGBTI), che le disposizioni in materia di non discriminazione possono estendersi anche alle attività preparatorie che precedono, ad esempio, la selezione per un posto di lavoro, a determinate condizioni. In tali casi concreti, dichiarazioni pubbliche, come quelle rilasciate durante un programma radiofonico che esprimono l'intenzione di non assumere candidati di un determinato orientamento sessuale, possono essere considerate come "condizioni di accesso all'occupazione", qualora esista un collegamento diretto tra tali dichiarazioni e la politica di assunzione del datore di lavoro, senza che il legame sia puramente ipotetico (CGUE, causa C-507/18, Associazione Avvocatura per i diritti LGBTI, para. 43).

[58] F. Consulich, *Il diritto penale al tempo dell'Intelligenza artificiale. Prospettive punitive nazionali dopo l'AI Act*, cit.

COME INTERPRETARE LA NOZIONE DI «CONTENUTO ILLEGALE» NEL QUADRO DEL REGOLAMENTO SUI SERVIZI DIGITALI? RIFLESSIONI IN UN'OTTICA DI DIRITTO DELL'UNIONE

Federico Ferri

SOMMARIO: 1. Introduzione. – 2. Cenni alla formulazione della definizione. – 3. Uno sguardo al contesto giuridico applicativo. – 4. Considerazioni sugli obiettivi perseguiti dalla misura di riferimento. – 5. Rilievi conclusivi.

1. *Introduzione*

Il regolamento (UE) 2022/2065 sui servizi digitali[1], noto anche come "legge sui servizi digitali" o *Digital Services Act* (DSA), introduce norme armonizzate sulla prestazione di servizi intermediari nel mercato interno. È stato presentato come un fiore all'occhiello della normativa dell'Unione europea (Unione o UE) riconducibile all'obiettivo del completamento del mercato unico digitale e all'ambizione di realizzare una vera e propria transizione digitale continentale a diritto primario costante, cioè senza prevedere modifiche del Trattato sull'Unione europea (TUE) e del Trattato sul funzionamento dell'Unione europea (TFUE).

Come ampiamente prevedibile, sono molteplici i profili giuridici di discussione sollevati dal regolamento. Tra questi vi è la nozione di «contenuto illegale» (sottinteso, online) di cui all'art. 3, lett. h), che costituisce l'oggetto di questo volume e che inevitabilmente attirerà l'attenzione di esperti di varie discipline giuridiche, inclusi studiosi del Diritto dell'Unione europea. È allora da quest'ultima precisazione che si intende partire per definire l'obiettivo del presente lavoro. La domanda alla quale si cercherà di rispondere è: nel tentativo di sondare la portata applicativa del concetto di «contenuto illegale», come potrebbe o dovrebbe essere interpretato l'art. 3, lett. h, del regolamento (UE) 2022/2065?

Prima di procedere, però, preme rappresentare che nel diritto dell'Unione la questione definitoria determina spesso difficoltà interpretative di rilievo. Anche solo riferendosi, per ovvie ragioni di opportunità, all'ecosistema giuridico nel quale si situa il DSA, ovverosia il diritto UE in materia di digitale, si nota con facilità che non mancano lacune concettuali più o meno profonde. Ad esempio, per molto tempo sono rimaste

[1] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in GUUE L 277/1 del 27 ottobre 2022.

oscure le nozioni cardine del paradigma della *sharing economy*, a cominciare dalla definizione operativa di «piattaforma online»[2]; che sono trascorsi anni prima che fossero quantomeno abbozzato il significato di «contenuto digitale», «servizio digitale» e «beni con elementi digitali»[3]; che il concetto di mercato unico digitale è tutto sommato ambiguo[4]; e che in diritto UE non esiste una definizione di «intelligenza artificiale», quanto piuttosto quella di «sistema di intelligenza artificiale», invero flessibile e suscettibile di lasciare ampi margini interpretativi[5], con tutto ciò che ne può conseguire.

Quanto appena accennato non deve indurre a pensare che il diritto dell'Unione europea viva di approssimazione. Anche nell'ordinamento giuridico dell'Unione circolano "anticorpi" che consentono – entro certi limiti – alle regole di volta in volta prodotte di beneficiare di un'attuazione effettiva, omogenea e ancorata al diritto di matrice più evidentemente costituzionale, nonostante eventuali carenze in merito alle definizioni di concetti (im)portanti.

Al riguardo, preme enfatizzare il valore aggiunto della giurisprudenza della Corte di giustizia dell'Unione europea (CGUE, Corte di giustizia, o Corte), che resta senza dubbio la principale autorità (anche) in merito alla trattazione delle questioni definitorie derivanti dal diritto dell'Unione. Già nei casi in cui l'attività di costruzione o riempimento di una nozione debba essere lasciata al diritto nazionale, la Corte ha statuito che ciò non può affatto comportare che gli Stati membri agiscano in maniera totalmente discrezionale[6]. Naturalmente, vi è da attendersi che il ruolo della Corte divenga ancor più incisivo qualora i concetti da vagliare siano stati definiti dal legislatore dell'Unione o debbano comunque avere un significato di diritto UE.

Pertanto, per costruire almeno le fondamenta di una risposta plausibile alla domanda di cui sopra, si procederà ragionando sui criteri di cui la CGUE, secondo una giurisprudenza ormai costante, si avvale per interpretare disposizioni di diritto dell'Unione: la formulazione testuale della disposizione analizzata, il contesto nel quale questa si inquadra, e gli obiettivi perseguiti dalla normativa di riferimento[7]; il tutto cercando

[2] In particolare, M. INGLESE, *The Collaborative Economy Legal Conundrum: A Way Forward Through Harmonization, in Legal Issues of Economic Integration*, in «Legal Issues of Economic Integration», XLV, (2018), pp. 375-396.

[3] Per considerazioni su questioni giuridiche relative a queste carenze si rinvia a J. HOJNIK, *Technology Neutral EU Law: Digital Goods Within the Traditional Goods/Services Distinction*, in «International Journal of Law and Information Technology», XXV (2017), pp. 63-84. Sulle incertezze attorno al concetto di «digital asset» si veda J. SOUKUPOVÁ, *Analysis of the Notion of Digital Assets in the Context of Fragmented Terminology*, in «The Lawyer Quarterly», XIV (2024), pp. 385-404.

[4] Sia permesso di rinviare a F. FERRI, *Bilanciamento dei diritti fondamentali e mercato unici digitale*, Giappichelli, Torino, 2022, pp. 53-56.

[5] C. SCHEPISI, *Prefazione*, in «Quaderni AISDUE», fascicolo speciale "L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive", I (2024), p. 12.

[6] Per considerazioni più approfondite su detti limiti, si veda B. DE WITTE, *Les compétences exclusives des états membres existent-elles?*, in Liber amicorum *per Antonio Tizzano : de la Cour CECA à la Cour de l'Union : le long parcours de la justice Européenne*, a cura di AA.VV., Giappichelli, Torino, 2018, pp. 301-315.

[7] V. *ex multis*: Corte di giustizia, causa C-292/82, *Merck Hauptzollamt Hamburg-Jonas*, 17 novembre 1983, ECLI:EU:C:1983:335, punto 12; C-223/98, *Adidas*, 14 ottobre 1999, ECLI:EU:C:1999:500, punto 23; C-491/01,

altresì di trarre elementi pertinenti dai lavori preparatori[8] e tenendo a mente il criterio della ragionevolezza[9], nonché i principi dell'effetto utile[10], dell'interpretazione conforme[11] e della leale cooperazione[12].

Lungi dall'indagare i profili di responsabilità a fronte di contenuti illegali online[13], nei paragrafi seguenti ci si prefigge perciò di chiarire i presupposti in virtù dei quali la nozione di «contenuto illegale», nell'economia del DSA, sembra destinata ad essere interpretata in maniera significativamente ampia; ciò sulla scorta di considerazioni analitiche che attengono ai criteri interpretativi testuale (par. 2), sistematico (par. 3) e teleologico (par. 4). Al termine dell'analisi saranno avanzati alcuni spunti conclusivi di riflessione (par. 5).

2. *Cenni alla formulazione della definizione*

Per interpretare al meglio la nozione di «contenuto illegale» nel regolamento (UE) 2022/2065, il primo passaggio da compiere è cercare di trarre informazioni utili dal testo dell'art. 3, lett. h (che non sarà riprodotto di seguito, in quanto già riportato altrove in questo volume). La sensazione è che l'esercizio da compiere a questo stadio si scontri con una formula volutamente vaga, e che pertanto le conclusioni intermedie sarebbero abbastanza riduttive. D'altronde, è sufficiente leggere la pagina *web* della Commissione sulle domande e risposte sul DSA per avere conferma di una circostanza ormai certa,

British American Tobacco (Investments) e Imperial Tobacco, 10 dicembre 2002, ECLI:EU:C:2002:741, punto 203; C-294/01, *Granarolo*, 13 novembre 2003, ECLI:EU:C:2003:611, punto 34; C-45/05, *Maatschap Schonewille-Prins*, 24 maggio 2007, ECLI:EU:C:2007:296, punto 30; C-561/13, *Hoštická e altri*, 15 ottobre 2014, ECLU:EU:C:2014:2287, punto 29; C-222/14, *Maïstrellis*, 16 luglio 2015, ECLI:EU:C:2015:473, punto 30; C-509/22, *Girelli Alcool*, 18 aprile 2024, ECLI:EU:C:2024:341, punto 77.

[8] In questo senso si vedano, ad esempio, Corte di giustizia, C-548/18, *BGL BNP Paribas*, 9 ottobre 2019, EU:C:2019:848, punto 25; C-24/19, *A e a. (Impianti eolici ad Aalter e Nevele)*, 25 giugno 2020, ECLI:EU:C:2020:503, punto 37; C-624/20*, E.K. contro Staatssecretaris van Justitie en Veiligheid*, 7 settembre 2022, ECLI:EU:C:2022:639, punto 28; C-63/23, *Sagrario e a. contro Subdelegación del Gobierno en Barcelona*, 12 settembre 2024, ECLI:EU:C:2024:739, punto 37. V. diffusamente anche S. Lattanzi, *«Travaux preparatoires» del diritto dell'Unione europea: tassonomia, ruolo e funzioni*, CEDAM, Padova, 2022.

[9] P. De Pasquale, A. Circolo, *Il criterio della ragionevolezza nella più recente giurisprudenza della Corte di giustizia*, in «Il Diritto dell'Unione europea», XXIX (2024), pp. 1-52.

[10] I. Ingravallo, *L'effetto utile nell'interpretazione del diritto dell'Unione europea*, Cacucci, Bari, 2017.

[11] A. Bernardi, *L'interpretazione conforme al diritto dell'Unione europea: profili e limiti di un vincolo problematico. Atti del Convegno inaugurale del Dottorato di ricerca "Diritto dell'Unione europea e ordinamenti nazionali" del Dipartimento di giurisprudenza dell'Università di Ferrara, Rovigo*, 15-16 maggio 2014, Jovene, Napoli, 2015.

[12] F. Casolari, *Leale cooperazione tra stati membri e Unione europea: studio sulla partecipazione all'Unione al tempo delle crisi*, Editoriale Scientifica, Napoli, 2020.

[13] Sul tema ci si rifà anzitutto all'analisi sviluppata da G. Morgese, *Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE*, in «Federalismi.it», 12 gennaio 2022, pp. 79-126. Sull'evoluzione del tema nel quadro del DSA, cfr. G. Monga*, Responsabilità degli intermediari. Il Digital Services Act*, in *Il commercio elettronico*, a cura di M. Maggiore, Giappichelli, Torino, 2024, pp. 192-237. Per considerazioni alla luce di esempi specifici derivanti dalla prassi, si veda A. Vicinanza, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso Telegram al Digital Services Act*, in «Quaderni AISDUE», II (2025), pp. 1-18.

cioè che la legge sui servizi digitali non definisce ciò che è illegale online: le definizioni – per così dire – "mancanti" sono contenute in altre normative UE o disposte da misure nazionali, con il risultato che se un contenuto è illegale solo in un determinato Stato membro di norma dovrebbe essere rimosso unicamente nel rispettivo territorio[14].

Ad ogni modo, si ritiene utile illustrare per sommi capi come la nozione di «contenuto illegale» si sia evoluta nel corso dell'*iter* legislativo che ha condotto all'adozione della legge sui servizi digitali. In particolare, nella proposta della Commissione, all'art. 2, lett. g), tale concetto veniva definito come «qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni»[15]. Una simile ricostruzione pare più fluida rispetto a quella dell'atto legislativo. Al contempo, tuttavia, rappresentava una rivisitazione maggiormente elaborata in confronto alla concettualizzazione essenziale di cui alla precedente raccomandazione della Commissione sulle misure per contrastare efficacemente i contenuti illegali online, peraltro ripresa testualmente nello *Staff Working Document* di accompagnamento alla proposta: «qualunque informazione non conforme al diritto dell'Unione o alle leggi di uno Stato membro interessato»[16].

È plausibile che vi siano due ragioni di fondo per giustificare il cambio di registro linguistico nell'ultima parte della definizione concordata da Parlamento europeo e Consiglio.

Da una parte, sostituendo la locuzione «disposizioni normative» con la parola «diritto», il legislatore dell'Unione ha forse ritenuto opportuno scongiurare alla radice il rischio di interpretazioni eccessivamente restrittive da parte delle autorità competenti degli Stati membri. La tesi che si sostiene sembra essere accreditata da scelte di carattere formale/sostanziale effettuate già in sede di redazione del testo dei Trattati istitutivi, con le quali si è inteso aprire a un approccio quasi omnicomprensivo rispetto alle varie fonti di produzione. Emblematico è il caso dell'art. 114 TFUE, avente ad oggetto le misure sovranazionali di armonizzazione nell'ambito del mercato interno, che allude al ravvicinamento delle disposizioni non solamente legislative, ma anche regolamentari ed amministrative degli Stati membri.

Per altro verso, nella definizione prevista all'art. 3, lett. h), del DSA si intravede in maniera più nitida il ruolo subalterno del diritto nazionale, laddove si menziona, quale

[14] https://ec.europa.eu/commission/presscorner/detail/it/qanda_20_2348. Per tentare di limitare gli effetti potenzialmente negativi di tale scelta, è stata adottata la Raccomandazione (UE) 2023/2425 della Commissione del 20 ottobre 2023 sul coordinamento delle risposte agli incidenti, in particolare derivanti dalla diffusione di contenuti illegali, in vista della piena entrata in applicazione del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio («regolamento sui servizi digitali»), in GUUE L del 26 ottobre 2023.

[15] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM(2020) 825 final, 15 dicembre 2020.

[16] Raccomandazione (UE) 2018/334 della Commissione del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali online, in GUUE L 63/50, 6 marzo 2018. punto 4, lett. d). Si veda anche SWD (2020) 348 final, p. 2.

possibile elemento costitutivo della fattispecie «contenuto illegale» anche la contrarietà al diritto di uno Stato membro, ma sempre che questo diritto sia conforme a quello dell'Unione. Tale aggiunta richiama inevitabilmente il principio del primato del diritto UE, al netto di qualsivoglia ragionamento sull'effetto diretto della regola di volta in volta assunta a termine di confronto[17]. Inoltre, si ritiene che così facendo si sia inteso costruire un canale di comunicazione più scorrevole tra il DSA e quella giurisprudenza della Corte di giustizia che ha contribuito a rafforzare gli argini alla pretesa arbitrarietà degli Stati membri in campi d'azione sottoposti alla loro responsabilità esclusiva[18].

Conviene poi aggiungere qualche breve osservazione su cosa non debba essere scambiato aprioristicamente con un contenuto illegale a norma del DSA. Rimane infatti in sospeso, almeno in una certa misura, la qualificazione giuridica dei contenuti «dannosi». Questa categoria viene menzionata in pochi passaggi del regolamento, specialmente in alcuni considerando. A prima vista, l'utilizzo estemporaneo di una simile espressione potrebbe determinare perplessità, stante l'assenza di un'apposita definizione. Viene però in aiuto la relazione introduttiva alla proposta della Commissione[19], dalla quale si evince anzitutto che tra contenuti illegali e contenuti dannosi non sussiste un rapporto genere-specie, nel senso che i secondi possono configurare ipotesi conformi al diritto UE e/o nazionale. Inoltre, la relazione chiarisce che i portatori di interessi consultati prima della preparazione della proposta di regolamento avevano concordato, in linea generale, sul fatto che i contenuti dannosi non dovessero essere definiti né assoggettati a obblighi di rimozione, poiché la questione era stata ritenuta particolarmente delicata e idonea a causare gravi implicazioni per la protezione della libertà di espressione; libertà, questa, che assume un peso specifico di prim'ordine nel sistema di tutele derivante dal DSA, come si avrà modo di spiegare nel prosieguo dell'analisi.

3. *Uno sguardo al contesto giuridico applicativo*

Se dal criterio testuale non emergono spunti particolarmente significativi per avere un'idea più precisa di come debba essere inteso il concetto di «contenuto illegale» quale cardine del regolamento (UE) 2022/2065, dal contesto in cui l'art. 3, lett. h), si inserisce possono invece ricavarsi elementi di maggiore interesse.

Rimanendo entro il perimetro del regolamento, è appena il caso di volgere lo sguardo verso la parte motivazionale dello stesso. In effetti, la Corte di giustizia è solita interpre-

[17] In argomento, si rinvia a L.S. Rossi, C. Tovo, *Il principio del primato del diritto dell'Unione Europea*, in *Europa*, a cura di G. Amato, Istituto della Enciclopedia Italiana fondata da Giovanni Treccani, Roma, 2023, pp. 97-109.

[18] Ci si riferisce, in particolare, a sentenze sui limiti alle prerogative degli Stati membri in ambiti quali la sicurezza nazionale (art. 4, par. 2, TUE), l'ordine pubblico e la sicurezza interna (art. 72 TFUE): cf., ad esempio, Corte di giustizia, cause riunite C-715/17, C-718/17 e C-719/17, *Commissione c. Polonia, Repubblica Ceca e Ungheria*, 2 aprile 2020, ECLI:EU:C:2020:257, punto 145; C-511/18, *La Quadrature du Net*, 6 ottobre 2020, ECLI:EU:C:2020:791, punto 99.

[19] COM(2020) 825 final, cit., p. 10.

tare le disposizioni di regolamenti, direttive e decisioni anche avvalendosi dei considerando più pertinenti, prima di cercare soccorso, se del caso, nei lavori preparatori o in ulteriori strumenti che concorrono a formare il contesto di riferimento. Ebbene, il considerando 12 del DSA mette a disposizione dell'interprete alcune importanti coordinate.

Innanzitutto, il considerando 12 anticipa un dato di chiaro valore: il concetto di «contenuto illegale» – si legge – «dovrebbe essere definito in senso lato». Se ne può desumere che la nozione in parola deve essere, per forza di cose, ampia. Il punto è che la costruzione di questo concetto diviene funzionale alla garanzia di un ambiente online sicuro, prevedibile e affidabile. Non si tratta, naturalmente, si una peculiarità esclusiva del DSA, bensì di una finalità tipica del mercato unico digitale dell'Unione e, più in generale, della transizione digitale europea. Non a caso, infatti, il considerando 12 sottolinea la necessità che il concetto di «contenuto illegale» sia riferito il più possibile alle norme vigenti nell'ambiente offline, rievocando quel mantra ormai noto nella *soft law* UE secondo cui ciò che è illegale offline deve essere considerato illegale anche online.

Per orientare efficacemente l'interpretazione del concetto in questione, il considerando 12 aggiunge un elenco non tassativo di esempi di contenuti illegali. Sostanzialmente, tale concetto copre "anche" le informazioni, indipendentemente dalla loro forma, che riguardano i prodotti, i servizi e le attività illegali; in aggiunta, esso assorbe le ipotesi di incitamento all'odio, contenuti terroristici e discriminatori. Sono contenuti illegali pure quelli che le norme applicabili rendono tali poiché riguardanti attività illegali[20].

Vi è poi un inciso, nel considerando 12, che non era stato contemplato nella proposta della Commissione e che simboleggia un'eccezione dal punto di vista della tecnica legislativa a livello UE. Si tratta di una frase che enuncia un esempio di ciò che non deve essere considerato contenuto illegale[21]. Questo slancio appare alquanto significativo, dal momento che permette di dettagliare ulteriormente lo spazio operativo che il concetto di «contenuto illegale» dovrebbe avere in uno scenario giuridico multilivello.

Oltre alla parte motivazionale del DSA, il contesto che fa da sfondo all'art. 3, lett. h), ricomprende altre misure complementari. Su tutte, il regolamento (UE) 2022/1925 sui mercati digitali (*Digital Markets Act* o DMA)[22] e, in misura minore ma non certo marginale, il regolamento (UE) 2024/1689 sull'intelligenza artificiale (*Artificial Intelli-*

[20] A tenore del considerando 12, «(t)ra queste figurano, a titolo illustrativo, la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il cyberstalking (pedinamento informatico), la vendita di prodotti non conformi o contraffatti, la vendita di prodotti o la prestazione di servizi in violazione della normativa sulla tutela dei consumatori, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore, l'offerta illegale di servizi ricettivi o la vendita illegale di animali vivi».

[21] Il considerando 12 del DSA si riferisce a video di un testimone oculare di un potenziale reato e spiega che detto contenuto non dovrebbe essere considerato illegale «per il solo motivo di mostrare un atto illecito quando la registrazione o la diffusione di tale video al pubblico non è illegale ai sensi del diritto nazionale o dell'Unione».

[22] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 19 ottobre 2022 del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in GUUE L 265/1 del 12 ottobre 2022.

gence Act o *AI Act*)[23] e il regolamento (UE) 2024/1083 sulla libertà dei media (*European Media Freedom Act* o *EMFA*)[24]. Senza che vi sia bisogno di indugiare oltremodo sulle interconnessioni questi tra strumenti, ci si limita qui a ricordare (per poi sviluppare ulteriormente il ragionamento nel paragrafo successivo) come anche il DMA, l'*AI Act* e l'EMFA siano volti, in ultima analisi, a restringere il margine di azione di attori che hanno alte probabilità di condizionare il mercato unico digitale e di giocare un ruolo ambivalente nella lotta contro i contenuti illegali online[25].

Infine, merita una menzione a parte l'armamentario giuridico che l'Unione europea ha messo in campo per rispondere a determinate minacce rivolte contro l'Unione stessa o alcuni Stati membri, e facenti capo, direttamente o indirettamente, alla Federazione Russa. Ci si riferisce ai pacchetti di sanzioni adottati nell'ambito della politica estera e di sicurezza comune, che includono misure restrittive con cui l'UE ha deciso di sospendere le trasmissioni e le licenze (nel territorio degli Stati membri) di media sostenuti dal governo russo e ritenuti responsabili di azioni di propaganda e disinformazione[26]. Ora, con precipuo riferimento alle ipotesi di disinformazione, va detto che il DSA riconduce questa fattispecie ai «contenuti fuorvianti o ingannevoli»[27], che non sono di per sé necessariamente illegali[28]. Tuttavia, nella legge sui servizi digitali sia la disinformazione sia i contenuti illegali sono presentati come categorie altamente rischiose per la società europea[29], tanto da essere spesso menzionate l'una accanto all'altra nella parte motivazionale dell'atto. Si reputa quindi pertinente e rilevante enfatizzare la scelta dell'Unione di rispondere a pericoli paragonabili alla circolazione di contenuti illegali online con iniziative a tratti senza precedenti, perché non solo esulano dalla sfera della legislazione sovranazionale, incidono in modo diretto e intenso sui destinatari e dipendono dal raggiungimento dell'unanimità degli Stati membri in Consiglio, ma configurano una novità assoluta anche nel panorama delle sanzioni UE.

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

[24] Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media), in GUUE 2024/1083 del 17 aprile 2024.

[25] Si vedano in particolare i considerando 62 del DMA, 110 dell'*AI Act*, e 45 dell'EMFA.

[26] Si vedano. in particolare Decisione (PESC) 2022/351 del Consiglio del 1° marzo 2022 che modifica la decisione 2014/512/PESC concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina in GUUE L 65/5 del 2 marzo 2022, e il Regolamento (UE) 2022/350 del Consiglio del 1° marzo 2022 che modifica il regolamento (UE) n. 833/2014 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, in GUUE L 65/1 de 2 marzo 2022.

[27] Si veda il considerando 84 del DSA.

[28] Si veda anche M. Husovec, *The Digital Services Act's Red Line: what the Commission Can and Cannot Do About Disinformation*, in «Journal of Media Law», XVI, (2024), pp. 49-50.

[29] V. DSA, specialmente considerando 2 e 9. Il considerando 104 allude alla disinformazione quale rischio sistemico sulle società e sulla democrazia.

4. *Considerazioni sugli obiettivi perseguiti dalla misura di riferimento*

Occorre, da ultimo, ampliare gli orizzonti interpretativi e addentrarsi nelle finalità del regolamento (UE) 2022/2065.

Il primo rilievo è che, come osservato in dottrina, il fulcro del DSA è rappresentato dal potere del prestatore di servizi intermediari di adottare misure restrittive a fronte di contenuti illegali, senza la necessità di un previo provvedimento di un'autorità[30]. Attorno a questo dato di fatto conviene svolgere riflessioni di carattere più generale.

Intanto, il DSA è una misura di armonizzazione, come testimoniato anche dalla scelta del legislatore dell'Unione di utilizzare come base giuridica il predetto art. 114 TFUE. L'armonizzazione ricercata con il DSA, a tenore dell'art. 1, riguarda soprattutto taluni punti chiave relativi alla prestazione dei servizi intermediari nel mercato interno: l'esenzione condizionata dalla responsabilità, gli obblighi di *due diligence* per determinate categorie di *providers* e vari aspetti concernenti l'attuazione e l'esecuzione regolamento. Verosimilmente, tale misura dà corpo a un riscontro per certi versi tardivo rispetto alle teorie più accreditate sull'esigenza di mettere mano alla normativa sovranazionale in materia di servizi, giudicata in buona parte carente[31], anche in considerazione della consistente incidenza di questa porzione di mercato rispetto al prodotto interno lordo dell'Unione.

Il concetto di «contenuto illegale» di cui all'art. 3, lett. h), del DSA dovrà dunque essere interpretato e applicato in modo da non risultare un elemento di frammentazione del mercato interno, cosa che richiede necessariamente un'interpretazione il più possibile aderente all'effetto utile dell'intero atto legislativo; ciò specie se si tiene presente che, a causa del carattere intrinsecamente transfrontaliero di Internet, eventuali legislazioni nazionali riguardanti diverse componenti del regolamento avrebbero un'incidenza probabilmente negativa sul mercato.

Sarebbe tuttavia limitante considerare la legge sui servizi digitali come una misura unicamente preposta al perseguimento di obiettivi di mercato. Essa presenta infatti una doppia anima: accanto alla dimensione mercantilistica, vi è quella relativa alla tutela e alla promozione dei diritti fondamentali[32], che nello strumento in questione

[30] G. Proietti, *L'impianto regolatorio della società dell'informazione tra vecchi e nuovi equilibri. Il fenomeno del* deep fake, in «MediaLaws», VIII (2024), pp. 336-337.

[31] Si rinvia a vari contenuti del Rapporto "Una nuova strategia per il mercato unico al servizio dell'economia e della società europea", presentato da Mario Monti all'allora Presidente della Commissione europea, José Manuel Barroso, il 9 maggio 2010. Per un'analisi più recente, si veda il Rapporto "The future of European competitiveness", presentato da Mario Draghi il 9 settembre 2024.

[32] Cfr. anche G. Caggiano, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *Verso una legislazione europea su mercati e servizi digitali*, a cura di G. Caggiano, G. Contaldi, P. Manzini, Cacucci editore, Bari, pp. 3-30; G. Frosio, C. Geiger, *Taking fundamental rights seriously in the Digital Services Act's Platform Liability Regime, in* «European Law Journal» XXIX, (2023), pp. 31-77.

assume contorni quasi assiologici[33]. L'art. 1 del regolamento, in questo senso, è emblematico, giacché associa a finalità di mercato la creazione di un ambiente online sicuro, prevedibile e affidabile, «in cui i diritti fondamentali sanciti dalla Carta (…) siano tutelati in modo effettivo».

Non si tratta di un connotato distintivo esclusivo del DSA, atteso che altri atti legislativi pensati per dare impulso al mercato unico digitale e alla transizione digitale europea muovono da una ragion d'essere del tutto analoga[34]: ne sono esempi tangibili il DMA[35], l'EMFA[36] e, soprattutto, l'*AI Act*[37]; anche il Regolamento (UE) 2016/679, ossia il regolamento generale sulla protezione dei dati personali (GDPR)[38], è ispirato da queste complesse dinamiche, benché abbia per base giuridica l'art. 16 TFUE, sul diritto alla protezione dei dati a carattere personale, a sua volta riconosciuto e garantito l'art. 8 della Carta dei diritti fondamentali[39]. I propositi riconducibili alla salvaguardia di certi diritti fondamentali nell'ambiente online in un impianto giuridico strumentale al buon funzionamento di un mercato interno in costante evoluzione rendono così il DSA una manifestazione della dottrina del costituzionalismo digitale (europeo)[40], e quindi un atto condizionato dalle traiettorie di forze in parte contrapposte, ma che ormai non possono più essere considerate separatamente[41].

È in questa ulteriore cornice che occorre completare la lettura dell'art. 3, lett. h), del DSA. La nozione di «contenuto illegale» non può prescindere da un'interpretazione costituzionalmente orientata e indirizzata verso l'art. 6 TUE, il quale – tra le altre cose –

[33] F. Ferri, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in «Il Diritto dell'Unione europea», XXVII (2022), spec. pp. 306-315.

[34] Più in generale, si veda C. Amalfitano, F. Ferri, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in *La trasformazione digitale in Europa. Diritti e principi*, a cura di R. Torino, S. Zorzetto, Giappichelli, Torino, 2023, pp. 1-34.

[35] Cfr., in specie, C. Massa, *Ultimi sviluppi della riforma del digitale in Europa: il Digital Markets Act tra costituzionalismo europeo e concorrenza*, in *Quaderno AISDUE serie speciale, Atti del Convegno "L'Unione europea dopo la pandemia", Bologna 4-5 novembre 2021*, a cura di Aa.Vv., Editoriale Scientifica, Napoli, 2022, pp. 293-316.

[36] L. Ciliberti, *DSA e EMFA: speciale responsabilità delle piattaforme online e tutela della libertà dei media*, in «Rivista italiana di informatica e diritto», VI (2024), pp. 213-357.

[37] Ad esempio, C. Schepisi, *Diritti fondamentali, principi democratici e rule of law: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, in «Studi sull'integrazione europea», XVII (2022), pp. 41-66.

[38] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GUUE L 119/1 del 4 maggio 2016.

[39] Ancora, sulla doppia anima di cui sopra – nello specifico riguardante il GDPR – si veda in particolare, D. Messina, *Online Platforms, Profiling, and Artificial Intelligence: New Challenges for the GDPR and, in Particular, for the Informed and Unambiguous Data Subject's Consent*, in «MediaLaws», III (2019), p. 163.

[40] O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Bloomsbury Publishing, Oxford, 2021; E. Celeste, *Digital Constitutionalism. The Role of Internet Bills of Rights*, Routledge, London, 2022; G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge, 2022.

[41] Per tutti, V. Kosta, *Fundamental Rights in EU Internal Market Legislation*, Hart publishing, Oxford, 2018.

riconosce ai diritti fondamentali garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo (CEDU) e risultanti dalle tradizioni costituzionali comuni agli Stati membri il rango di principi generali di diritto UE, per poi assegnare alla Carta dei diritti fondamentali lo «stesso valore giuridico dei trattati» (istitutivi dell'Unione stessa)[42].

Diviene allora di assoluto rilievo il fatto che DSA sia manifestamente innevato da esigenze di tutela dei diritti fondamentali, al punto da essere stato presentato anche come «human-rights-infused regulation»[43]. Ne deriva che la Carta dovrà poter essere utilizzata come "scudo protettivo" contro i contenuti illegali. In altre parole, la legge sui servizi digitali (proposta in concomitanza con il lancio della Strategia per rafforzare l'applicazione della Carta[44] e poco prima della pubblicazione di una relazione annuale sull'applicazione della Carta che verteva proprio sulla tutela dei diritti fondamentali nell'ambiente digitale[45]) offre alla Carta numerose disposizioni di appoggio con annessi interstizi che le consentono di penetrare nel corpo dell'atto e di essere invocata con maggiore probabilità di successo anche allo scopo di limitare il più possibile la diffusione dei contenuti illegali online.

A riprova di quanto si afferma, e a mero titolo esemplificativo, il considerando 1 del DSA precisa da subito come la trasformazione digitale e il maggiore utilizzo dei servizi oggetto del regolamento abbiano anche dato origine a nuovi rischi e sfide per i singoli destinatari; e il considerando 3 collega le azioni di prevenzione e contrasto dei contenuti illegali da parte dei prestatori di servizi intermediari all'esercizio dei diritti fondamentali. Ecco che allora nel DSA l'approccio al rischio rispetto ai beni da tutelare è stato centralizzato, a differenza di quanto accaduto in precedenti atti comunque ascrivibili alla dottrina del costituzionalismo digitale europeo (in particolare, il GDPR)[46]. Una manifestazione assai visibile di questa scelta è la previsione di obblighi più stringenti per piattaforme e motori di ricerca particolarmente condizionanti, proprio perché si ritiene che possano essere maggiormente in grado di mettere a repentaglio i diritti fondamentali attraverso condotte attive od omissive in relazione alla diffusione dei contenuti illegali online[47]. È anche in considerazione di questi aspetti che nella proposta della

[42] Per considerazioni diffuse sul tema si vedano, *ex multis*, C. Amalfitano, *Il diritto non scritto nell'accertamento dei diritti fondamentali dopo la riforma di Lisbona*, in «Il Diritto dell'Unione europea», XXI (2016), pp. 21-70, L.S. Rossi, *"Stesso valore giuridico dei Trattati"? Rango, primato ed effetti diretti della Carta dei diritti fondamentali dell'Unione europea*, «Il Diritto dell'Unione europea» XXI (2016), pp. 329-356.

[43] A.P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, in *Digital Platform Regulation: Global Perspectives on Internet Governance*, a cura di T. Flew, F.R. Martin (eds.), Springer, Cham, 2022, p. 76.

[44] Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Tutela dei diritti fondamentali nell'era digitale" - Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea, COM(2021) 819 final, 10 dicembre 2021.

[45] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Strategia per rafforzare l'applicazione della Carta dei diritti fondamentali dell'Unione europea", COM(2020) 711 final, 2 dicembre 2020.

[46] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in «Common Market Law Review», LIX (2022), pp. 473-500.

[47] Ci si riferisce soprattutto a piattaforme e motori di ricerca online di dimensioni molto grandi. Sono tali le piattaforme e i motori di ricerca online che hanno, in particolare, un numero medio mensile di destinatari attivi

Commissione il collegamento tra obiettivi di contrasto ai contenuti illegali e protezione dei diritti fondamentali era risultato dirimente per giustificare il rispetto dei principi di sussidiarietà e proporzionalità[48], quali principi fondamentali relativi all'esercizio delle competenze dell'Unione a tenore dell'art. 5, par. 3 e par. 4, TUE.

Rimane casomai da chiedersi quali siano i diritti fondamentali realmente esposti, e dunque meritevoli di tutela mediante la legge sui servizi digitali. La domanda è lecita se si tiene a mente che l'approccio delineato con il DSA – anche in funzione dell'attuazione degli obblighi in materia di contenuti illegali – è chiaramente orientato a privilegiare la tutela della libertà di espressione e informazione, sancita dall'art. 11 della Carta e dall'art. 10 della CEDU. Lo dimostrano numerosissimi passaggi dell'atto, rinvenibili sia all'interno della parte motivazionale, sia in vari articoli.

Ma vi è di più. In linea con la visione del Commissario europeo per l'agenda digitale nel quinquennio 2019-2024 in occasione della presentazione del DSA (Margrethe Verstager), nonché con l'opinione di diversi autori, si ritiene che natura e obiettivi del DSA affondino le radici oltre la Carta, arrivando direttamente fino al nucleo identitario dell'ordinamento giuridico dell'Unione, costituito dai valori fondanti enunciati dall'art. 2 TUE[49], segnatamente lo stato di diritto, la democrazia e – appunto – la tutela dei diritti fondamentali[50]. Attraverso molte disposizioni della legge sui servizi digitali, insomma, si riesce a intravedere, quantomeno in filigrana, quella che è stata concepita come una «imperialist extension of European constitutional values»[51], oltre che una scelta con cui sarebbe possibile delineare in maniera ancora più netta l'identità in senso assiologico dell'Unione europea[52]. Tale collegamento tra contrasto ai contenuti illegali online nel quadro del DSA e difesa dei valori UE traspare anche nelle pieghe di un

del servizio nell'Unione pari o superiore a 45 milioni (art. 33, par. 1, DSA). La designazione è effettuata dalla Commissione europea. Maggiori informazioni sono disponibili a questo link: https://digital-strategy.ec.europa.eu/it/policies/list-designated-vlops-and-vloses.

[48] COM(2020) 825 final, cit., pp. 6-7.

[49] Corte di giustizia, C-157/21*, Repubblica di Polonia c. Parlamento europeo e Consiglio*, 16 febbraio 2022, ECLI:EU:C:2016:970, punto 145.

[50] Secondo Verstager, «[t]here's no doubt […] that platforms – and the algorithms they use – can have an enormous impact on the way we see the world around us. And that's a serious challenge for our democracy. Because today, a few big platforms are increasingly important as the place where we go for news and information, the place where we carry on our political debates. They define our public space – and the choices they make affect the way our democracy works. They affect the ideas and arguments we hear – and the political choices we believe we can make. They can undermine our shared understanding of what's true and what isn't – which makes it hard to engage in those public debates that are every bit as important, for a healthy democracy, as voting itself. So we can't just leave decisions which affect the future of our democracy to be made in the secrecy of a few corporate boardrooms. That's why one of the main goals of the Digital Services Act […] will be to protect our democracy, by making sure that platforms are transparent about the way these algorithms work – and make those platforms more accountable for the decisions they make» (Speech 30 October 2020 "Algorithms and democracy" – Algorithm Watch Online Policy Dialogue, 30 October 2020, ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/algorithms-and-democracy-algorithmwatch-online-policy-dialogue30-october-2020_en).

[51] G. De Gregorio, *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in «Diritti comparati», 17 maggio 2021.

[52] F. Resta, *I poteri privati e gli àrbitri dei diritti*, in «MediaLaws», 1 dicembre 2020.

atto di *soft law* ma pur sempre d'impatto come la Dichiarazione comune europea sui diritti e i principi digitali per il decennio digitale, proclamata solennemente nel 2023 da Parlamento europeo, Consiglio dell'Unione e Commissione[53].

Le considerazioni appena svolte non sembrano perdere valore alla luce del *focus* del DSA sulla libertà di espressione e informazione, prima ancora che su altri diritti fondamentali. Invero, come affermato dalla Corte di giustizia nella sentenza *Tele2 Sverige*, questa libertà è dotata di una importanza particolare, sì da costituire «uno dei fondamenti essenziali di una società democratica e pluralista, facente parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione è fondata»[54]. E il Tribunale di primo grado, nella sentenza *R.T. France c. Consiglio*, resa a conclusione di un'azione volta ad ottenere l'annullamento di misure restrittive UE contro media russi per contrastare le già accennate campagne di propaganda e disinformazione[55], ha indirettamente rafforzato questo binomio: la pronuncia, infatti, lega saldamente l'art. 11 della Carta, i valori dell'Unione e fattispecie che, come visto in precedenza, nell'insieme del DSA hanno sostanza assimilabile (ancorché non identica) a quella della categoria dei contenuti illegali.

5. *Rilievi conclusivi*

L'indagine realizzata nei paragrafi precedenti suggerisce che, a prescindere dalle incertezze alimentate dall'art. 3, lett. h, del regolamento (UE) 2022/2065, occorre che all'espressione «contenuto illegale» corrisponda una concezione particolarmente estesa. Propendere per un'interpretazione restrittiva di tale nozione darebbe infatti luogo a cortocircuiti. Si rischierebbe innanzitutto di privare la disposizione in esame di un grado accettabile di effettività, in controtendenza rispetto a più riferimenti testuali del DSA. Aumenterebbero poi le probabilità di compromettere la sostenibilità di detto concetto in una logica di sistema. Senza contare che, nella peggiore delle ipotesi, si inibirebbero interessi evidentemente proiettati su un piano costituzionale, nel quale si incontrano la Carta e – a tratti – i valori fondanti dell'Unione.

Di conseguenza, se è vero che l'art. 3, lett. h, del DSA sembra lasciare vasti spazi di manovra in ambito esegetico, si ritiene che l'interprete dovrà comunque rispettare diversi limiti, al fine di garantire al meglio il rispetto del diritto dell'Unione anche al di là della lettera della disposizione, e comunque in ossequio al più ampio dovere di collaborazione tra livelli. Pertanto, sarà compito anche delle autorità nazionali competenti, con a capo i giudici interni, garantire che il concetto di «contenuto illegale» sia

[53] Cfr. anche P. De Pasquale, *Verso una Carta dei diritti digitali (fondamentali)dell'Unione europea?*, in «Il Diritto dell'Unione europea», 17 marzo 2022.

[54] Corte di giustizia, C-203/15 e C-698/15*, Tele2 Sverige AB*, 21 dicembre 2016, ECLI:EU:C:2016:970, punto 93.

[55] Tribunale di primo grado, T-125/22, *RT France c. Consiglio dell'Unione europea*, 27 luglio 2022, ECLI:EU:-T:2022:483. Il Tribunale ha rigettato il ricorso esperito contro le misure che disponevano le sanzioni contestate.

applicato in funzione delle priorità che emergono dal quadro giuridico che si è tentato di tratteggiare.

Sulla scorta di queste osservazioni finali, non è da escludere che la nozione di «contenuto illegale» finisca per generare ulteriori paradossi, peraltro in seno al sistema UE di tutela dei diritti fondamentali. In particolare, si immagina che l'art. 11 della Carta, volto a tutelare tanto la libertà di espressione quanto la libertà di informazione, in combinazione con l'art. 10 della CEDU, non si limiti ad essere invocato quale prerogativa principale di chi, ai sensi del DSA, deve poter essere difeso dagli effetti dei contenuti illegali online (i destinatari del servizio); esso ben potrebbe essere fatto valere con forza uguale e contraria anche dagli attori preposti al raggiungimento di questo obiettivo primario (i prestatori del servizio, specie quelli assoggettati ad obblighi più rigidi) e dai soggetti che intendono far circolare le proprie idee attraverso le attività di tali operatori. Questa triangolazione di interessi potenzialmente confliggenti entro il campo d'azione dell'art. 11 della Carta potrebbe quindi costituire un nuovo banco di prova per la tenuta di una normativa rispetto alla quale il concetto di «contenuto illegale» è a dir poco cruciale.

DISINFORMAZIONE ED ECOSISTEMI DIGITALI: DAL PARADIGMA PUNITIVO ALLE ISTITUZIONI DI LIBERTÀ

Corrado Caruso

1. *In breve*

L'ascesa della disinformazione digitale induce a interrogarsi sulla idoneità del diritto penale ad arginare questo fenomeno e, per il costituzionalista, a chiedersi se il suo compito possa limitarsi a *giustificare*, alla luce dei molteplici valori costituzionali di cui è costellato l'ordinamento, un intervento repressivo orientato al *contenuto* o al *punto di vista*.

Per rispondere a questa domanda è necessario anzitutto esplorare le relazioni comunicative che hanno luogo all'interno delle piattaforme digitali, le quali favoriscono un processo comunicativo emozionale che polarizza gli utenti, intrappolati nelle rispettive bolle (par. 2). Il fenomeno della disinformazione, inteso come costante processo volontario di alterazione della corrispondenza tra i fatti e la loro descrizione, trova nell'ecosistema digitale il proprio *habitat* naturale: l'obiettivo non è tanto convincere l'uditorio della bontà di una certa tesi, come nei tradizionali meccanismi di propaganda, quanto assumere il *potere* di determinare la verità (par. 3). Di fronte a queste tendenze, non è opportuno riconoscere un *diritto alla verità* dall'incerto contenuto capace, in una paradossale eterogenesi dei fini, di funzionalizzare la stessa libertà di espressione ai fini del regime politico, ma è invece necessario assumere la verità su fatti di interesse pubblico quale ideale prescrittivo, «bene politico» di rango costituzionale, precondizione della libera dialettica democratica (par. 4).

Simili tendenze sollecitano il costituzionalista a un cambio di approccio metodologico: non è possibile analizzare l'impatto della disinformazione attraverso le antiche lenti dogmatiche della libertà negativa, che esprime un divieto di interferenza dello Stato nella sfera individuale. È necessario invece prendere atto del ruolo che le piattaforme digitali svolgono nella conformazione della autonomia individuale e, di riflesso, della

sfera pubblica per evocare la necessaria configurazione delle libertà come *istituzioni*, spazi sociali che richiedono un obbligo positivo di regolazione al fine di salvaguardare il contenuto di valore positivizzato dalle fattispecie costituzionali. Le situazioni di libertà connesse all'art. 21 Cost. individuano le coordinate del *discorso pubblico*, uno spazio istituzionale ove hanno luogo interazioni comunicative che, attraverso il conflitto tra opposte visioni del mondo, legittimano sul piano sostanziale i meccanismi procedurali del circuito democratico-rappresentativo. Per svolgere le sue funzioni, il discorso pubblico non può però essere ridotto a un magma indistinto di pulsioni emotive né può venire meno un grado minimo di corrispondenza tra la realtà e le sue, pur ideologicamente diverse, narrazioni. Se questa corrispondenza venisse meno, sarebbe impossibile la stessa la reciproca precomprensione tra cittadini e, quindi, la stessa convivenza democratica (par. 5).

Non si tratta di verificare sino a che punto la singola notizia falsa possa essere ricompresa nella sfera di protezione offerta dall'art. 21 Cost. Il diritto penale è teleologicamente e strutturalmente inidoneo ad arginare questo fenomeno: non solo per le *eccedenze autoritarie* che i reati di opinione portano con sé, ma anche per la sostanziale *ineffettività* di tale risposta nei confronti dei problemi sollevati dalla sfera pubblica digitale (par. 6).

Si tratta, viceversa, di predisporre un'impalcatura istituzionale che protegga l'apertura dei canali di formazione della sfera pubblica dai processi di privatizzazione e *self-closed fragmentation* realizzati dalle grandi *corporations* del Web. Il recente attivismo regolatorio dell'Unione europea deve essere collocato in questa cornice teorica: lungi dal concretizzare un intervento *orientato al contenuto* o al *punto di vista*, e cioè alla selezione contenutistica dei messaggi digitali, la disciplina europea impone procedure e obblighi di trasparenza che incidono sul modello infrastrutturale adottato dalle piattaforme (par. 7). La regolazione sovranazionale ha posto le premesse per una *double-track regulation*, che lascia agli Stati membri la definizione dei contenuti illegali e all'Unione le misure di regolazione delle "infrastrutture" digitali. Questa *istituzionalizzazione procedurale* della sfera pubblica, realizzato soprattutto dal *Digital Services Act*, ha condotto a nuove situazioni soggettive connesse alle dinamiche di governo degli ecosistemi digitali, tra le quali meritano menzione il diritto a un intervento proporzionato nella rimozione dei contenuti emessi in rete o il diritto a non subire sistemi di raccomandazioni basati sul *targeting* (par. 8).

Nonostante si tratti di un primo passo di cui sarà necessario valutare l'efficacia, il saggio saluta con favore l'intervento sovranazionale, che persevera nella strategia di un *federalizing process* condotto attraverso i valori del costituzionalismo liberaldemocratico e volto a preservare il discorso pubblico europeo dalle minacce che provengono dall'attuale quadro geopolitico (par. 9).

2. *I caratteri della sfera pubblica digitale: partecipazione, privatizzazione e frammentazione*

L'avvento di Internet amplifica tendenze in parte note: nella seconda metà del '900, l'irrompere del fattore tecnologico e dalla diffusione del sistema radiotelevisivo comporta una privatizzazione della sfera pubblica. Le tecnostrutture private hanno sovvertito l'orizzontalità della comunicazione a favore di processi mediatici verticali e unidirezionali, valorizzando l'intrattenimento a detrimento della informazione con il fine di aumentare gli introiti pubblicitari[1].

Gli albori del Web sembrano rafforzare questo processo di disintermediazione e di privatizzazione della sfera pubblica in forme nuove, coerenti con le peculiarità del mezzo di diffusione. Il Web ha favorito la nascita di relazioni sociologiche collocate nella cornice dello scambio di informazioni attraverso apparati tecnologici, dando origine a un sistema di «autocomunicazione di massa»[2], che apparentemente sostituisce le modalità comunicative tradizionali, contraddistinte da verticalità e unidirezionalità della comunicazione. Nella società digitale, emerge un processo di *soggettivazione* che marginalizza i «mediatori dell'interesse generale»[3] e la selezione specializzata delle notizie e dei fatti di interesse generale a favore di un processo di frammentazione e atomizzazione[4].

Superata la prima fase di sviluppo della Rete, e con, essa, la credenza ottimistica che Internet avrebbe condotto a una sorta di *agorà* globale caratterizzata dall'eguale partecipazione alla sfera pubblica e dalla orizzontalità della informazione, il Web è andato sviluppandosi grazie alla intermediazione delle piattaforme digitali: la loro disintermediazione cela in realtà una re-intermediazione, attraverso le loro modalità di funzionamento tecnico, delle comunicazioni in rete.

I dati lasciati dall'utente tra le maglie dei fornitori di servizi servono a questo scopo: queste tracce, che per quantità e varietà sono catalogate sotto l'etichetta di *big data*, diventano oggetto di trattamenti automatizzati mediante algoritmi informatici in grado di precostituire l'ecosistema digitale entro cui si trova ad agire l'utente. Le piattaforme non si limitano, dunque, a registrare e a trasmettere ma *processano* dati e informazioni attraverso strumenti di intelligenza artificiale[5]: lungi, dunque, dall'offrire un servizio passivo di mera intermediazione, esse contribuiscono a ordinare, selezionare e a rendere visibili i contenuti inseriti o trasmessi dagli utenti.

[1] Sui mutamenti della sfera pubblica, per tutti, J. HABERMAS, *Storia e critica dell'opinione pubblica*, Laterza, Roma-Bari, 2006.

[2] M. CASTELLS, *Comunicazione e potere*, UBE, Milano, 2009, XXI.

[3] Così C. SUNSTEIN, *#republic. La democrazia nell'epoca dei social media*, il Mulino, Bologna, 2017, p. 30.

[4] J. HABERMAS, *Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere*, in «Theory, Culture & Society», 39/4 (2022), pp. 153, 157.

[5] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, OUP, New York, 2014, ix.

Nella seconda fase di sviluppo del Web, le piattaforme digitali, situate in posizione oligopolistica, delineano quindi le infrastrutture economiche, tecniche e giuridiche entro cui si colloca l'azione dell'utente in rete. Il funzionamento tecnico è finalizzato, infatti, alla massimizzazione del profitto di queste grandi *corporations* che accumulano capitali attraverso il trattamento dei dati personali. Le *big tech* incarnano due nuove forme di capitalismo tra loro complementari: il capitalismo informativo[6], retto sul plusvalore economico delle informazioni immesse dall'utente, e quello della sorveglianza, ove il plusvalore è dato non solo dal materiale informativo grezzo ma anche, e soprattutto, dai *behavioral data*, che consentono di prevedere e orientare, attraverso il *targeting*, le scelte dell'utente nell'ecosistema digitale[7]. Accanto agli aspetti tecnici ed economici vi è poi quello giuridico: nel caso dei *social media*, ad esempio, l'utente intrattiene con le piattaforme digitali un rapporto contrattuale, caratterizzato dallo scambio di dati in cambio del servizio di comunicazione. Al momento della registrazione, l'utente si impegna a rispettare le condizioni generali d'uso unilateralmente delineate dal prestatore del servizio. Tra queste, particolare rilievo assumono gli standard che attengono al contenuto dei messaggi pubblicati, dal contenuto non perfettamente sovrapponibile agli illeciti previsti dall'ordinamento e che assicurano grande discrezionalità alla piattaforma sia sulla scelta di intervenire sia sul tipo di "sanzione" da comminare[8].

Anche questa tendenza è però destinata ad essere superata nella nuova fase che sta vivendo la Rete. Se, nella seconda fase cui si accennava poc'anzi, c'è una distinzione soggettiva tra l'organizzazione finalizzata al profitto delle *corporations* del Web e l'impresario politico che immette un certo flusso comunicativo, nel senso che gli attori politici si servono delle piattaforme per costruire consenso attorno ad alcuni temi, questa separazione viene ora meno. Alcuni esempi (Trump con *Truth*, Musk con *X*) mostrano come le modalità tecniche di funzionamento della piattaforma siano ormai al servizio di una certa linea politica: l'impresario politico e i suoi collaboratori definiscono le scelte editoriali della *propria* piattaforma, servendosi della sua struttura per costruire le proprie cause e amplificare il consenso attorno ad esse.

[6] J. Cohen, *Between Truth and Power. The Legal Construction of Informational Capitalism*, OUP, New York, 2019, p. 6.

[7] Cfr. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019, p. 64 ss.

[8] Per talune recenti vicende giurisdizionali che, con opposti esiti, hanno interessato la rimozione di contenuti e profili di Forza Nuova e Casa Pound da parte di Facebook e Twitter sia consentito il rinvio a C. Caruso, *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei social network*, in Liber Amicorum *per Pasquale Costanzo*, in «Consulta Online» (2020).

3. *La natura della disinformazione digitale*

Il ruolo giocato dalle piattaforme aiuta a comprendere il fenomeno della disinformazione digitale, che è possibile esplorare senza interrogarsi sui limiti filosofici della teoria della corrispondenza tra descrizione e realtà dei fatti.

Le teorie postmoderne[9] hanno messo in discussione la rigida distinzione tra soggetto narrante e oggetto narrato e, dunque, la pretesa di una univoca lettura dei fatti. In base a questi approcci, quanto meno nelle varianti più radicali, non sarebbe possibile definire una verità oggettiva: esisterebbero solo *prospettive soggettive*, visioni del mondo tra loro alternative e influenzate dal contesto e dai valori del soggetto narrante[10].

Queste posizioni hanno certamente contribuito al retroterra culturale della cd. «post-verità», ma non è necessario contestare i loro assunti per comprendere e valutare le attuali strategie di disinformazione. Con questo termine non si fa riferimento alla errata o discutibile ricostruzione di un certo fatto ma a flussi di informazioni clamorosamente false che assumono una *parvenza di verità* grazie all'enorme capacità diffusiva delle piattaforme digitali. I *mass-media* influenzano i comportamenti, il clima sociale[11] e financo la stessa *percezione* della verità: l'avvento della società di massa segna una mutazione della menzogna politica, intesa come negazione della corrispondenza tra i fatti rilevanti per la *polis* e la loro descrizione. Se «[l]a menzogna politica tradizionale […] riguardava […] segreti – dati che non erano mai stati resi pubblici – o […] intenzioni» di future condotte, le menzogne politiche contemporanee o postmoderne «si occupano efficacemente di cose che non sono affatto dei segreti, ma sono conosciute praticamente da tutti»[12].

Queste premesse aiutano a inquadrare la disinformazione digitale. Secondo la definizione offerta dal Gruppo di esperti nominato dalla Commissione europea[13] e rilanciato da quest'ultima nella sua comunicazione sul contrasto delle false informazioni online[14], la disinformazione consiste nella diffusione di una serie di notizie «rivelat[e]si fals[e] o fuorviant[i] concepit[e], presentat[e] e diffus[e] a scopo di lucro per ingannare intenzionalmente il pubblico, e che [possono] arrecare un pregiudizio pubblico. Il pregiudizio pubblico include minacce ai processi politici democratici e di elaborazione delle politiche e a beni pubblici quali la tutela della salute dei cittadini, dell'ambiente e della sicurezza dell'UE».

Questa definizione sconta una certa vaghezza contenutistica, tanto che il Gruppo di esperti e la Commissione si sono premurati di escludere dal concetto la satira e la

[9] Per tutti, J. LYOTARD, *La condizione postmoderna*, Feltrinelli, Milano, 2004.

[10] Per una panoramica, L. MCINTYRE, *Post-Truth*, MIT Press, Cambridge (MA), 2018, p. 124 ss.

[11] Secondo quanto intuito già da M. MCLUHAN, *Understanding Media: The Extensions of Man*, McGraw-Hill, New York, 1964.

[12] H. ARENDT, *Verità e politica*, Bollati Boringhieri, Torino, 1995, p. 64.

[13] European Commission, *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation* (2018).

[14] Commissione europea, *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236 final.

parodia, mentre resta incerta la possibilità di includere i fenomeni di *misinformation* e *malinformation*, pure ritenuti, dal report redatto per il Consiglio di Europa, tra i sintomi dell'attuale *information disorder*[15].

Questa vaghezza definitoria si spiega alla luce della strategia inaugurata dalle istituzioni europee con l'istituzione del Gruppo di esperti[16], volta a delineare *policies* poi confluite in diverse iniziative legislative (tra cui spicca, come si vedrà tra poco, il *Digital Services Act*). In altri termini, le iniziative dell'Unione non mirano a definire i confini della libertà di espressione o di informazione, a chiarire quali siano i contenuti illegali da perseguire (anzitutto) penalmente (compito che resta nelle mani degli Stati membri); le istituzioni dell'Unione prendono atto, piuttosto, dell'esistenza del fenomeno ed individuano le *best practices* necessarie a ripulire l'ecosistema digitale. Non a caso, nonostante la *misinformation* non fosse stata espressamente inclusa nella definizione originaria, la *infodemia* scoppiata contestualmente al Covid-19 ha portato le istituzioni europee a includere anche la diffusione in buona fede di notizie false (ad esempio, su possibili cure miracolose contro il virus) nella disinformazione idonea ad arrecare pregiudizi pubblici[17].

Sono quindi le modalità e le finalità di diffusione a dare pregnanza al concetto di disinformazione. A questo riguardo giocano un ruolo centrale gli strumenti di intelligenza artificiale (si pensi alla creazione di video o immagini finte, cd. *deep fakes*) e l'architettura algoritmica delle piattaforme: sono gli algoritmi infatti a definire, sulla base delle preferenze disseminate in rete dagli utenti, l'ordine di visualizzazione dei messaggi, privilegiando contenuti personalizzati e sensazionalistici[18]. Inoltre, i messaggi falsi o di bassa qualità, che spesso rimandano a siti sorgente di oscura gestione, sono collegati a messaggi pubblicitari che "monetizzano" la falsa informazione. Attraverso servizi automatizzati (*bot*) e falsi profili, magari orchestrati su vasta scala (cd. fabbriche di troll), questi messaggi diventano poi virali, rendendo credibile il contenuto degli stessi[19].

Per tale rargione, nella definizione del fenomeno assumono rilievo lo scopo o la finalità soggettiva della diffusione, il pregiudizio "pubblico" che si vuole arrecare[20] e le modalità di diffusione[21].

[15] Per *misinformation* si intende generalmente l'informazione falsa ma non creata per arrecare intenzionalmente un danno, mentre per *malinformation* una «informazione basata sulla realtà», ma diffusa per danneggiare una persona, un gruppo, o un Paese. Cfr. C. WARDLE, H. DERAKSHAN, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe report DGI(2017)09, p. 20.

[16] Il primo intervento in materia viene dalla Conclusioni del marzo 2015 dal Consiglio europeo con la richiesta, indirizzata all'Alto rappresentante per la politica estera, di reagire alla disinformazione russa. A seguito di tale indicazione, è stata creata la *East Strategic Communication Task Force*.

[17] *Commission Communication on the European democracy action plan*, COM/2020/790 final.

[18] Commissione europea, *Contrastare*, cit., 4.

[19] *Contrastare*, cit. ult., 6.

[20] E. BIETTI, O. POLLICINO, *Truth and deception across the Atlantic: a roadmap of disinformation in the US and Europe*, 11, in «Italian Journal of Public Law», 43 (2019), p. 45.

[21] Insistono su tale aspetto R.O. FATHAIGH, N. HELBERGER, N. APPELMAN, *The perils of legally defining disinformation*, in «Internet Policy Review», 10/4 (2021), p. 5.

Il fenomeno della disinformazione può essere inteso, allora, come costante processo volontario di alterazione digitale della realtà, finalizzato a incidere sulle dinamiche di governo della sfera pubblica: l'obiettivo non è tanto convincere l'uditorio della bontà di una certa tesi, come nei tradizionali meccanismi di propaganda, quanto assumere il *potere* di determinare la verità attraverso una realtà alternativa che influenzi le scelte delle persone[22]. Si avvera, dunque, quanto preconizzato da alcuni teorici del passato pure collocati su opposte posizioni culturali: la tecnologia cessa di essere fattore neutrale per diventare strumento diretto di influenza e controllo delle masse[23], l'«*a priori* tecnologico» diviene «*a priori* politico», trasformando «la base del dominio»[24]. Le modalità di creazione e diffusione digitale delineano un processo di de-umanizzazione del messaggio, con tecnologie algoritmiche che orientano il comportamento umano e definiscono l'agenda di discussione pubblica. Peraltro, il depauperamento, in termini di risorse e lettori, dei media tradizionali porta il giornalismo a un certo conformismo rispetto alle modalità di funzionamento delle piattaforme digitali: nella selezione delle notizie viene data preminenza ai contenuti sensazionalistici, che meglio si prestano alla viralità digitale, così da abbassare ulteriormente il livello qualitativo della sfera pubblica.

Le cascate informative portano ad atteggiamenti di emulazione in forza dei quali, di fronte alla diffusione massiva di un certo tipo di messaggi, gli utenti cessano di affidarsi alle precedenti convinzioni o informazioni, per seguire il flusso delle notizie diffuse dai propri contatti online soprattutto se, tra questi, vi è un legame affettivo o comunque una certa omofilia[25]. Emergono così vere e proprie camere dell'eco (*eco chamber*), che escludono in radice la possibilità di venire a contatto con idee, visioni del mondo o informazioni *alternative.* Queste *filter bubbles*, edificate grazie all'opaco algoritmo che seleziona i messaggi rilevanti per l'utente[26], favoriscono un processo comunicativo emozionale che polarizza gli utenti, intrappolati nei rispettivi bozzoli informativi. Si rafforza così una identificazione di tipo plebiscitario tra il soggetto da cui origina il flusso disinformativo e il gruppo cui il messaggio è rivolto[27]. L'orizzontalità della comunicazione, che pure caratterizzava la Rete degli esordi, viene ad essere smarrita a favore di un conflitto eterodiretto tra opposte, inconciliabili tifoserie che accentuano la *disruption* della sfera pubblica[28].

[22] L. McIntyre, L., *Post-truth*, The MIT Press, Cambridge (MA), 2018, p. 117.

[23] C. Schmitt, *Le categorie del politico*, il Mulino, Bologna, 1972, p. 179.

[24] H. Marcuse, *L'uomo a una dimensione. L'ideologia della società industriale avanzata*, Einaudi, Torino, 1968, p. 167, p. 158.

[25] C. Sunstein, *#republic*, cit., pp. 149 ss.

[26] E. Pariser, *The filter bubble: what the Internet is hiding from you*, Penguin Books, London, 2011.

[27] Sul cd. cd. *groupthink*, forma di psicologia sociale che rafforza le convinzioni di gruppi ideologicamente omogenei e il legame con il *leader* di riferimento, cfr. A. Nicita, *Il mercato delle verità. Come la disinformazione minaccia la democrazia*, il Mulino, Bologna, 2021, p. 99.

[28] J. Habermas, *Reflections*, cit., p. 159.

4. *La verità politica come bene costituzionale*

Non sono mancati i tentativi di relativizzare queste desolanti tendenze[29]. In parte perché, se analizzate in prospettiva storica, la frammentazione e la verticalizzazione della sfera pubblica sono in corso da tempo, almeno da quando la radiotelevisione ha assunto un ruolo centrale nella diffusione dell'informazione. Inoltre, è stato sostenuto come non sia possibile stabilire empiricamente una causalità diretta tra la diffusione della disinformazione e un determinato accadimento politico[30]. Anche la teoria della camera dell'eco è stata sottoposta a revisione critica: alcuni sociologi della comunicazione hanno evidenziato come, nell'ambito dei *social network*, i cd. *weak ties* (i "legami deboli", e cioè contatti che operano nei nostri ecosistemi digitali ma a noi affettivamente lontani) contribuiscono a portare alla nostra attenzione messaggi che interrompono l'uniformità contenutistica dell'ecosistema digitale[31]. Infine, nonostante il ruolo giocato dagli algoritmi nella costruzione degli ecosistemi digitali, è stato sottolineato il ruolo delle scelte dell'utente nella esclusione di certi contenuti dalla propria sfera di attenzione[32].

Ad alcune di queste obiezioni è però possibile rispondere. In primo luogo, è innegabile l'influenza delle infrastrutture tecnologiche sulla conformazione dell'identità digitale della persona e, dunque, sulla sua consapevole autodeterminazione: l'infosfera pone infatti una reciproca contaminazione tra le scelte della persona e la costruzione dell'ecosistema digitale. Inoltre, per quanto orientate al pluralismo ideologico, le nostre imperfette democrazie si reggono pur sempre «sulla ragionevole presunzione che l'apparenza corrisponda alla realtà»[33]. Il corretto esercizio delle libertà politiche dipende, in fondo, da una certa coincidenza tra i fatti e la loro descrizione: «il diritto dei cittadini di scegliere i propri governanti, la controllabilità del potere politico, la competizione tra i partiti per il potere di governo presuppongono che i singoli possano contare sulla corrispondenza al vero di quanto viene detto e fatto»[34]. Non si tratta di riconoscere un diritto soggettivo alla verità dall'incerto contenuto capace, in una paradossale eterogenesi dei fini, di funzionalizzare la stessa libertà di espressione ai fini del regime politico[35], ma di assumere la verità su fatti di interesse pubblico quale ideale

[29] Sottolineano tale aspetto N. ZANON, *Fake news e diffusione dei social media: abbiamo bisogno di un'"Autorità Pubblica della Verità"?*, in «MediaLaws», 1 (2018), pp. 12 ss., M. BASSINI, G. VIGEVANI, *Primi appunti su fake news e dintorni*, in «MediaLaws», 1 (2017), pp. 11 ss.

[30] Cfr. Y. BENKLER, R. FARIS, H. ROBERTS, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, OUP, New York, 2018, p. 341 ss., a proposito della Brexit e dell'elezione di Trump.

[31] In tal senso, P. BARBERÀ, *Social Media, Echo Chambers, and Political Polarization*, in N. PERSILY, J.A. TUCKER (a cura di), *Social Media and Democracy. The State of the Field, Prospects for Reform*, CUP, Cambridge, p. 41.

[32] M. MONTI, *Le Internet platforms, il discorso pubblico e la democrazia*, in «Quaderni costituzionali» (2019), p. 822.

[33] Così L. VIOLANTE, *Politica e menzogna*, Einaudi, Torino, p. 4, nello stesso senso F. PARUZZO, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, ESI, Napoli, 2022, p. 40.

[34] L. VIOLANTE, cit. ult., *ibidem*.

[35] Mette in guardia da tale pericolo A. PACE, *Mezzi di diffusione e comunicazione di massa*, in A. Pace, M. Manetti, *Articolo 21, Commentario della Costituzione, Rapporti civili (artt. 13-28)*, Zanichelli, Bologna-Roma, 2006, pp. 532-533.

prescrittivo, «bene politico»[36] di rango costituzionale, precondizione della libera dialettica democratica. Non è dunque necessario dimostrare una diretta causalità tra la massiccia diffusione del falso e un determinato accadimento politico: per giustificare una regolazione (non dei contenuti ma) dei canali di trasmissione della disinformazione è sufficiente il *tentativo* di inquinare la dialettica democratica.

La Costituzione offre le coordinate fondamentali per cogliere la necessità di una risposta istituzionale all'*information disorder*: i contesti materiali, insegna il principio personalista di cui all'art. 2 Cost., influenzano la soggettività e plasmano la personalità. Quando tali contesti traducono un rapporto di subordinazione sociale deve essere attivata l'azione dei pubblici poteri per realizzare il pieno sviluppo della persona umana (art. 3, secondo comma, Cost.). La persona, per dirla con i fautori del personalismo comunitario, «si oppone all'individuo in quanto ella è dominio, scelta, formazione, conquista di sé»[37].

A volgere l'attenzione al testo dell'art. 21 Cost., tuttavia, si trovano poche indicazioni sulle modalità di governo della sfera pubblica e sulla disciplina dei mezzi di diffusione del pensiero. Nonostante parte della dottrina abbia recentemente rivalutato le scelte compiute dai Costituenti[38], l'attuale formulazione dell'art. 21 Cost. denota una certa sottovalutazione rispetto ai meccanismi di formazione dell'opinione pubblica. La mancata menzione della libertà di informazione (come situazione soggettiva distinta rispetto al diritto di manifestazione del pensiero), del suo risvolto passivo (il diritto o l'interesse ad essere informato), l'assenza di un richiamo alla necessaria regolazione in senso pluralistico dei mezzi di informazione (se si esclude la scarna previsione sul regime di pubblicità delle fonti di finanziamento della stampa periodica) tradiscono un approccio culturale fortemente legato al periodo liberale, quando i diritti erano essenzialmente concepiti come libertà dallo Stato, dalle interferenze del potere pubblico nella sfera individuale[39].

5. *Ripensare il paradigma teorico: dalle libertà negative alle istituzioni di libertà*

La paratia del diritto soggettivo ben poco può fare di fronte alle dinamiche di funzionamento delle piattaforme digitali. Questi soggetti sono, infatti, veri e propri poteri privati in competizione col potere pubblico[40], che esprimono ordinamenti giuridici alternativi agli Stati-nazione, fondati sulla coincidenza tra ordinamento (*Ordnung*) e localizzazione territoriale (*Ortung*)[41]. Il pluralismo giuridico e la differenziazione so-

[36] F. D'Agostini, *Diritti aletici*, in «Biblioteca della libertà», LII, 218 (2017), pp. 8 ss.

[37] Così E. Mounier, *Rivoluzione personalista e comunitaria*, Edizioni di Comunità, Milano, 1955, p. 58.

[38] G.E. Vigevani, *Informazione e potere*, in M. Cartabia, M. Ruotolo (a cura di), *I Tematici, V - Potere e costituzione*, Giuffrè, Milano, 2023, p. 225.

[39] A. Barbera, *Articolo 2*, in G. Branca (a cura di), *Commentario della Costituzione. Artt. 1-12. Principi fondamentali*, Zanichelli, Bologna-Roma, 1975, p. 53.

[40] M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in «La Rivisita "Gruppo di Pisa"», 1 (2021), pp. 177 ss.

[41] C. Schmitt, *Il nomos della terra: nel diritto internazionale dello* Jus publicum Europaeum, Adelphi, Milano, p. 25.

ciale che caratterizzano la società globale, l'esistenza cioè di una pluralità di organizzazioni private che operano su scala transazionale secondo regole autonome, funzionali alla soddisfazione dei rispettivi interessi settoriali, hanno sollecitato la teorizzazione delle costituzioni civili o societarie[42], sistemi normativi sorti dall'incontro tra fonti di autonormazione di istituzioni globali private o para-pubbliche e decisioni para-giurisdizionali di soggetti impolitici (quali corpi arbitrali, comitati etici etc.).

Questa estroflessione del linguaggio e delle categorie del costituzionalismo cela uno slittamento di potere. Le *tech companies* avanzano pretese di sovranità: non solo operano costantemente oltre le frontiere nazionali ma esercitano funzioni tradizionalmente appannaggio della statualità (si pensi non solo al già citato controllo sui contenuti espressivi ma anche alle monete virtuali e, più in generale, alle frontiere artificiali del metaverso). La *lex digitalis*, ispirata all'efficientismo tecnico e modellata sugli interessi delle piattaforme, ha una dimensione teleologica autonoma, potenzialmente antagonista al valore della persona umana e alle modalità di funzionamento dei sistemi democratici. Questa conclusione non implica necessariamente un disinteresse delle piattaforme rispetto all'interesse generale della comunità politica (che i teorici del costituzionalismo sociale tendono a confinare al *sistema politico*, come sottosistema pariordinato e concorrente agli altri insiemi sociali). Ad esempio, all'indomani della pandemia Meta ha istituito un programma di *fact-cecking* indipendente, ha aggiornato le proprie condizioni d'uso per escludere dal discorso pubblico *fake news* sui vaccini, fino a istituire un *Board* particolarmente qualificato, indipendente dal management, incaricato di decidere sulla rimozione di contenuti controversi[43]. Si tratta però di sforzi che non sembrano correggere in profondità le modalità di funzionamento delle piattaforme digitali.

Non è sufficiente opporre a questo scenario il figurino dommatico della libertà di espressione come libertà negativa. Allo stesso modo, è insufficiente il paradigma della efficacia orizzontale dei diritti (cd. *Drittwirkung*), che non rinuncia all'ancoraggio ai diritti soggettivi e postula comunque una equiordinazione delle pretese in questione, lasciando alle valutazioni *case by case* dei giudici l'individuazione della situazione soggettiva prevalente[44]. I contenuti e i confini delle libertà sono sempre la variabile di un complessivo assetto istituzionale[45]: di fronte a poteri sociali collocati in posizioni dominanti, a strutture che, per dimensioni e capacità di azione, sono dotate di una *vis* conformativa delle situazioni individuali e dei processi collettivi di deliberazione

[42] G. Teubner, *La cultura del diritto nell'epoca della globalizzazione: l'emergere delle costituzioni civili*, Armando, Roma, pp. 105 ss.

[43] Cfr. E. Douek, *The Meta Oversight Board and the Empty Promise of Legitimacy*, in 37 «Harvard Journal of Law & Technology», 2 (2024), pp. 385 ss.

[44] Favorevoli a un simile approccio M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Aracne, Roma, 2019, pp. 191 ss., O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Hart, Oxford, 2021, p. 203.

[45] Così G. Amato, *Libertà (dir. cost.)*, in «Enc. dir.», vol. XXIV, Giuffrè, Milano, 1974, p. 277.

democratica, è inevitabile un'azione complessiva di riequilibrio all'interno delle stesse organizzazioni che ospitano le interazioni comunicative.

Nella progressiva cattura dell'individuo e delle sue prerogative da parte di organizzazioni private orientate allo sfruttamento o comunque alla subordinazione della persona, la libertà diviene sinonimo di un'istanza di liberazione dai rapporti di dominio che innervano la società[46]. Il principio personalista illumina i diritti fondamentali previsti dalla Costituzione, i quali non hanno più soltanto una «funzione soggettivo-individuale di garanzia del cittadino contro lo Stato, ma svolgono anche una funzione oggettivo-istituzionale di integrazione […] nel sistema sociale, e […] si qualificano come diritti di partecipazione ai processi della produzione sociale (materiale e culturale)»[47].

Risulta, quindi, necessario, «utilizzare come peculiari schemi conoscitivi più istituti di libertà che diritti di libertà […] in un quadro complessivo che veda il cittadino rivendicare […] "contropoteri" […] e il potere pubblico correlativamente "promuovere" oltre che "garantire libertà"»[48].

Le istituzioni di libertà prendono atto del rilievo dei contesti, dei nuovi equilibri di potere e degli spazi sociali da cui emergono nuovi diritti o rinnovate minacce verso la persona, richiedendo un obbligo positivo di regolazione al fine di salvaguardare il contenuto di valore positivizzato dalle singole previsioni costituzionali.

Non ha torto chi critica alcune vetuste categorie e presupposti del costituzionalismo liberale: la teoria delle libertà negative presupponeva in fondo una rigida separazione tra Stato e società, non più coerente con l'effervescenza del pluralismo sociale del tempo presente[49]. L'insieme di principi e valori codificati nella nostra Carta fondamentale spingono però a ripensare quel modello, a superare l'individualismo a favore del personalismo e l'astensionismo del potere pubblico a favore dell'interventismo democratico. Il costituzionalismo non mira esclusivamente alla stabilizzazione normativa, non esprime un insieme di valori o regole riflessivi, chiamati appunto a registrare un dato equilibrio sociale; manifesta piuttosto un'esigenza di *trasformazione* politica, di correzione degli squilibri esistenti nei diversi contesti di formazione della personalità[50].

È necessario dunque orientare l'azione istituzionale verso una adeguata *politica delle libertà* che individui le migliori *policies* in vista dello sviluppo dei valori codificati dalla Costituzione.

[46] In tal senso già A. Barbera, *Articolo 2*, in G. Branca, *Commentario della Costituzione. Artt. 1-12. Principi fondamentali*, Zanichelli, Bologna-Roma, 1975, pp. 65 ss., più recentemente P. Pettit, *Il repubblicanesimo. Una teoria della libertà e del governo*, Feltrinelli, Milano, 2000, p. 27 ss.

[47] Così L. Mengoni, *Ermeneutica e dogmatica giuridica*, Giuffrè, Milano, 1996, p. 74.

[48] A. Barbera, *Articolo 2*, cit., p. 76.

[49] Cfr. A. Golia jr., *The Critique of Digital Constitutionalism*, in «Max Planck Institute for Comparative Public Law & International Law (MPIL), Research Paper», 13 (2022).

[50] In senso simile v. A. Morrone, *Costituzione*, in C. Caruso, C. Valentini (a cura di), *Grammatica del costituzionalismo*, il Mulino, Bologna, p. 42.

La politica delle libertà è inevitabile laddove il testo della Costituzione non sia aggiornato alle evoluzioni sociali e tecnologiche, quando è necessario riallineare, in altri termini, i precetti costituzionali al sistema sociale. Simile dinamica ha in fondo caratterizzato il processo di istituzionalizzazione della libertà di informazione, formula riassuntiva di una serie di principi e situazioni soggettive che mirano a salvaguardare l'obiettività e l'apertura pluralistica della sfera pubblica. Con riguardo al sistema radiotelevisivo, ad esempio, il riconoscimento della libertà di informazione ha richiesto l'inveramento dei noti principi del *pluralismo esterno*, inteso come necessaria presenza di una pluralità di soggetti attivi sul mercato, e del *pluralismo interno*, concepito come pluralità di punti di vista, equidistanza e obiettività all'interno del mezzo[51].

L'abbandono di una teoria atomistica della libertà di espressione porta dunque a dare rilievo a tutti quei principi e a quei diritti, pretensivi o oppositivi (libertà di stampa, pluralismo informativo, apertura concorrenziale del mercato dell'informazione, trasparenza nelle fonti di finanziamento dei mass media, diritto di cronaca, valorizzazione di una informazione obiettiva etc.), che consentono l'inveramento del *discorso pubblico*, di uno spazio istituzionale aperto ad interazioni comunicative che, attraverso il conflitto tra opposte visioni del mondo, legittimano, sul piano sostanziale, i meccanismi procedurali del circuito democratico-rappresentativo[52]. Nell'ambito di un ordine sociale differenziato, caratterizzato da una pluralità di sottosistemi[53], il discorso pubblico sublima i valori presupposti dall'art. 21 (autonomia, partecipazione, pluralismo) e li protegge dall'azione, teleologicamente orientata, di sottosistemi concorrenti (l'autorità pubblica che agisce in funzione della propria autocoservazione, le comunità culturali che ambiscono alla tutela della propria identità collettiva, le tecnostrutture private orientate alla massimizzazione del profitto).

Per svolgere la funzione di legittimazione democratica ed evitare la sua diluizione a un magma indistinto di pulsioni emotive, il discorso pubblico deve avere un livello qualitativo minimo, che consenta l'autodeterminazione e la reciproca comprensione politica dei partecipanti intorno ad alcuni elementi discorsivi essenziali.

Se la teoria della sfera pubblica descrive, sul piano sociologico, le funzioni di intermediazione che questa ha storicamente svolto tra Stato e società, la teoria del discorso pubblico rimanda, sul piano prescrittivo, alle condizioni che l'ordinamento deve soddisfare per salvaguardare la sfera pubblica dai processi di privatizzazione, *self-closed fragmentation* e inquinamento dell'informazione favoriti dalle grandi *corporations* del web.

[51] Per un *excursus*, M. MANETTI, *Freedom of Speech and the Regulation of Fake News*, in M. Graziadei, M. Torsello (a cura di), *Italian National Reports to the XXIst International Congress of Comparative Law* - Asunción 2022, ESI, Napoli, pp. 433 ss.

[52] Sia consentito il rinvio a C. CARUSO, *La libertà di espressione in azione. Contributo a una teoria costituzionale del* discorso pubblico, BUP, Bologna, pp. 157 ss.

[53] N. LUHMANN, *I diritti fondamentali come istituzione*, Dedalo, Bari, 2002, p. 47, p. 56.

6. *Correggere la disinformazione:* game over *per il diritto penale?*

In questo scenario, auspicare l'intervento del diritto penale per ripulire l'ecosistema digitale rischia di risultare problematico sotto il profilo della tutela di cui all'art. 21 Cost. e ineffettivo, incapace cioè di arginare il fenomeno della *digital pollution*[54].

Sotto il primo profilo, vi sono già, nella trama dell'ordinamento italiano, limitazioni penalistiche che colpiscono il *contenuto* espressivo[55] o il *punto di vista*[56], assecondando una selezione eterodeterminata delle opinioni capace di arretrare la soglia di punibilità sino a incriminare le scelte di valore dell'individuo e, dunque, la sua libertà ideologica. Molte di tali fattispecie sollevano dubbi di compatibilità con la Costituzione. Se, infatti, il discorso pubblico crea le premesse per una identificazione condivisa dei cittadini, esso postula una sostanziale neutralità legislativa, una «astinenza epistemica» e «neutralità valutativa» della autorità pubblica[57] in ordine al *tipo* di opinione in questione. L'art. 21 Cost. richiede l'ammissione, nel discorso pubblico, non solo delle manifestazioni verbali che *meritano* di essere riferite per la loro intrinseca qualità o perché servono un qualche ideale di giustizia, ma anche delle opinioni irriverenti dell'uomo della strada, delle idee politicamente scorrette del dissenziente, della moralità, banale ed esecrabile, dell'intollerante. Per tale ragione possono dirsi di dubbia costituzionalità quelle fattispecie che, difettando di materialità, aprono le porte all'incriminazione ideologica e agli incerti lidi del diritto penale d'autore.

Tali considerazioni valgono, almeno in parte, anche per la repressione delle false informazioni[58], fattispecie che sono state ritenute in dottrina non contrastanti con l'art. 21 Cost., là ove puniscono il soggettivamente falso idoneo a ledere beni giuridici di rango costituzionale[59].

Tra queste però non supera il vaglio di costituzionalità il discusso reato di cui all'art. 656 c.p., che punisce a titolo contravvenzionale la diffusione di notizie false, esagerate e tendenziose. Tale norma è stata faticosamente salvata dalla Corte costituzionale grazie a una concezione eticizzante di ordine pubblico, bene giuridico che riproduce «l'ordine istituzionale vigente», diretto alla «preservazione delle strutture giuridiche della

[54] A queste conclusioni giunge anche T. GUERINI, Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Torino, Napoli, 2020, pp. 202 ss., che evoca invece il paradigma regolatorio tedesco, per certi versi anticipatorio dell'intervento sovranazionale.

[55] Ad esempio, una limitazione per contenuto sono quelle di cui all'art. 414 c.p. (apologie di delitto e istigazione a delinquere) o all'art. 656 c.p., che punisce la diffusione di notizie false, esagerate e tendenziose.

[56] Si pensi a quanto previsto dall'art. 415 c.p. che punisce l'istigazione all'odio tra classi sociali.

[57] Così C. VISCONTI*, Aspetti penalistici del discorso pubblico*, Giappichelli, Torino, 2008, p. 247.

[58] Per una panoramica delle fattispecie v. T. GUERINI, Fake news *e diritto penale*, cit., pp. 97 ss. All'elenco riportato dall'A. si possono aggiungere anche i reati di truffa, aggiotaggio e manipolazione del mercato.

[59] Cfr. P. BARILE, *Diritti dell'uomo e libertà fondamentali*, il Mulino, Bologna, 1984, nonché A. PACE, *Delimitazione della garanzia costituzionale: esclusione del 'subiettivamente' falso. Ancora sul fondamento e sui limiti del c.d. diritto di mentire come aspetto del diritto di difendersi in giudizio*, in A. Pace, M. Manetti, *Commentario della Costituzione. Art. 21. Rapporti civili. La libertà di manifestazione del proprio pensiero*, Zanichelli, Bologna, 2006, pp. 89-90.

convivenza sociale»[60]. Come si è cercato di sostenere altrove, non è però sufficiente, al fine di comprimere la libertà di espressione, individuare beni giuridici in astratto idonei a tale scopo. Tale ricerca, piuttosto agevole in un testo costituzionale orientato ad una spiccata poliarchia assiologica, tradisce un errore metodologico fondamentale: la Costituzione non è un prontuario di valori, allineati e auto-evidenti, che l'interprete può selezionare per giustificare, a mo' di *conversation stopper*, la limitazione penalistica di fattispecie libertà. Sarebbe alto il rischio di sovvertire il rapporto tra la *regola* del riconoscimento della libertà e l'*eccezione* della sua limitazione o, per dirla altrimenti, rovesciare la presunzione di illegittimità di misure ispirate a una *ratio* diversa da quella del buon costume, unico limite esplicitamente ammesso dalla Costituzione[61]. A maggior ragione di fronte a fattispecie penali che lambiscono la libertà di espressione, il richiamo a «beni di rango costituzionale sempre e comunque opponibili» al diritto soggettivo rischia di «annichilire la libertà di pensiero, dato che la rete degli interessi costituzionalmente rilevanti copre una gran parte dei rapporti giuridici intrecciabili nel nostro ordinamento»[62].

D'altro canto, l'intervento del diritto penale sarebbe verosimilmente ineffettivo, incapace cioè di ergere una adeguata linea di resistenza nei confronti delle campagne disinformazione proprio per le caratteristiche, già evidenziate, di tale fenomeno. Dietro alla disinformazione digitale non si nasconde solo una *singola* notizia inattendibile, ma una serie di falsità diffuse capillarmente allo scopo di incidere sui processi di decisione politica. Nella viralità di tale fenomeno, gioca poi un ruolo fondamentale l'elemento tecnico, basato sull'algoritmo e su strumenti di intelligenza artificiale, che rende difficilmente esperibile una imputazione di responsabilità penalistica. Infine, a meno di non immaginare un modello di imputazione per le piattaforme costruito su quello della stampa periodica, comunque difficilmente realizzabile, non va dimenticato che la disinformazione digitale è un fenomeno transnazionale, che spesso sottende pressioni e conflitti geopolitici e, in quanto tale, sfugge dagli argini e dalle paratie erette dagli strumenti giuridici interni.

[60] Cfr. Corte cost., sent. n. 19/1962 (poi confermata dalle successive sentt. nn. 199/1972, 210/1976). Ad avviso della Corte, le notizie false, esagerate e tendenziose costituiscono «una forma di endiadi» che riguarda «ogni specie di notizie che, in qualche modo, rappresentino la realtà in modo alterato», idonee per ciò stesso a turbare l'ordine pubblico.

[61] Così C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, in ID., *Diritto costituzionale vivente: Capo dello Stato ed altri saggi*, Giuffrè, Milano, 1992, p. 136, ID., *La libertà di manifestazione del pensiero e l'ordine pubblico*, in «Giur. cost.» (1962), p. 194.

[62] Come già osservava L. PALADIN, *Libertà di pensiero e libertà di informazione: le problematiche attuali*, in «Quad. cost.» (1987), p. 11. Per l'idea che la teoria dei diritti fondamentali, e della libertà di espressione in particolare, non possa essere ridotta a una questione di bilanciamento, sia consentito il rinvio a C. CARUSO, *La libertà di espressione in azione*, cit.

7. *La lotta per la sovranità digitale europea*

Di fronte a imprese che operano in via autoritativa sul piano transazionale è perciò inevitabile un'azione più ampia, che apra ai valori costituzionali i sistemi autopoietici digitali. Nel contesto europeo, questa sfida richiede un doppio binario che lasci a livello nazionale la determinazione dell'illiceità dei contenuti e all'azione sovranazionale la sfida per la sovranità digitale.

È questa in fondo la strategia dell'Unione europea enunciata a più riprese dalla Commissione Von der Leyen[63]: per quanto il concetto di sovranità applicata ai contesti digitali incontri rilevanti incertezze semantiche, rimandando ora alla sovranità *del* digitale, e cioè al potere delle *tech companies* sulla società, ora alla sovranità *sul* digitale, e cioè alla supremazia del potere politico sulle infrastrutture digitali[64], è quest'ultima l'accezione da preferire: la sovranità digitale allude all'imposizione di forme di controllo e influenza sulla responsabilità e sul potere organizzativo delle *tech corporations*[65].

L'Unione europea ha dunque arricchito l'approccio iniziale fondato su *soft law*[66] e autoregolazione, che ha portato alla sottoscrizione, da parte di piattaforme digitali e associazioni di inserzionisti, di un apposito codice[67], all'istituzione di un osservatorio sui media digitali incaricato di mappare, con l'aiuto di *fact checkers organizations* le strategie di disinformazione online[68] e all'adozione di un Piano di azione volto a rafforzare la sinergia delle istituzioni europee in vista, in particolare, delle elezioni del Parlamento europeo[69].

Il codice ha impegnato i sottoscrittori ad assumere comportamenti e *policies* che potessero contrastare questo fenomeno. In particolare, esso impegnava le piattaforme a ridurre le entrate provenienti da inserzionisti che perseguono strategie di disinformazione; a incrementare la trasparenza sul finanziamento dei messaggi politici e *issue based*; a intensificare gli sforzi di rimozione di falsi *account*; a investire in strumenti tecnologici che dessero priorità, nelle ricerche o nella esposizione dei messaggi, a informazioni «rilevanti, autentiche, accurate e autorevoli»; ad assicurare maggiore trasparenza sulle ragioni di un eventuale targeting degli utenti da parte del *political advertising*[70].

Nonostante il codice abbia dato qualche esito positivo[71], la mancata uniformità di alcune definizioni, l'assenza, tra i sottoscrittori, di rilevanti associazioni di inserzionisti e di *fact-checker organizations*, la carenza di criteri e indicatori idonei a misurare

[63] V. in particolare il discorso sullo Stato dell'Unione (2020).

[64] G. Finocchiaro, *La sovranità digitale*, in «Dir. pubbl.» (2022), p. 811.

[65] In questo senso, L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in «Philosophy & Technology», 33 (2020), p. 371.

[66] V. la già citata comunicazione COM(2018) 236 final.

[67] *EU Code of Practice on Disinformation* (2018).

[68] *European Digital Media Observatory*, istituito il 1° giugno 2020.

[69] *Action Plan against Disinformation* JOIN(2018) 36 final.

[70] *EU Code of Practice on Disinformation*, cit., 3-4.

[71] *Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement*, SWD (2020) 180 final. Significativo, ad esempio, il dato dei profili falsi silenziati grazie a strumenti di intelligenza artificiale.

la *performance* delle piattaforme digitali, hanno indotto la Commissione ad adottare nuove linee guida[72] che hanno portato a una versione rafforzata del codice[73]. Questo promuove sforzi definitori (ad esempio in tema di *political and issue based acts*, rinviando alla proposta di regolamento europeo sul *political advertisement*), allarga la platea dei sottoscrittori (coinvolgendo *fact checking oganizations* e altre associazioni di inserzionisti) e individua indicatori quantitativi (*Service Level Indicators*) e qualitativi (*Qualitative Reporting Elements*) capaci di guidare la Commissione nel monitoraggio delle azioni intraprese dalle piattaforme (Pollicino 2023a, 1063).

La novità più importante del codice sta però nel contesto della sua adozione, nei suoi riferimenti al *Digital Services Act* (DSA) entrato in vigore poche settimane dopo[74].

Con tale regolamento, l'Unione europea ha preso atto dell'insufficienza dell'autoregolazione ed ha sposato una strategia di co-regolazione, volta ad offrire la cornice normativa entro cui collocare i codici di condotta. Si tratta di una prospettiva radicalmente diversa, che ha visto tramontare l'approccio libertario dei primi interventi normativi finalizzati a consentire la nascita e lo sviluppo dei servizi digitali (si pensi alla dir. 2000/31/CE).

Questa rinnovata strategia, formalmente diretta alla integrazione e allo sviluppo competitivo dei mercati digitali, mira nella sostanza a promuovere diritti e valori riconosciuti dalla Carta dei diritti fondamentali e provenienti dalle tradizionali costituzionali comuni, secondo una tendenza che ha portato parte della dottrina a considerare tali riforme espressione di un rinnovato costituzionalismo digitale[75].

Il primo esempio di tale approccio può essere rinvenuto nel GDPR, cui hanno fatto seguito la direttiva sul diritto d'autore[76] e, più recentemente, il DSA. Accanto ad essi si colloca il *Digital Market Act* (DMA)[77], che qualifica espressamente le piattaforme digitali come *gatekeepers*, secondo una terminologia che, nel diritto *antitrust*, sta a indicare detentori di potere di mercato capaci di controllare l'accesso a una data infrastruttura ingenerando dipendenza economica negli altri operatori[78]. Tale regolamento non mira tanto a disciplinare il discorso pubblico digitale, quanto ad evitare pratiche concorrenziali sleali nei confronti di utenti finali e/o commerciali dalle imprese che, in virtù della posizione oligopolistica, rendono non contendibile la loro situazione di mercato[79].

[72] *Guidance on Strengthening the Code of Practice on Disinformation*, COM(2021) 262 final.

[73] *The Strengthened Code of Practice on Disinformation* (2022).

[74] Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali, di modifica della direttiva 2000/31CE (regolamento sui servizi digitali).

[75] In questi termini, G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, CUP, Cambridge, 2022, pp. 38 ss., M. Monti, *Regolazione del discorso pubblico online e processi costituzionali di integrazione. Una comparazione UE e USA*, Editoriale Scientifica, Napoli, 2025, pp. 233 ss.

[76] Dir. (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

[77] Reg. (UE) 2022/1925.

[78] Così G. Tiberi, *L'irresistibile ascesa della sovranità digitale europea*, in Ferri, G. (a cura di), *Diritto e nuove tecnologie*, ESI, Napoli, 2022, pp. 131-132.

[79] La qualifica di *gatekeepers* viene data dalla Commissione sulla base di una serie di parametri qualitativi e quantitativi stabiliti dall'art. 1 del DMA.

8. *Il* Digital Services Act *come paradigma*

Se il DMA si preoccupa di ristabilire obblighi di *fairness* e competitività all'interno dei mercati digitali, il DSA tenta di correggere la frammentazione della sfera pubblica, amplificando la trasparenza e tentando di correggere la posizione di subalternità dell'utente. Per la prima volta, infatti, vengono riconosciuti «rischi sistemici» legati ai servizi di intermediazione delle *tech corporations*. Se, per un verso, viene confermata la esenzione di responsabilità in relazione ai contenuti[80], per altro verso il regolamento individua obblighi e procedure volti a mitigare questi rischi sistemici. Alcune soluzioni sono di carattere generale, applicabili a tutte le piattaforme, altre sono rivolte alle *very large online platforms* (VLOP), individuate dalla Commissione sulla base di criteri essenzialmente quantitativi[81].

Quanto alle procedure di carattere generale, va ricordato il meccanismo di segnalazione e azione, nel caso di individuazione di un contenuto illegale. Il DSA ripartisce gli oneri della procedura tra utente e piattaforma: individua gli elementi e le informazioni che il primo deve inserire nella richiesta; definisce un ordine di priorità delle segnalazioni, dando precedenza alle richieste provenienti dai «segnalatori attendibili» previamente certificati[82]; impone alle seconde un obbligo di motivazione per le eventuali restrizioni specificando il tipo di sanzione applicabile (rimozione del contenuto, disattivazione dell'accesso etc.) alla luce dei fatti a sostegno della decisione[83], così come la predisposizione di un sistema di gestione interno dei reclami; infine, ammette la possibilità di rimettere eventuali controversie a organismi extragiudiziali di risoluzione delle controversie appositamente certificati, rimedio da affiancare agli ordinari ricorsi giurisdizionali[84].

Il DSA pone le premesse per una *digital process of law*, pensata per disinnescare i conflitti tra utenti e piattaforme ed evitare *chilling effects* su contenuti tutelati dalla libertà di espressione. Individua inoltre una serie di obblighi volti a ridisegnare gli ecosistemi digitali, nel tentativo di limitare il potere di influenza delle piattaforme sull'autodeterminazione individuale. È stato così introdotto l'obbligo di progettare, organizzare e gestire interfacce online in modo da non ingannare e manipolare i destinatari dei servizi, affinché questi prendano «decisioni libere e informate». Alla progettazione e gestione dell'interfaccia sono connessi alcuni obblighi di trasparenza, tra cui la necessità di esplicitare i parametri utilizzati nei sistemi di raccomandazione (con contestuale diritto dell'utente di modificare detti parametri) e di indicare in maniera

[80] Cfr. artt. 4-8, reg. 2022/2065.

[81] Cfr. art. 33 DSA. Il 25 aprile la Commissione ha emesso un comunicato stampa che reca l'elenco delle VLOP: *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*.

[82] Cfr., rispettivamente, artt. 16 e 22 DSA.

[83] Art. 17 DSA. L'art. 23 prevede poi la sospensione dal servizio gli utenti che con frequenza forniscono contenuti manifestamente illegali, così come la sospensione dal potere di segnalazione per i soggetti che, con altrettanta frequenza, presentano segnalazioni manifestamente infondate.

[84] Art. 21 DSA.

«inequivocabile» quando un contenuto suggerito sia da considerare pubblicità, oltre ai committenti e ai soggetti sponsorizzati dall'avviso commerciale[85].

Questo quadro generale deve poi essere integrato con le specifiche previsioni dedicate alle VLOP, cui spetta l'individuazione e l'analisi di rischi sistemici (*risk assesment*), tra cui vengono annoverati gli eventuali pericoli ai diritti della persona, ai «processi democratici, [al] dibattito civico e [ai] processi elettorali, nonché [a]lla sicurezza pubblica» anche a causa di «campagne di disinformazione»[86]. Questi rischi devono essere mitigati (*risk mitigation*) attraverso una serie di azioni volte a incidere sulla presentazione e la diffusione dei contenuti, tra cui particolare rilievo assume la necessità di contrassegnare i cd. *deep fakes*[87]. Inoltre, in coerenza con quanto previsto dal GDPR, è riconosciuto un vero e proprio diritto a un sistema di raccomandazione non basato sulla profilazione[88] e ulteriori obblighi di trasparenza sulla pubblicità online[89].

Agli obblighi di *due diligence* previsti dall'art. 41, si affianca poi una vera e proprio norma di chiusura che riconosce alla Commissione il potere di imporre o suggerire «misure specifiche, efficaci e proporzionate» quando «circostanze eccezionali comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione»[90].

Non vi è dubbio che tale assetto pone le premesse per un regime di *responsabilità condizionata* a carico delle piattaforme. A tal fine, il DSA individua anche i soggetti incaricati alla vigilanza e alla comminazione delle sanzioni, delineando un sistema a raggiera: i poteri di vigilanza e sanzione sono perciò affidati agli Stati membri e ai rispettivi coordinatori dei servizi digitali (l'autorità a tale scopo individuata dai singoli Stati) per ciò che concerne il rispetto degli obblighi applicabili alla generalità delle piattaforme. La Commissione è invece titolare esclusiva di tali prerogative in relazione agli obblighi più rilevanti a carico delle VLOP (*risk assessement*, *risk mitigation*, ulteriori oneri di trasparenza per la pubblicità online, sistemi di raccomandazione non basati sulla profilazione)[91]. Il coordinamento tra questi due livelli è assicurato dal comitato europeo per i servizi digitali, composto dai coordinatori nazionali e presieduto dalla Commissione[92].

Il DSA non rappresenta un intervento isolato: prima che lo stesso regolamento fosse adottato, l'Unione si è preoccupata di ristabilire un riequilibrio (una sorta di pluralismo esterno) tra piattaforme digitali e media tradizionali. In effetti, una delle caratteristiche del capitalismo digitale dell'informazione è il progressivo depauperamento della stampa a causa della diffusione dei suoi contenuti, estrapolati dagli utenti e condivisi all'interno delle piattaforme.

[85] Cfr. artt. 27 e 26.

[86] Cfr. art. 34, Considerando (82) (83) DSA.

[87] Art. 35 (1), lett. k).

[88] Art. 38 DSA.

[89] Art. 39 DSA.

[90] Art. 36 DSA. A questa disposizione si aggiunge quanto previsto dall'art. 48, che prevede la possibilità di elaborare appositi protocolli di crisi sottoscritti dalla Commissione e dalle piattaforme.

[91] Cfr. art. 56 DSA.

[92] Art. 61 DSA.

Per tale ragione, il regolamento europeo sul diritto d'autore ha previsto una disposizione, ora inserita nell'art. 43-*bis* della l. n. 633/1941, che prevede un equo compenso, a favore delle imprese editoriali e degli autori, per i contenuti giornalistici utilizzati e diffusi dai «prestatori di servizi della società dell'informazione»[93].

Non solo: la necessità di un consentire un riequilibrio qualitativo della sfera pubblica europea passa anche dalla *Legge europea per la libertà di media*, che assicura il diritto di ricevere «una pluralità di notizie […] a beneficio del dibattito pubblico», la libertà editoriale dei media, le modalità di nomina e le garanzie a tutela dell'indipendenza dei vertici del servizio pubblico, obblighi di trasparenza e l'istituzione del comitato europeo per i servizi di media composto dalle autorità garanti dei singoli stati membri[94].

9. *Verso il discorso pubblico europeo*

Simile quadro normativo è destinato ad assumere un'importanza fondamentale per la sfera pubblica digitale e, di conseguenza, per il discorso pubblico europeo. Rispetto al capitalismo dell'informazione, e alla necessaria ridistribuzione delle risorse finanziare che simile accumulazione richiede, ancora molto vi è da fare[95].

Non mancano poi incertezze: quanto alla riuscita del DSA, molto dipenderà dal suo *enforcement* sia a livello statale sia a livello europeo. Non vi è dubbio, infatti, che l'obiettivo di uniformare la regolazione dei servizi digitali, indicato nel considerando (4) del regolamento, può essere messo in pericolo dalla stessa scelta del "doppio binario" regolatorio, che lascia alle legislazioni nazionali l'individuazione dei contenuti illegali. L'Unione ha però mostrato di prendere sul serio la propria regolazione, aprendo recentemente due distinti procedimenti sanzionatori nei confronti di *Tik Tok*: il primo in relazione ai sistemi di raccomandazione e di trasparenza sul finanziamento dei messaggi elettorali in vista del primo turno delle elezioni presidenziali rumene[96]; il secondo, più generale, con riferimento alla mancata istituzione, richiesta dal DSA, di un *repository* concernenti le informazioni relative ai committenti e al finanziamento degli avvisi pubblicitari[97].

Le misure adottate, alle quale deve essere aggiunto il regolamento relativo alla trasparenza e al targeting della pubblicità politica[98], rappresentano un primo passo per una regolazione del discorso pubblico coerente con i valori europei. Di fronte ai nuovi

[93] Cfr. anche il regolamento attuativo dell'AGCOM di cui alla delibera n. 3/23/CONS, che ha stabilito i criteri per la determinazione del compenso.

[94] Cfr. Reg. (UE) 2024/1083.

[95] Per alcune proposte, A. Jr Golia, *The Critique of Digital Constitutionalism*, in «Max Planck Institute for Comparative Public Law & International Law (MPIL), Research Paper», pp. 21 ss.

[96] Cfr. il comunicato stampa della Commissione europea, 17 dicembre 2024.

[97] Cfr. il comunicato stampa della Commissione europea, 15 maggio 2025.

[98] Reg. (UE) 2024/900.

contesti digitali, che conformano i diritti e inquinano il discorso pubblico europeo, le misure europee tentano di limitare la discrezionalità delle piattaforme nella regolazione dei contenuti e nella costruzione dell'ecosistema digitale. Attraverso l'imposizione di nuovi obblighi e l'introduzione di articolate procedure, nuovi diritti vengono riconosciuti e istituzionalizzati (si pensi al diritto a un intervento proporzionato nella rimozione dei contenuti o al diritto a non subire sistemi di raccomandazioni basati sul *targeting*). Questa opera di istituzionalizzazione procedurale della sfera pubblica, fondata sull'azione congiunta di Unione e Stati membri, non solo pone le premesse per una integrazione attraverso i valori[99], ma definisce anche un discorso pubblico europeo orientato ai diritti e al pluralismo, alternativo, nello scenario geopolitico globale, sia ai paradigmi autoritari del modello cinese sia al *laissez faire* dell'approccio statunitense[100].

La vicenda delle sanzioni contro Russia Today[101] dimostra come la posta in gioco, in Europa, sia più ampia della semplice protezione della libertà di espressione dagli abusi del pubblico potere: a rischio, infatti, in un quadro geopolitico minacciato da nuovi e vecchi autoritarismi, è la salvaguarda del discorso pubblico da manipolazioni, interferenze e minacce ibride che incombono sulla democrazia europea.

[99] Così G. Pitruzzella, *Identità, linguaggio e integrazione europea*, in «Rivista AIC», 1, pp. 107 ss.

[100] Per i diversi modelli regolatore adottati dai grandi players *globali* v. A. Bradford, *Digital Empires. The Global Battle to Regulate Technology*, OUP, New York, 2023 nonché, con specifico riferimento agli USA, M. Monti, *Regolazione del discorso pubblico online*, cit., pp. 83 ss.

[101] Il Regolamento UE n. 2022/350 ha vietato la diffusione nel territorio degli Stati membri delle trasmissioni di Russia Today e delle notizie rese dall'agenzia di stampa Sputnik, controllate entrambe dal governo russo. Nella pronuncia T-125/22 *RT France v Conseil*, (2022), il Tribunale dell'Unione europea ha salvato la misura restrittiva e ha ricondotto le attività di tali soggetti alla «propaganda di guerra»: «le campagne di disinformazione sono tali da rimettere in discussione i fondamenti delle società democratiche e fanno parte integrante dell'arsenale della guerra moderna» (par. 162). Sul punto v. M. Monti, *Il "Sedition Act" europeo? Spunti dalla comparazione sull'esclusione di Russia Today e Sputnik dal mercato dell'informazione unionale*, in «Osservatorio AIC» (2023), pp. 21 ss.

DISINFORMAZIONE E MANIPOLAZIONE DEL CONSENSO ELETTORALE TRA "POTERE PUNITIVO" DELLE PIATTAFORME ONLINE E TUTELA DEI DIRITTI FONDAMENTALI DEGLI UTENTI

Emanuele Birritteri

1. *Considerazioni introduttive*

La disinformazione online – specie avuto riguardo alla manipolazione del consenso elettorale – è un fenomeno molto complesso e di difficile inquadramento sotto i profili sociologico e giuridico[1].

Le prime difficoltà sono di carattere definitorio, per quanto risulti piuttosto diffusa e accettata la distinzione tra disinformazione e misinformazione: la prima (disinformazione) viene identificata nella condotta di chi diffonde un messaggio in rete che, per il suo contenuto o per il modo in cui viene presentato, può dirsi oggettivamente falso, a condizione che chi lo veicola sia consapevole di tale falsità e agisca allo scopo di perseguire finalità specifiche[2]; la seconda (misinformazione), invece, riguarderebbe per lo più il comportamento di chi diffonde una comunicazione falsa senza scopi specifici e

[1] Diffusamente sul punto v. le indagini monografiche di T. GUERINI, Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020, p. 20 ss., S. SASSI, *Disinformazione contro costituzionalismo*, Editoriale scientifica, Napoli, 2021, e G. SUFFIA, *Pulire l'infosfera. Intelligenza artificiale e contrasto alla disinformazione*, Giuffrè, Milano, 2022. Per un inquadramento v. altresì A. VISCONTI, *Alcune considerazioni criminologiche e politico-criminali sulle c.d. "Fake News"*, in «*Jus*», 1, (2020), p. 43 ss. Nella letteratura internazionale v., per tutti, J. HORDER, *Criminal Fraud and Election Disinformation: Law and Politics*, Oxford University Press, Oxford, 2022, *passim*. Per una più ampia analisi e *literature review* rispetto ai vari temi che saranno affrontati in questo capitolo sia consentito altresì il rinvio a E. BIRRITTERI, *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato*, in «Diritto penale contemporaneo – Rivista trimestrale», 4 (2021), p. 304 ss.

[2] Per una ricostruzione v. F. PIZZETTI, Fake news *e allarme sociale: responsabilità, non censura*, in «Rivista di Diritto dei Media», 1 (2017), p. 49. V. anche G. MATUCCI, *Informazione online e dovere di solidarietà. Le fake news tra educazione e responsabilità*, in «Rivista AIC», 1 (2018), p. 9, secondo cui dovrebbe trattarsi di scopi di carattere manipolatorio.

anche laddove sia in realtà inconsapevole di tale carattere della notizia che contribuisce "colposamente" a far circolare[3].

Non è semplice comprendere queste dinamiche della società digitale, essendo molto differenti le motivazioni che spingono le persone a diffondere informazioni false in rete più o meno consapevolmente.

A volte, infatti, determinati individui diffondono notizie false per finalità di profitto economico (è il caso, ad esempio, del noto fenomeno del c.d. *clickbait*[4]).

In altri casi, invece, le false notizie vengono dolosamente diffuse in rete per influenzare l'opinione pubblica, spingendola ad aderire ad un certo punto di vista o a collocarsi su specifiche "posizioni" rispetto a tematiche sensibili sul piano sociopolitico (ad es. il sostegno a un certo partito o candidato, la propria visione su temi legati ai diritti civili, all'immigrazione, etc.)[5]. Condotte, queste ultime, che possono avere motivazioni variegate ed essere frutto dell'agire di singolo o di gruppi o potenze stranieri interessati, nell'ambito di complicate strategie geopolitiche, ad influenzare il dibattito pubblico e finanche l'esito delle elezioni di altri Paesi. A tal fine, ci si serve, oltre che di raffinate metodologie di manipolazione del consenso, di avanzate tecniche informatiche (quali l'utilizzo di *bot* automatici, l'interazione coordinata di *fake account* etc.) volte ad aumentare artificiosamente le interazioni sulla notizia falsa e, quindi, la sua visibilità[6].

Questi meccanismi sono ulteriormente alimentati dallo stesso funzionamento tecnologico degli algoritmi dell'ecosistema digitale e delle piattaforme di interazione sociale sul *web*. Ad esempio, come noto, i sistemi di raccomandazione tendono a riproporre all'utente contenuti sempre più in linea con la propria attività online. La piattaforma, infatti, basa i suoi profitti sulla maggiore permanenza dell'utente in rete, con la conseguenza di poter anche innescare una continua riproposizione nei suoi riguardi di contenuti falsi o fuorvianti, ove questi abbiano in precedenza attratto la sua attenzione[7]. Questi ultimi rischiano così di divenire rapidamente virali in rete con tutto ciò che di negativo può derivarne per la salvaguardia di interessi quali l'integrità del dibattito pubblico e dei processi elettorali[8].

[3] Cfr., *ex multis*, R. Perrone, Fake news *e libertà di manifestazione del pensiero: brevi coordinate in tema di tutela costituzionale del falso*, in «Nomos», 2 (2018), p. 5. Una efficace tassonomia può leggersi anche in T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle* fake news *e delle infodemie*, in «Discrimen», 16 giugno 2020, p. 11 ss.

[4] A. Costantini, *Istanze di criminalizzazione delle* fake news *al confine tra tutela penale della verità e repressione del dissenso*, in «Diritto penale contemporaneo – Rivista trimestrale», 2 (2019), p. 63.

[5] Cfr. diffusamente G. Matucci, *Informazione online e dovere di solidarietà*, cit., p. 10.

[6] V.M. Bassini, G.E. Vigevani, *Primi appunti su* fake news *e dintorni*, in «Rivista di Diritto dei Media», 1 (2017), p. 16. Sui temi qui affrontati v. anche F. De Simone, 'Fake news', 'post truth', 'hate speech': *nuovi fenomeni sociali alla prova del diritto penale*, in «Archivio penale», 1 (2018), pp. 4-5.

[7] V.O. Pollicino, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, «Rivista di Diritto dei Media», 1, (2018), p. 81. V. diffusamente anche G. Marchetti, *Le fake news e il ruolo degli algoritmi*, in «Rivista di Diritto dei Media», 1 (2020), p. 29 ss., e G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in «Rivista di Diritto dei Media», 1 (2018), p. 26 ss.

[8] Oltre ai contributi già citati, v.: M. Fumo, *Bufale elettroniche, repressione penale e democrazia*, in «Rivista di Diritto dei Media», 1 (2018), p. 84; E. Scaroina, *Giustizia penale e comunicazione nell'era di* Twitter *tra controllo*

È chiaro, allora, quanto sia difficile il compito dei decisori pubblici di delineare *policy* di regolazione, anche sul versante punitivo, di siffatte dinamiche.

In questo contributo affronteremo la questione da un angolo visuale specifico, correlato alla disamina del ruolo delle piattaforme online nel contrasto alla disinformazione e alla manipolazione del consenso elettorale in rete alla luce degli obblighi di compliance definiti dal Regolamento europeo del 2022 relativo al mercato unico dei servizi digitali (il *Digital Services Act* - DSA).

Ci soffermeremo, in particolare, su tre aspetti: 1) in primo luogo, facendo, per così dire, qualche passo indietro, proveremo a menzionare alcune ragioni per cui, specialmente nell'ambito del contrasto alla disinformazione e alla manipolazione del consenso elettorale, non si può prescindere dal coinvolgimento proattivo dei grandi operatori privati; 2) successivamente, metteremo in luce i punti principali dell'assetto di regolazione definito sul punto dal DSA avuto riguardo alle obblighi di compliance imposti alla piattaforme non solo rispetto al contrasto dei contenuti illeciti, ma anche, e con riferimento al tema di questo scritto dovremmo forse dire *soprattutto*, di quelli che siano lesivi semplicemente dei c.d. *standard della community*, cioè delle *condizioni d'uso del servizio* che, alla luce di quanto prevede lo stesso regolamento europeo, deve essere la stessa piattaforma ad autonormare; 3) infine, cercheremo di evidenziare le criticità di alcune scelte di fondo compiute con questa importante riforma, specie rispetto ai profili dei limiti ai poteri degli operatori privati e della tutela dei diritti fondamentali degli utenti.

2. *Il necessario coinvolgimento dei grandi operatori privati nel contrasto alla manipolazione del consenso elettorale online*

Le strategie di politica del diritto negli ultimi anni, soprattutto in ambito europeo, si sono caratterizzate per il tentativo di coinvolgere sempre più, e con un ruolo proattivo, le grandi piattaforme e in generale, potremmo dire con una formula di sintesi, gli *operatori digitali privati* nella lotta ad allarmanti fenomeno online come discorsi d'odio, le discriminazioni nei confronti di minoranze, e, per quanto più qui ci interessa, la disinformazione e la manipolazione del consenso elettorale tramite tali servizi offerti sul web[9], specie con riferimento a tentativi di attori stranieri di influire sugli esiti delle elezioni di altri stati nel contesto di complesse dinamiche geopolitiche[10].

democratico e tutela dell'onore, in «Archivio penale», 3 (2018), p. 6; N. Zanon, Fake news *e diffusione dei* social media*: abbiamo bisogna un'"Autorità Pubblica della Verità"?*, in «Rivista di Diritto dei Media», 1 (2018), p. 13.

[9] V., per tutti, A. Gullo, *Contenuti, scopi e traiettoria della ricerca: le nuove frontiere della* compliance *nel mercato digitale*, in «Rivista di Diritto dei Media», 2 (2023), p. 13 ss.

[10] Per un inquadramento di tali aspetti e per un'ampia *literature review*, anche sotto il profilo empirico e sociologico, si veda la ricerca finanziata dal MAECI (realizzata dall'Harvard Kennedy School e dall'Università Luiss e diretta da Antonio Gullo, Irene Pasquetto, Gianni Riotta e Costanza Sciubba Caniglia) dal titolo "Come individuare e contrastare operazioni coordinate di disinformazione in Italia. Casi di studio e indicazioni di policy

Si tratta infatti di fenomeni che hanno trovato nel digitale una sorta di naturale terreno di proliferazione. Online, questi contenuti si propagano in modo virale e spesso incontrollato, oltre che a velocità allarmanti, con tutto ciò che di negativo ne consegue[11].

La scelta di cercare di coinvolgere questi grandi operatori privati del mercato digitale nello svolgimento di un compito tipicamente pubblico come quello del contrasto a questi comportamenti può ricondursi a una pluralità di ragioni e, come ogni significativa opzione di politica del diritto, presenta criticità e punti di forza. Cercheremo quindi di menzionarne alcune.

La prima (e forse più importante) motivazione potrebbe sintetizzarsi con una espressione che può ben restituire l'idea molto pragmatica che sta alla base dell'impostazione di fondo del *Digital Services Act*: i decisori pubblici e lo Stato con le sue istituzioni punitive, molto semplicemente, *non possono farcela da soli*.

Nella lotta contro alcune degenerazioni della società digitale, una risposta che si affidi al solo diritto penale, o in generale esclusivamente pubblica, potrebbe risultare, nella gran parte dei casi, lenta, incompleta e inefficace[12].

Per quanto più in questa sede ci interessa dobbiamo chiederci: rispetto a un contenuto che si ritenga miri a manipolare il consenso elettorale, o che venga considerato fonte di disinformazione, come facciamo a tracciare una linea di confine chiara tra falso e vero, tra fatti e opinioni soggettive? In ogni caso, ammesso che sia possibile tracciare con tassatività e chiarezza questo incerto confine, e ovviamente non sempre lo è, può un contenuto falso, di per sé e autonomamente, qualificarsi come illecito o penalmente rilevante? Il diritto penale può occuparsi di punire la mera falsità?

Di questi temi ci si è già occupati nel presente volume[13] e la risposta a questi interrogativi, pressoché unanime, è negativa[14], ma, a prescindere dalle legittime posizioni di ciascuno, già solo porsi queste domande chiarisce quanto sia complessa e tortuosa la strada che ha di fronte a sé il diritto penale quando si tratta di offrire una risposta, *e di offrire una risposta efficace*, a queste istanze di tutela.

Interrogarsi su quale possa essere il ruolo del diritto penale nel contrasto al fenomeno della disinformazione online impone invero di concentrarsi su due questioni di fondo tra loro interconnesse: *a)* se, *de iure condito*, possa assumere rilevanza penale la mera diffusione di una notizia falsa, a prescindere dalla lesione o dalla messa in pericolo di interessi diversi dalla mera veridicità della notizia in sé; *b)* se, *de iure condendo*, la verità (dell'informazione in generale e delle notizie condivise online) possa assurgere a bene giuridico autonomamente presidiabile dal diritto penale.

per istituzioni pubbliche e private", il cui ultimo report, con rinvio anche agli elaborati finali dei precedenti due cicli della ricerca, è reperibile al seguente link: urly.it/319fdb.

[11] Cfr. la dottrina richiamata *supra sub* par. 1.

[12] Sia consentito, per una più ampia disamina, rinviare ancora a E. Birritteri, *Punire la disinformazione*, cit., p. 304 ss.

[13] Cfr. il contributo di A. Costantini in questo volume.

[14] Cfr. infra in questo paragrafo per tutti i riferimenti.

È agevole risponde negativamente alla prima domanda: in base al diritto vigente, come bene si è evidenziato in dottrina, la diffusione di una falsa notizia in quanto tale non assume mai rilievo penale in quanto tale, ma solo ove la comunicazione arrechi offesa a beni giuridici diversi (ad es.: l'ordine pubblico, l'onore individuale, etc.)[15].

Il secondo quesito è invece più complesso, ma la risposta aiuterà a comprendere la ragione per la quale il nostro legislatore penale ad oggi non ha mai criminalizzato la semplice condotta di disinformazione, neanche nei contesti elettorali.

Già da un punto di vista etico, anzitutto, l'esistenza di un dovere morale di verità in capo al singolo è una questione su cui anche in filosofia sono state espresse posizioni non univoche[16], essendo controversa la stessa possibilità di poter sempre agevolmente distinguere il falso dal vero, la realtà dei fatti dalle opinioni e dall'approccio soggettivo all'interpretazione di certe vicende. Più complesso è un accadimento, del resto, più sfumato diventa il confine tra oggettivo e soggettivo[17].

Ad ogni modo, occorre affrontare necessariamente la questione sul piano della tutela della libertà di espressione ai sensi dell'art. 21 della Costituzione

Nella dottrina costituzionalistica, invero, si discute sulla possibilità di estendere la garanzia costituzionale relativa al *free speech* (art. 21 Cost.) alla protezione del diritto di esternare (anche) notizie false. Tralasciamo ovviamente le ipotesi in cui la falsa comunicazione leda interessi diversi dalla mera veridicità dell'informazione: in questi casi, infatti, l'assenza in Costituzione di "diritti tiranni"[18] impone di bilanciare la libertà di espressione con altri interessi meritevoli di tutela che possono, a certe stringenti condizioni, legittimare la punizione della c.d. "parola pericolosa"[19].

Ci concentriamo, invece, sulla possibilità di estendere le garanzie dell'art. 21 alle affermazioni false in sé, perché solo rispondendo a questo interrogativo saremo in grado di capire se sia ipotizzabile la criminalizzazione della disinformazione in quanto tale.

Sul punto, è stato evidenziato come per stabilire se una comunicazione debba essere protetta ai sensi dell'art. 21 Cost. non conti il fatto che essa possa dirsi vera o falsa – senza

[15] Sul punto la dottrina è unanime. V., *ex multis*: A. COSTANTINI, *Istanze di criminalizzazione delle* fake news, cit., 68; C. DEL BÒ, *La protezione dal falso e la tutela del vero tra filosofia e diritto*, in «Governare la paura» (2019), p. 100; E. LEHNER, *Fake news e democrazia*, in «Rivista di Diritto dei Media», 1 (2019), p. 16; C. MELZI D'ERIL, Fake news *e responsabilità: paradigmi classici e tendenze incriminatrici*, in «Rivista di Diritto dei Media», 1 (2017), p. 64; C. PERINI, Fake news *e post-verità tra diritto penale e politica criminale*, in «Diritto penale contemporaneo», 20 dicembre 2017, p. 3; D. PULITANÒ, *Cura della verità e diritto penale*, in *"Verità" del precetto e della sanzione penale alla prova del processo*, a cura di G. Forti, G. Varraso e M. Caputo, Jovene, Napoli, 2014, p. 90.

[16] V., per tutti, T. PADOVANI, *Menzogna e diritto penale*, Pisa University Press, Pisa, 2014, p. 257 ss.

[17] Sui problematici contenuti del concetto di verità v. A. GULLO, *Brevi note sulla verità come limite del diritto di cronaca*, in «Diritto e formazione», 5 (2002), p. 631.

[18] Si veda al riguardo l'insegnamento della Corte Costituzionale nella nota vicenda ILVA (Corte Cost., sent. 9 aprile 2013, n. 85 in *cortecostituzionale.it*).

[19] Per un'approfondita disamina v. il lavoro monografico di A. GALLUCCIO, *Punire la parola pericolosa? Pubblica istigazione, discorso d'odio e libertà di espressione nell'era di internet*, Giuffrè, Milano, 2020. V. diffusamente anche M. PELISSERO, *La parola pericolosa. Il confine incerto del controllo penale del dissenso*, in «Questione giustizia» (2015), p. 4.

considerare, peraltro, che non è sempre possibile stabilirlo con sufficiente oggettività –, ma l'atteggiamento psicologico del dichiarante, che godrebbe della garanzia costituzionale anche in caso di «espressione di fatti obiettivamente errati, qualora in buona fede essi vengano ritenuti veri da parte di chi ne afferma l'esistenza»[20], mentre esulerebbe dal raggio applicativo dell'art. 21 l'affermazione di un fatto falso nella consapevolezza soggettiva, da parte dell'agente, della sua non rispondenza al vero; si spiega, infatti, che la Costituzione protegge l'esternazione di un "proprio" pensiero e tale non è quello che scientemente diverge dalla rappresentazione dei fatti interiorizzata dal dichiarante[21].

Tuttavia, ciò non significa che queste ultime affermazioni debbano essere considerate illecite[22] o, a maggior ragione, legittimamente criminalizzabili. Ed infatti si è parimenti chiarito come non sia rinvenibile alcun generalizzato dovere esplicito o implicito di verità nel sistema di valori della nostra Carta fondamentale[23]. Neanche il diritto del cittadino di essere informato (e non solo di informare) può declinarsi nella pretesa positiva di ricevere notizie che abbiano un certo contenuto[24], ma al più in quella di poter accedere a ogni mezzo o contenuto informativo nel libero dibattito pubblico senza l'interposizione di alcun ostacolo per la realizzazione di una società pluralista[25].

In definitiva, allora, la possibilità di sanzionare penalmente la diffusione di notizie false non può prescindere dall'individuazione di interessi diversi dalla mera veridicità dell'informazione che possano essere validamente protetti dallo *ius criminale* al metro della Costituzione[26].

Quando il legislatore ha tentato di proporre l'introduzione di nuovi reati per punire la mera diffusione in rete di notizie false, però, la dottrina non ha mancato di muovere (giuste) critiche a fronte dell'individuazione di beni giuridici ed elementi costitutivi di fatti di reato dal contenuto indeterminato e inafferrabile; norme, quindi, non rispettose dei requisiti minimi di tassatività della legge penale e apparse sin da subito in frontale contrasto con i correlati principi fondamentali di garanzia. Non a caso, simili novelle non hanno mai visto la luce, non essendo neanche iniziato l'esame in Parlamento[27].

[20] N. Zanon, Fake news *e diffusione dei* social media, cit., p. 13. Cfr. altresì A. Candido, *Libertà di informazione e democrazia ai tempi delle* fake news, in «Federalismi» (2020), p. 20, 111. Sul punto v. anche E. Scaroina, *Giustizia penale e comunicazione nell'era di* Twitter, cit., p. 17.

[21] V., con chiarezza: G. Matucci, *Informazione online e dovere di solidarietà*, cit., p. 5; T. Padovani, *Menzogna e diritto penale*, cit., p. 331; R. Perrone, Fake news *e libertà di manifestazione del pensiero*, cit., p. 9.

[22] Cfr. la dottrina richiamata nella nota precedente.

[23] Cfr. A. Candido, *Libertà di informazione e democrazia*, cit., p. 110.

[24] V. anche S. De Flammineis, *Diritto penale, beni giuridici collettivi nella sfida delle* fake news*: principio di offensività ed emergenze*, in «Sistema penale», 6 (2020), p. 140, e E. Lehner, *Fake news e democrazia*, cit., p. 17. Per un'ampia riflessione, in generale, su questi temi si veda anche S. Foà, *Pubblici poteri e contrasto alle* fake news. *Verso l'effettività dei diritti aletici?*, in «Federalismi», 11 (2020), p. 248 ss.

[25] V.M. Bassini, G.E. Vigevani, *Primi appunti*, cit., p. 18.

[26] Per ulteriori spunti rispetto a tale conclusione v., volendo, E. Birritteri, *Punire la disinformazione*, cit., p. 311.

[27] V., in particolare, l'A.S. 2688 (c.d. d.d.l. Gambaro), che ha inteso puntare, anzitutto, sull'introduzione di un nuovo reato, l'art. 656-*bis* c.p., volto a sanzionare la pubblicazione o diffusione «…attraverso piattaforme

Non si è mancato, peraltro, di ipotizzare la criminalizzazione non della diffusione di notizie false in generale, ma, per così dire, di specifiche declinazioni delle condotte manipolatorie (anche del consenso) in questione.

Nel 2025, ad esempio, con la legge n. 132 del 2025, recante "Disposizioni e deleghe al Governo in matera di intelligenza artificiale"[28], è stato introdotto nel codice penale il nuovo art. 612-*quater*, rubricato "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza di intelligenza artificiale", che punisce con la reclusione da uno a cinque anni chiunque «…cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità»[29].

Si tratta di una fattispecie criminosa che assume una non secondaria importanza nell'ambito delle strategie pubbliche di lotta alla disinformazione in rete, in quanto volta a contrastare i danni potenzialmente associati alla messa in circolazione nel web dei cc.dd. *deep fake*, uno degli strumenti potenzialmente più insidiosi utilizzati da chi intende diffondere notizie false in rete, specie nell'ambito di azioni coordinate di *disinformation* e soprattutto nelle fasi elettorali. Si pensi a un *deep fake* diffuso durante le elezioni che, con la creazione di un video totalmente artefatto ma non difficilmente identificabile come tale alla luce delle straordinarie capacità dei sistemi di intelligenza artificiale, rappresenti falsamente un candidato mentre commette un grave fatto di reato[30].

informatiche destinate alla pubblicazione o diffusione presso il pubblico, con mezzi prevalentemente elettronici o comunque telematici, [di] notizie false, esagerate o tendenziose che riguardano dati o fatti manifestamente infondati o falsi», nonché dei nuovi artt. 265-*bis* e 265-*ter* c.p., rispettivamente dedicati alla repressione di chiunque diffonde o comunica «…voci o notizie false, esagerate o tendenziose, che possono destare pubblico allarme, o svolge comunque un'attività tale da recare nocumento agli interessi pubblici o da fuorviare settori dell'opinione pubblica, anche attraverso campagne con l'utilizzo di piattaforme informatiche destinate alla diffusione online», nonché della diffusione di «…campagne d'odio contro individui o di campagne volte a minare il processo democratico, anche a fini politici». Per una più ampia disamina dei progetti di riforma in materia v. A. COSTANTINI, *Istanze di criminalizzazione delle* fake news, cit., p. 60 ss., e, volendo, E. BIRRITTERI, *Punire la disinformazione*, cit., p. 321 ss.

[28] Per un'analisi del d.d.l. v.: G. BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in «Diritto penale e processo», 8 (2024), p. 991 ss.; B. ROMANO, *Il DDL in materia di IA: l'utilizzo nell'attività giudiziaria e in ambito sanitario*, in «Rivista italiana di medicina legale», 1-2 (2024), p. 409 ss.

[29] Il secondo comma del reato di nuovo conio sancisce poi che il «il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate». Avuto riguardo alla possibilità di utilizzare il diritto penale nel contrasto alla disinformazione, si era già rilevata in dottrina la possibilità di ricavare un limitato spazio di intervento penalistico nell'ambito del settore elettorale, ad es. proprio rispetto alle condotte di creazione di cc.dd. *deepfake*: v. T. GUERINI, Fake news *e diritto penale*, cit., p. 209.

[30] Per un ampio inquadramento del fenomeno v. di recente V. AZZALI, N. ELLECOSTA, *La questione "deepfake" in Italia: una panoramica*, in «Rivista di Diritto dei Media», 3 (2023), p. 72 ss.; M. CAZZANIGA, *Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai* deepfakes, in «Rivista di Diritto dei Media», 1 (2023), p. 170 ss.

Non è del resto un caso che il recente d.d.l. A.C. 2212, presentato alla Camera dei deputati nel mese di gennaio del 2025 e recante modifiche "alla legge 4 aprile 1956, n. 212 (*n.d.r.* sulle norme relative alla disciplina della propaganda elettorale) e altre disposizioni per prevenire l'alterazione o la manipolazione delle campagne elettorali e referendarie attraverso la diffusione di contenuti ingannevoli prodotti mediante sistemi di intelligenza artificiale" proponga l'introduzione nella l. n. 212 del 1956 di un nuovo reato (art. 9-*novies*) volto a punire con la reclusione da uno a quattro anni «chiunque, al fine di alterare il libero svolgimento delle campagne elettorali o referendarie o di manipolarne il risultato, cede, pubblica o altrimenti diffonde contenuti ingannevoli o manipolatori generati in tutto o in parte con sistemi di IA»[31]. Ciò, peraltro, nel contesto di ulteriori misure volte a proibire la creazione e la diffusione di simili contenuti nelle fasi elettorali e a renderli, con appositi sistemi di etichettatura e filigrana elettronica, agevolmente identificabili, con l'attribuzione all'Autorità per le garanzie nelle comunicazioni (AGCOM), in caso di inosservanze, del potere di applicare sanzioni amministrative e misure accessorie interdittive e cautelari di blocco tecnico[32].

È necessario però comprendere se la criminalizzazione di questi comportamenti sia una scelta opportuna e soprattutto realmente efficace, o se invece non possa ritenersi più adeguato (e soprattutto efficace, alla luce delle note criticità in punto di tempistiche procedimentali penalistiche) puntare sul coinvolgimento proattivo degli operatori privati del settore per arginare la diffusione di simili contenuti, che certamente possono a volte influire in modo sensibilmente negativo su interessi collettivi di rilievo come, ad esempio, l'integrità dei processi elettorali.

La risposta penale, infatti, appare per tutte le ragioni pocanzi esposte difficilmente percorribile, quantomeno rispetto al fenomeno generale della mera diffusione in sé di notizie false, al netto di sue specifiche declinazioni peculiari, come la diffusione di *deep fake*, che si ritengano o meno legittimamente criminalizzabili e che in ogni caso costituiscono solo una parte di un fenomeno più ampio, per cui sono necessarie misure di contrasto di largo respiro. E ciò anche con riferimento manipolazione del consenso elettorale.

Occorre quindi andare alla ricerca di strategie alternative di complessiva gestione di simili, complesse dinamiche sociali, senza cedere alla tentazione di rispondere con il solo strumento penale a problemi che richiedono soluzioni ben più articolate.

[31] Il testo del d.d.l. è reperibile al seguente link: https://www.camera.it/leg19/126?&leg=19&idDocumento=2212.

[32] L'art. 2 dell'A.C. 2212, peraltro, unitamente a talune eccezioni circa il divieto di diffusione di tali *content* relative, ad esempio, a programmi a scopo didattico, informativo o di satira politica, consente a chiunque «sia vittima di forme di alterazione, manipolazione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità o trattamento illecito di dati personali, attraverso la diffusione di contenuti ingannevoli o manipolati generati in tutto o in parte da sistemi di IA» di presentare al titolare del trattamento o al gestore del sito internet o della piattaforma digitale un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti in parola, previa conservazione dei dati originali. L'istanza è presenta contestualmente all'AGCOM che può, tramite i già menzionati provvedimenti cautelari, ordinare ai prestatori di disabilitare l'accesso ai contenuti.

Per contrastare questi fenomeni online, allora, è indispensabile ottenere la collaborazione delle grandi piattaforme digitali, che hanno le capacità tecniche, organizzative, economiche e gestionali per individuare e rimuovere rapidamente contenuti illeciti o semplicemente (come spesso sarà nei casi di disinformazione) meramente lesivi delle loro condizioni d'uso del servizio.

Del resto, una difesa a spada tratta del tradizionale *principio di neutralità* della rete e dei *provider*, quantomeno in termini assoluti e inflessibili, sarebbe per certi versi anacronistica. Si tratta infatti di un principio la cui *ratio* storica risale agli albori di internet, quando l'interesse di molti Stati e di molti sistemi economici era soprattutto quello di lasciare il web libero di sprigionare a pieno tutte le sue straordinarie potenzialità senza essere imbrigliato in complessi meccanismi e oneri regolamentari[33].

Ed è invero nel senso di un coinvolgimento attivo degli attori privati che, come subito diremo[34], si è mosso in particolare il legislatore eurounitario.

3. *La "rivoluzione" del* Digital Services Act *europeo tra obblighi di compliance e "potere punitivo" delle piattaforme online*

Il *Digital Services Act* ha mantenuto fermo il tradizionale risvolto penalistico del principio di neutralità dei *provider* – e cioè l'assenza di obblighi generali di sorveglianza o di accertamento attivo di fatti che indichino la presenza di attività illegali in capo a tali operatori con riferimento ai contenuti immessi in rete dagli utenti[35] – ma, allo stesso tempo, il nuovo Regolamento ha introdotto in questo ambito un significativo apparato *piramidale* di obblighi di compliance a carico degli attori privati, nel senso che l'intensità di questi obblighi di *due diligence* cresce in misura direttamente proporzionale all'importanza del soggetto regolato[36].

[33] Sui temi da ultimo citati v., anche per ulteriori riferimenti bibliografici, M. CUNIBERTI, *Potere e libertà nella rete*, in «Rivista di Diritto dei Media», 3 (2018), p. 40 ss. Sui temi correlati all'evoluzione della disciplina della responsabilità dei *provider* v. ampiamente anche la dottrina richiamata *infra sub* par. n. 3.

[34] V. il paragrafo successivo.

[35] In argomento v. più di recente, per un commento sull'impatto del DSA, S. BRASCHI, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider*?*, in «Diritto penale e processo», 3 (2023), p. 367 ss., e L. D'AGOSTINO, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act, in «Rivista di Diritto dei Media», 2 (2023), p. 16 ss. Ancor prima v., ex multis: R. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'"Internet Service Provider"*, in «Diritto penale e processo», 5 (2013), p. 600 ss.; A. INGRASSIA, *Responsabilità penale degli "internet service provider": attualità e prospettive*, in «Diritto penale e processo», 12 (2017), p. 1621 ss.; A. MANNA, *La prima affermazione, a livello giurisprudenziale, della responsabilità penale dell'internet* provider*: spunti di riflessione tra diritto e tecnica*, in «Giurisprudenza costituzionale», 2 (2010), p. 1856 ss.; B. PANATTONI, *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online*, in «Diritto penale contemporaneo – Rivista trimestrale», 2 (2019), p. 33 ss.; L. PICOTTI, *La responsabilità penale dei* service-providers *in Italia*, in «Diritto penale e processo», 4 (1999), p. 501 ss.; S. SEMINARA, *La responsabilità penale degli operatori su internet*, in «Il Diritto dell'informazione e dell'informatica», 4-5 (1998), p. 745 ss.

[36] V.A. GULLO, *Contenuti, scopi e traiettoria*, cit., p. 13 ss. Per un ampio inquadramento dell'argomento e per una più approfondita *literature review* sui temi affrontati in questo paragrafo sia consentito altresì rinviare a

E ciò segna ovviamente un decisivo cambio di paradigma.

Il DSA, infatti, introduce una serie di *due diligence obligation* per determinati *provider*, con un innovativo sistema di obblighi strutturato secondo vari 'livelli' di intensità crescente e diversificati in base al particolare destinatario degli stessi, tenendo conto della sua importanza e della dimensione del *business*; in particolare, a ogni nuovo livello 'aggiuntivo' alcuni operatori vengono chiamati a conformarsi a disposizioni ulteriori che vanno a sommarsi (e non già a sostituirsi) a quelle dei livelli precedenti[37].

Il regolamento muove in tal senso dalla dimensione 'base' delle previsioni applicabili a tutti i prestatori di servizi intermediari, tra cui il dovere di definire termini e condizioni del servizio nel rispetto, tra l'altro, dei diritti fondamentali sanciti dalla 'Carta' europea e in particolare della libertà di espressione (art. 14) e quello di pubblicare (*ex* art. 15) relazioni periodiche sulle attività di moderazione dei contenuti immessi in rete dagli utenti[38].

Si passa poi, a livello 'intermedio', alle regole per prestatori di servizi di memorizzazione e piattaforme online, tra cui, *ex multis*, il dovere di: *a)* predisporre meccanismi di *notice and action* per consentire agli utenti di presentare segnalazioni circa la presenza di contenuti illegali (art. 16); *b)* fornire motivazioni dettagliate sulle restrizioni imposte (art. 17); *c)* istituire sistemi interni di gestione dei reclami (art. 20) e meccanismi (art. 22) per trattare in via prioritaria le segnalazioni presentate dai c.d. *trusted flaggers*[39].

Si giunge, quindi, all'ultimo 'gradino' concernente le più gravose regole applicabili soltanto alle piattaforme online e ai motori di ricerca di 'dimensioni molto grandi'. Qui il legislatore ha ampiamente valorizzato le metodologie classiche della *corporate compliance*, richiedendo, ad esempio, alle c.d. VLOPs (*Very Large Online Platforms*) e ai c.d. VLOSEs (*Very Large Online Search Engines*) di: *a)* effettuare attività di *risk assessment* e *management* (artt. 34 e 35) dei 'rischi sistemici' legati ai servizi digitali e alla possibilità che siano utilizzati per diffondere contenuti illegali o generare un impatto negativo su interessi individuali e collettivi fondamentali, quali il benessere psicofisico della persona, la salute pubblica, e, per quanto qui più interessa, il *dibattito civico e i processi elettorali*[40]; *b)* sottoporsi ad *audit* indipendenti esterni annuali

E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori*, in «Rivista di Diritto dei Media», 2 (2023), p. 52 ss.

[37] Per un primo inquadramento generale v. anche B. Tassone, *Riflessioni introduttive*, in «Diritto di Internet», 1 (2023), p. 3 ss. Nella letteratura internazionale v. altresì A. Turillazzi, M. Taddeo, L. Floridi, F. Casolari, *The digital services act: an analysis of its ethical, legal and social implications*, in «Law, Innovation and Technology», 15/1 (2023), p. 83 ss.

[38] Rispetto a tali obblighi diversificati in dottrina si è subito parlato di approccio '*pyramid base*': v. M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi intermediari, ai prestatori di servizi di* hosting *e ai fornitori di piattaforme* online *(Artt. 11-32 – Capo III, Sezioni, 1, 2, 3 e 4)*, in «Diritto di Internet», 1 (2023), p. 21.

[39] V. anche P. Leerssen, *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, in «Computer Law & Security Review», 48 (2023), p. 6.

[40] Sui temi qui indagati v. anche N. Zingales, *The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence*, in *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, a cura di J. van Hoboke, J.P. Quintais, N. Appelman, R. Fahy, I. Buri e M. Straub, Verfassungsbooks, Berlino, 2023, pp. 213-214.

(art. 37) e istituire una apposita funzione di compliance (art. 41) per il monitoraggio della conformità dell'organizzazione agli obblighi del DSA[41].

Sotto tale profilo il regolamento costituisce una normativa all'avanguardia, che tenta – sostanzialmente per la prima volta nello scenario globale – di definire ciò che prima del DSA mancava del tutto: *i.e.*, una regolamentazione che, attraverso obblighi specifici e calibrati sull'importanza di ciascun operatore privato, riconducesse e disciplinasse l'esercizio del potere degli operatori digitali di autonormare le *policy* interne di funzionamento e utilizzo dei loro servizi entro i confini di una specifica 'cornice' legislativa pubblicistica[42]. Ciò alla luce dell'impatto che tali attività di regolazione ed *enforcement* privati possono generare sui diritti fondamentali degli utenti: si pensi, per quanto qui interessa, alla definizione delle politiche della piattaforma in merito alla condivisione di notizie false che, come sappiamo, può influire in modo significativamente negativo sulla libertà di espressione dei soggetti destinatari delle misure di moderazione dei contenuti adottate, ad esempio, dai grandi *social network*.

Il DSA richiede perciò di svolgere un'attività di valutazioni di simili rischi all'esito della quale, poi, i grandi operatori devono introdurre misure di *risk managament*, anche di carattere tecnico, per mitigare il potenziale impatto negativo sui diritti fondamentali, ad es. tramite l'adeguamento dei sistemi di raccomandazione[43].

Un punto, quest'ultimo, che è del resto decisivo.

Ad esempio, come noto e già ricordato[44], tali meccanismi di tendono a riproporre all'utente contenuti sempre più in linea con la propria attività e con ciò che risulta aver precedentemente attratto la sua attenzione, la piattaforma infatti basa i suoi profitti sulla maggiore permanenza dell'utente in rete, con la conseguenza di innescare un continuo "bombardamento" nei suoi riguardi, ad esempio, di contenuti falsi, tesi anche alla manipolazione del consenso elettorale, come dei post che diano informazioni obiettivamente false sui requisiti per accedere al voto. Questi contenuti rischiano così

[41] Su questi temi v. anche A.P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, in *Digital Platform Regulation. Global Perspectives on Internet Governance*, a cura di T. Flew e F.R. Martin, Palgrave Macmillan, Londra, 2022, p. 79.

[42] V. diffusamente anche G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in «Giornale di diritto amministrativo», 1 (2023), p. 116 ss., e L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in «Rivista trimestrale di diritto pubblico», 4 (2022), p. 1108. V. in argomento da ultimo, anche con note critiche, U. Ruffolo, *Piattaforme e "content moderation" negoziale*, in «Giurisprudenza italiana», 2 (2024), p. 442 ss.

[43] Su questi temi v. anche A. Manganelli, A. Nicita, *Regulating Digital Markets. The European Approach*, Palgrave Macmillan, Londra, 2022, p. 177 ss. Su questi temi v. di recente anche: M. Capparelli, *Disinformazione online, intelligenza artificiale (IA) e ruolo dell'autoregolamentazione*, in «Giurisprudenza italiana», 2 (2024), p. 480 ss.; L. Fabiano, *Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati*, in «Il diritto dell'informazione e dell'informatica», 4-5 (2023), p. 597 ss.; B. Grazzini, *"Fake news" e disinformazione*, in «Giurisprudenza italiana», 2 (2024), p. 491 ss.; E. Longo, *Libertà di informazione e lotta alla disinformazione nel "Digital Services Act"*, in «Giornale di diritto amministrativo», 6 (2023), p. 737 ss.; S. Sassi, *L'Unione Europea e la lotta alla disinformazione "online"*, in «Federalismi», 15 (2023), p. 183 ss.

[44] V. *supra* par. 1 anche per tutti i relativi riferimenti.

di divenire rapidamente virali in rete con tutto ciò che di negativo può derivarne per l'integrità del dibattito pubblico e dei processi elettorali.

Si richiedono, poi, come visto, ulteriori adempimenti di dettaglio che mutuano le tradizionali metodiche della *corporate compliance* (svolgimento di *audit* indipendenti, monitoraggio costante delle misure di gestione del rischio adottate, introduzione di una funzione aziendale di compliance). Un modello di regolazione, questo, che valorizza la compliance e la *prevenzione mediante virtuosa organizzazione*, che stanno diventando la cifra delle strategie di politica del diritto europee di questi anni (pensiamo, solo per fare un paio esempi, al GDPR e alla recente CSDDD – *Corporate Sustainability Due Diligence Directive*)[45].

Il DSA, poi, delinea un consistente apparato di *enforcement* a presidio del rispetto di queste nuove regole[46].

Tutti gli Stati membri, anzitutto, sono tenuti a nominare un coordinatore dei servizi digitali, quale primaria autorità incaricata di vigilare sul rispetto del regolamento. Nella logica della competenza concorrente, i coordinatori nazionali dei servizi digitali condividono il compito di monitorare l'osservanza del regolamento, e di applicare le correlate misure sanzionatorie in caso di inosservanza dei relativi obblighi, con la Commissione europea. Quest'ultima, in particolare, assume il ruolo di interlocutore primario (e addirittura 'esclusivo' per ciò che concerne le *due diligence obbligation* di cui alla sezione V del Capo III del Regolamento) nei confronti di piattaforme e motori di ricerca di 'dimensioni molto grandi', essendovi chiaramente la volontà di contrapporre un attore sovranazionale e 'di peso' rispetto a società multinazionali e detentrici di rilevanti poteri[47].

Pur non prevedendosi l'introduzione di sanzioni penali, i poteri di cui godono le autorità di *enforcement* sono molto significativi, potendosi applicare (v. gli artt. 52, 74 e 76), in caso di inosservanza degli obblighi del DSA, sanzioni pecuniarie fino al 6 % del fatturato mondiale annuo del *provider* e fino all'1% del reddito annuo o del fatturato mondiale del fornitore per i casi di mancata cooperazione e altre violazioni 'minori', oltre a penalità di mora per le perduranti inosservanze (secondo un meccanismo riconducibile, in sostanza, al *paradigma ingiunzionale*)[48].

L'apparato sanzionatorio per l'inosservanza di questi obblighi di compliance è quindi in grado di assumere un significativo livello di incisività, con la Commissione europea che peraltro esercita direttamente e *ha già esercitato* i suoi poteri di *enforcement* proprio nei confronti delle piattaforme di "dimensioni molto grandi". Si pensi

[45] Sul punto v. ancora A. Gullo, *Contenuti, scopi e traiettoria*, cit., p. 13 ss.

[46] V. in argomento l'approfondito saggio di R. Sabia, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in «Rivista di Diritto dei Media», 2 (2023), p. 88 ss.

[47] V.R. Sabia, *L'*enforcement *pubblico del* Digital Services Act, cit., p. 104.

[48] V. ancora R. Sabia, *L'*enforcement *pubblico del* Digital Services Act, cit., p. 98 ss.

al procedimento formale avviato, appunto, dalla Commissione europea contro Meta proprio in relazione al contrasto alla disinformazione durante i periodi elettorali[49].

I punti davvero centrali, però, a nostro avviso sono due.

Il DSA, infatti, menziona soltanto le macro-tipologie di misure che le piattaforme *possono* (*e non per forza devono*, ecco il punto) autonormare e adottare al fine di gestire e mitigare i rischi sistemici connessi all'impatto dei loro servizi sui diritti fondamentali e sugli interessi individuali e collettivi in gioco, compresa l'integrità dei processi elettorali e il dibattito civico.

In tutto il regolamento, insomma, il regolatore europeo è sempre ben attento a non imporre agli operatori modelli "preconfenzionati", misure particolari o dettagliate politiche sull'organizzazione e la gestione operativa dei loro servizi, lasciando loro, anche in tale sede, un ampio margine di apprezzamento.

La convinzione pare essere quella dell'impossibilità di positivizzare analiticamente le cautele imposte sulla base di un modello anche solo per alcune parti uguale per tutti, e della necessità, piuttosto, di lasciare liberi i soggetti regolati di costruire autonomamente le proprie regole interne secondo una pura logica *taylor made*, fornendo indicazioni di scopo di carattere generale e qui, in qualche misura, anche una metodologia di *risk analysis* oltre a un elenco di possibili contromisure e ambiti di rischio specifici da considerare.

La tendenza è quella di *procedimentalizzare* la salvaguardia dei diritti fondamentali degli utenti, piuttosto che imporre un modello di tutela improntato sull'imposizione di specifiche scelte di merito da parte dell'operatore privato circa le modalità di gestione dei contenuti[50].

La scelta finale circa le *policy* da adottare in concreto, quindi, spetterà sempre agli operatori, il che è un tema molto rilevante anche sul versante sanzionatorio, nella misura in cui il DSA, in tale ambito, potrà a rigore dirsi violato allorquando i soggetti regolati abbiamo in tutto o in parte omesso o non effettuato correttamente, secondo i criteri metodologici di analisi e gestione forniti dal regolatore europeo, lo svolgimento delle attività di *risk assessment* e *management*, e non già, di per sé, per la (ben motivata) scelta di non adottare (o di adottare in un certo modo) le specifiche, singole misure di gestione del rischio, rispetto alle quali le *corporation* mantengono un autonomo potere decisorio[51].

Si pensi ad esempio alla decisione di non adeguare (o di adeguare in modo diverso dalle aspettative del regolatore) i propri sistemi di raccomandazione per evitare che finiscano per rendere virali contenuti falsi, punto molto delicato perché ovviamente incide sugli interessi economici e sullo stesso modello di *business* delle piattaforme.

[49] Tutte le informazioni di dettaglio sul procedimento sono reperibili al seguente link: urly.it/319fvt.

[50] Su tali problematiche v., per tutti, il volume di G. PITRUZZELLA, O. POLLICINO, *Disinformation and Hate Speech. A European Constitutional Perspective*, Egea, Milano, 2020, *passim*.

[51] Sia consentito, circa gli aspetti da ultimi trattati, rinviare per ulteriori riferimenti a E. BIRRITTERI, *Contrasto alla disinformazione,* Digital Services Act, cit., p. 75.

Anche sul piano, per così dire, dei diritti di difesa degli utenti, delle garanzie, cioè, da riconoscere loro per proteggersi contro i poteri para-sanzionatori delle piattaforme (pensiamo alla rimozione dei post o alla cancellazione dell'*account* anche di rilevanti personaggi politici), che pure possono incidere su diritti fondamentali come la libertà di espressione ovviamente, il regolamento è piuttosto timido e a parte le clausole generali dell'obbligo di fissare le condizioni d'uso «nel rispetto dei diritti fondamentali degli utenti», aggiunge ben poco su come in concreto si possa conciliare tale attività di *digital patrolling* con questi interessi fondamentali, visto il rischio di censure e *chilling effect* che tale *enforcement* può produrre rispetto al libero confronto democratico[52].

4. *Le criticità: i limiti ai poteri degli operatori privati e la tutela dei diritti fondamentali degli utenti*

Veniamo quindi alle controindicazioni di tale riforma e delle scelte di fondo compiute dal legislatore europeo in sede di adozione del DSA.

Anzitutto, delegare a questi operatori privati, in sede di definizione delle condizioni d'uso del servizio (vero aspetto cruciale per il contrasto alla disinformazione), il compito di definire i confini, per così dire, tra consentito e non consentito, tra ciò che è o non è disinformazione, e l'esercizio di una potestà para-punitiva nei confronti dell'utente che superi questi limiti autonormati dalla piattaforma, implica una legittimazione pubblica di una sorta di *ius puniendi* privato, le cui sanzioni tipiche vanno dalla rimozione del *post* e dei contenuti, alla sospensione o disabilitazione dell'*account*, alla c.d. demonetizzazione dei contenuti o alla riduzione tecnica della loro visibilità o viralità in rete[53].

Un diritto para-punitivo che, pur esercitato nel contesto di una piattaforma privata, ben può influire, è questo il punto centrale, su diritti fondamentali e sulle libertà di espressione e partecipazione degli individui, posto che ormai questi ambienti digitali costituiscono una delle principali e più importanti arene del dibattito pubblico[54] (è

[52] Sulle criticità dei meccanismi di *enforcement* del DSA v. anche: V. Colarocco, M. Cogode, *Gli obblighi applicabili a piattaforme* online *di dimensioni molto grandi (Artt. 33-43 – Capo III, Sezione 5)*, in «Diritto di Internet», 1 (2023), p. 32; J. Laux, S. Wachter, B. Mittelstadt, *Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA*, in «Computer Law & Security Review», 43 (2021), p. 43, 1.; A. Palumbo, J. Piemonte, *Delega di funzioni regolamentari e lotta ai rischi sistematici causati dalla disinformazione nel "Digital Services Act": quali rischi per la libertà di espressione?*, in «Rivista di Diritto dei Media», 3 (2023), p. 114 ss.

[53] Su questi temi v. già C. Pinelli, *"Postverità", verità e libertà di manifestazione del pensiero*, in «Rivista di Diritto dei Media», 1 (2017), pp. 6-7.

[54] Efficacemente sul punto E. Scaroina, *Giustizia penale e comunicazione nell'era di* Twitter, cit., 2. Sul tema v. anche M. Caterini, *Criminalità, politica e mass media*, in «*Politica del diritto*», 4, (2013), p. 601 ss., e A. Gullo, G. Piccirilli, *Disinformazione e politiche pubbliche: una introduzione*, in «Diritto penale contemporaneo - Rivista trimestrale», 4, (2021), p. 248 ss. Per un'ampia indagine si veda anche il volume di G. Pitruzzella, O. Pollicino, S. Quintarelli, *Parole e potere. Libertà di espressione, hate speech e fake news*, Egea, Milano, 2017, *passim*.

stata emblematica al riguardo la ormai risalente ma "storica" decisione del Comitato di controllo di Facebook di qualche anno fa sulla sospensione dell'account di Donald Trump[55]).

Infatti, il rischio di un esercizio non prudente di tale potere, o di un suo utilizzo non rispondente alla miglior cura dell'interesse collettivo, evidentemente è dietro l'angolo, unitamente al pericolo di uso di tali potestà punitive per censurare il libero confronto democratico.

Perché è vero che, come osservavamo all'inizio[56], della collaborazione di questi operatori non si può far a meno nel contrasto ai fenomeni di cui ci occupiamo, ma è altrettanto corretto rilevare che bisognerebbe limitare adeguatamente questo potere, imbrigliarlo entro confini ben definiti da una più precisa cornice di regole pubblicistiche, così da renderlo prevedibile nel suo esercizio e adeguatamente controllabile anche in sede di monitoraggio da parte di Stati membri e Commissione europea sul rispetto degli obblighi definiti dal regolamento.

L'impressione, infatti, avuto riguardo a molti contenuti del regolamento, è quella di essere di fronte a una *delega in bianco* operata dal decisore pubblico nei confronti di quello privato, che, oltre ai già menzionati rischi di uso indebito di tale potere, comporta anche quello di "lasciare soli" questi operatori, nel senso di demandargli, senza indicazioni chiare, puntuali e determinate, lo svolgimento di un bilanciamento molto complesso tra tutti gli interessi in gioco[57].

Non è un caso, del resto, che le politiche dei *social* principali come X e Meta differiscano storicamente su molti punti di non poca importanza proprio in tema di contrasto alla disinformazione[58]. Così come è significato evidenziare come Meta abbia deciso, nell'aprile del 2025, dopo l'elezione del Presidente Trump, di concludere il suo *third-party fact checking program* negli Stati Uniti[59], a ulteriore testimonianza della delicatezza e della natura eminentemente politica di questo potere di autonormazione.

La Commissione europea, ad ogni modo, può emanare degli orientamenti per supportare ulteriormente, e con indicazioni aggiuntive molto concrete e di dettaglio, gli operatori privati in questa attività di autonormazione, autoorganizzazione e *self-enforcement*.

In effetti, per esempio, ad aprile del 2024 la Commissione ha emanato degli orientamenti per l'attenuazione dei rischi sistemici correlati proprio ai processi elettorali[60].

[55] Un riepilogo del caso e della decisione adottata dal Comitato può leggersi al seguente link: urly.it/319fw3.

[56] V. *supra* par. 2 per tutti i riferimenti.

[57] Sia consentito, per ulteriori riferimenti, rinviare ancora a E. BIRRITTERI, *Contrasto alla disinformazione,* Digital Services Act, cit., p. 77.

[58] Per una ricostruzione, volendo v. E. BIRRITTERI, *Punire la disinformazione*, cit., p. 311 ss.

[59] Per il relativo comunicato ufficiale e ulteriori dettagli v.: https://about.fb.com/news/2025/03/testing-begins-community-notes-facebook-instagram-threads/.

[60] Si tratta della Comunicazione C/2024/3014 della Commissione europea recante "Orientamenti della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35,

Si tratta di un documento che contiene indicazioni molto utili e di dettaglio per gli operatori, nella logica della *partnership* pubblico-privato che è come noto la cifra della compliance.

Vi sono indicazioni puntuali, ad esempio: sul tema della gestione della pubblicità politica (oggetto, peraltro, di un nuovo regolamento europeo); sull'opportunità per le piattaforme, durante i periodi elettorali, di costruire squadre interne *ad hoc* chiaramente identificabili per il monitoraggio dei rischi di disinformazione e manipolazione del consenso, facendo attenzione a inserire nel *team* personale che conosca le dinamiche locali; sulla necessità di promuovere iniziative di alfabetizzazione mediatica degli utenti; sulla collaborazione con *fact-checker* indipendenti; sull'uso di etichette chiare apposte ai *post* potenzialmente problematici sul piano della disinformazione per favorire la verifica autonoma dei fatti da parte dei singoli anche tramite il rinvio a informazioni ufficiali, per esempio, sui requisiti di accesso al voto, o di *flag* che rendano identificabili chiaramente i c.d. *deep fake*.

Negli orientamenti si menziona anche l'interessante possibilità per l'operatore di richiedere alla commissione una verifica *ex ante* dell'adeguatezza del proprio sistema di gestione dei rischi, secondo modelli di compliance cooperativa *ex ante* sperimentati ampiamente anche in altri ambiti come quello fiscale, ad esempio[61].

Quando però, rispetto alle garanzie individuali, si passa al punto più delicato che è quello della tutela dei diritti fondamentali, a parte la consueta clausola generale dell'obbligo di rispettarli nel definire tali *policy* si trova ben poco, come del resto accade nel testo del regolamento. Su questo punto gli orientamenti si soffermano per poche righe in un documento di ben 19 pagine[62].

Viene data molta attenzione, allora, all'efficacia dell'*enforcement* e forse non altrettanta al supporto agli operatori nello strutturare dei sistemi di moderazione dei contenuti degli utenti che non si risolvano in censure illegittime.

La scelta di *policy* qui fatta propria dal decisore eurounitario ci pare presenti aspetti positivi e criticità.

Da un lato, invero, introdurre specifiche procedure di dettaglio sul piano della moderazione dei contenuti e dei reclami, valide per qualsiasi prestatore di servizi intermediari a prescindere dallo specifico mercato di riferimento, dal tipo di attività, dalla dimensione, secondo un modello *one size fits all*, sarebbe stato molto rischioso e, forse, controproducente, con il rischio di imporre oneri eccessivamente gravosi.

Dall'altro lato, però, pur senza legittimare inutili irrigidimenti burocratici, sarebbe stato a nostro avviso utile aggiungere qualche specificazione in più in merito ai "diritti di garanzia" minimali dell'utente sul piano delle misure che la piattaforma può

paragrafo 3, del regolamento (UE) 2022/2065", il cui testo è reperibile al seguente link: urly.it/319fw6.

[61] V., anche per tutti i relativi riferimenti e per un'ampia panoramica sulle tecniche di *cooperative compliance*, A. Gullo, Compliance, in «Archivio penale», 1 (2023), p. 4 ss. V. altresì ampiamente V. Mongillo, *Presente e futuro della* compliance *penale*, in «Sistema penale», 11 gennaio 2022, p. 8 ss.

[62] Cfr. p. 11 degli orientamenti citati *supra* (nota n. 60).

disciplinare e adottare incidendo sui suoi diritti fondamentali (su tutti, dalla nostra prospettiva, la libertà di espressione).

Ad es., *ex multis*, il principio di "legalità" in punto di definizione delle misure sanzionatorie e interdittive con i relativi corollari dell'irretroattività, della tassatività e della precisione delle previsioni punitive; il divieto di analogia; la chiara definizione dei soggetti con potestà di adottare tali regole; la proporzionalità del trattamento sanzionatorio; il divieto di responsabilità oggettiva e il principio di "colpevolezza", specificando l'elemento soggettivo necessario per integrare la violazione[63].

Del resto, sul piano dell'obbligo di motivazione in sede di adozione di misure di moderazione dei contenuti, l'art. 17 del DSA appare più sensibile alle esigenze sia di dettagliare maggiormente, e non solo con clausole di carattere generale, gli obblighi degli operatori, sia di rafforzare e specificare con più analiticità i diritti e le garanzie procedurali minime per gli utenti che subiscono simili misure para-punitive. L'ampiezza dell'obbligo motivazionale imposto da tale articolo del regolamento ai soggetti regolati, infatti, pur ponendo in capo ad essi significativi oneri gestionali e organizzativi, appare una soluzione necessaria in considerazione dei diritti fondamentali su cui simili attività possono significativamente incidere, fornendo una base di "informazioni di partenza" indispensabile per l'utente che voglia avvalersi degli strumenti di reclamo effettivamente disponibili a tutela della sua posizione, anche in considerazione del significativo squilibrio di "potere contrattuale" tra utente e piattaforma[64], per quanto pure rispetto ai meccanismi di ricorso "interni" il DSA sembri di nuovo lasciare agli operatori privati ampia potestà di disciplinarli nel modo ritenuto più opportuno[65].

5. *Considerazioni di sintesi*

Cerchiamo di compendiare in alcune battute finali gli aspetti principali emersi nel corso della disamina fin qui svolta.

Affidarsi alla risposta penalistica nel contrasto alla disinformazione in rete (anche in punto di manipolazione del consenso elettorale) presenta più controindicazioni che vantaggi.

Ciò non solo per le problematiche in punto di legittimazione, al metro della Costituzione e dei principi penalistici fondamentali, dell'eventuale criminalizzazione delle condotte di mera diffusione di notizie false, ma anche perché, come si è prima osservato,

[63] Sul punto si consenta il rinvio a E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act, cit., p. 85.

[64] Sul problema dell''asimmetria delle posizioni' degli attori qui in campo v. B. Carotti, *La politica europea sul digitale: ancora molto rumore*, in «Rivista trimestrale di diritto pubblico», 4 (2022), p. 998. Diffusamente cfr. anche G. Alpa, *Sul potere contrattuale delle piattaforme digitali*, in «Contratto e impresa», 3 (2022), p. 721 ss.

[65] Su tale dibattito v. anche F. G'sell, *The Digital Services Act: A General Assessment*, in *Content Regulation in the European Union. The Digital Services Act*, a cura di A. von Ungern-Sternberg, IRDT, Trier, 2023, p. 95, e V. Zeno-Zencovich, *The EU regulation of speech. A critical view*, in «Rivista di Diritto dei Media», 1 (2023), p. 14.

una risposta che si affidi al solo diritto penale, o in generale esclusivamente pubblica, potrebbe risultare lenta, incompleta e inefficace rispetto a un fenomeno che reclama a monte ben altre e più articolate misure di contrasto.

Occorre quindi costruire strategie alternative, coinvolgendo proattivamente gli operatori del settore privato, poiché quest'ultimi hanno le capacità organizzative, tecniche, economiche e il "potere contrattuale" per porre un argine efficace contro il dilagare di informazioni false in rete e per salvaguardare, quindi, gli interessi di rilievo anche pubblicistico in gioco[66] (nel nostro caso, l'integrità del dibattito civico e dei processi elettorali).

Ed è invero proprio questa la scelta compiuta dal legislatore europeo con il DSA, che ha costruito un articolato sistema di *enforcement* imperniato sulla partnership pubblico-privato, ponendo significativi obblighi di compliance in capo agli operatori del settore privato e specie a quelli di grandi dimensioni.

Si tratta certamente di un significativo e molto positivo passo avanti rispetto alla situazione precedente all'emanazione del nuovo regolamento, in cui mancava del tutto una cornice regolamentare pubblicistica volta a fornire una indispensabile piattaforma di regole pubbliche per disciplinare dei poteri che, pur esercitati in ambito privato, sono in grado di influire sui diritti fondamentali degli utenti, come si è cercato ampiamente di dimostrare[67].

Rimangono però talune perplessità sulle scelte di fondo compiute dal DSA, specie sul piano dei limiti ai poteri regolamentari (e para-punitivi) delle piattaforme e sulla più efficace tutela dei diritti degli utenti su cui tale *ius puniendi* privato è in grado di incidere talvolta anche in modo molto significativo.

Sul primo aspetto, si è detto che Il DSA menziona soltanto le macro-tipologie di misure che le piattaforme possono (e non per forza devono) autonormare e adottare al fine di gestire e mitigare i rischi sistemici connessi all'impatto dei loro servizi sui diritti fondamentali e sugli interessi individuali e collettivi in gioco, compresa l'integrità dei processi elettorali e il dibattito civico, essendo il legislatore europeo, in tutti gli articoli del regolamento, ben attento a non imporre agli operatori scelte di merito e modelli "preconfezionati".

[66] V. ampiamente P. Severino, voce *Disinformazione*, in *Studi in onore di Carlo Enrico Paliero*, a cura di G. Mannozzi, C. Perini, F. Consulich, C. Piergallini, M. Scoletta, C. Sotis, Giuffrè, Milano, 2022, p. 1373 ss. Per una *overview* dei vari approcci in materia v. già O. Pollicino, *The European approach to disinformation: comparing supranational and national measures*, in «Annuario di diritto comparato e di studi legislativi», 1 (2020), p. 175 ss. In generale, su queste dinamiche v. altresì: C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in «Quaderni costituzionali», 3 (2023), p. 543 ss.; A. Simoncini, *La co-regolazione delle piattaforme digitali*, in «Rivista trimestrale di diritto pubblico», 4 (2022), p. 1031 ss.; G.E. Vigevani, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in «Diritto costituzionale», 1 (2023), p. 41 ss.

[67] Ampiamente in argomento v. R. Ò Fathaigh, N. Helberger, N. Appelman, *The perils of legally defining disinformation*, in «Internet Policy Review», 10/4 (2021), p. 2 ss. In argomento v. anche P. Church, C.N. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in «*Global Privacy Law Review*», 4(1), (2023), p. 53 ss.

Se a guadagnarne è la flessibilità di questa regolazione e la possibilità che ciascun sistema di *risk assessment* e *management* venga adattato alle peculiarità di ciascuna organizzazione in una pura logica *taylor made*, il rischio è quello di una delega in bianco al settore privato.

Un mandato potenzialmente pericoloso per almeno due principali ragioni.

La prima è che tali attori vengono qui chiamati a operare complessissimi bilanciamenti tra interessi (anche fondamentali) contrapposti in assenza di più dettagliate indicazioni da parte del decisore pubblico. Nel nostro caso, avuto riguardo alla disinformazione nei contesti elettorali, si tratta invero di ricercare un difficile punto di equilibrio tra protezione dell'integrità del dibattito civico e dei processi elettorali e libertà di espressione degli utenti.

La seconda è il rischio di un esercizio non prudente di tale potere, o di un suo utilizzo non rispondente alla miglior cura dell'interesse collettivo, unitamente alla possibilità che tali potestà punitive vengano utilizzate per censurare il libero confronto democratico. E ciò sempre per le medesime ragioni correlate ai significativi margini di apprezzamento che il regolamento attribuisce ai soggetti regolati sul piano delle scelte di merito circa la costruzione delle loro *policy* interne, anche per ciò che riguarda il contrasto alla disinformazione elettorale.

Rispetto alle garanzie e ai diritti di difesa dei destinatari del servizio, si è osservato come il DSA sia piuttosto timido e, a parte le clausole generali dell'obbligo di fissare le condizioni d'uso «nel rispetto dei diritti fondamentali degli utenti», aggiunga ben poco su come in concreto si possa conciliare tale attività di *digital patrolling* con questi interessi, visto il rischio di censure e *chilling effect* che tale *enforcement* può produrre rispetto al libero confronto democratico e al *free speech*.

A fronte dell'indubbio miglioramento della legislazione in materia, quindi, le indicate questioni "aperte" potrebbero reclamare un ulteriore affinamento di queste strategie di regolazione, al fine di assicurare un equilibrio più armonico rispetto a meccanismi di contrasto a fenomeni che destano preoccupazione per la tenuta delle democrazie, ma che non possono legittimare ingiustificate compressioni di diritti e interessi di rango primario, che parimenti vanno posti al riparo dalle possibili conseguenze negative di simili dinamiche della nuova società digitale.

Gli spunti per riflettere sulle ulteriori, possibili prospettive evolutive, nel dibattito pubblico e accademico, sono molti.

Quel che è certo è che i penalisti e gli studiosi del diritto punitivo devono rimanere vigili e spingersi al di là della loro *comfort zone* per occuparsi anche di temi, come quello dei 'poteri punitivi' privati delle grandi piattaforme, all'apparenza lontani dal loro ambito d'elezione, ma dove la posta in gioco, in punto di salvaguardia dell'individuo e dei suoi *fundamental right*, è di importanza talvolta ben parificabile a quella della dimensione tradizionale della penalità.

Così come accade dinnanzi allo *ius puniendi* statale, invero, anche nel settore esaminato abbiamo osservato come venga in rilievo l'esigenza di limitare adeguatamente il

potere para-sanzionatorio dei grandi *player* del mercato digitale, di imbrigliarlo entro confini ben definiti da una più precisa cornice di regole pubblicistiche, così da renderlo prevedibile nel suo esercizio e adeguatamente controllabile tramite i meccanismi istituzionali previsti dal nuovo assetto di disciplina.

SEZIONE 2

OFFESE ALLA PERSONA E CONTESTI DIGITALI: NUOVE PROSPETTIVE

PARTE 1

CONTENUTI SESSUALI ILLECITI E MOLESTIE DIGITALI

CONTENUTO ILLECITO ONLINE E PEDO-PORNOGRAFIA. AMBIGUITÀ INTERPRETATIVE TRA PRODUZIONE ABUSIVA, *SEXTING* E CONDOTTE DIFFUSIVE

Malaika Bianchi

1. *Il riferimento alla "pornografia minorile" nella definizione di "contenuto illecito"*

Il nuovo Reg. UE 2022/ 2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali, sebbene contenga una definizione piuttosto ambigua di "contenuto illecito", richiama esplicitamente in più punti, fra le macroaree di intervento, la "pornografia minorile"[1]. Quando affronta i rischi connessi alla diffusione di contenuti illeciti, cita, a titolo esemplificativo, la circolazione di materiale pedopornografico[2], facendo altresì riferimento alla condivisione di immagini raffiguranti abusi sessuali su minori[3]. Occorre fin da ora premettere che, tuttavia, l'oggetto materiale dei delitti di pedo-pedopornografia non è circoscritto alle immagini raffiguranti abusi sessuali su minori. Il riferimento esplicito a tali contenuti semplifica, pertanto, solo apparentemente il compito dell'*internet provider*, poiché, in realtà, il quadro normativo nazionale in materia di produzione e diffusione di pornografia minorile (art. 600-*ter* c.p.) risulta tutt'altro che chiaro. Più precisamente, esso è stato talmente svuotato e, al contempo, ampliato di contenuti dalla giurisprudenza degli ultimi quindici anni, da rendere la sua attuale portata applicativa in parte non aderente al tenore letterale della disposizione.

[1] Considerando n. 64, ove fa riferimento a "contenuti manifestamente illegali connessi a reati gravi, come il materiale pedopornografico"; considerando n. 119, ove fa riferimento alla "rimozione delle pagine web che contengono o diffondono materiale pedopornografico"

[2] Considerando n. 80, ove fa riferimento ai "i rischi associati alla diffusione di contenuti illegali, quale la diffusione di materiale pedopornografico";

[3] Considerando n. 12, che richiama, fra le attività illegali, la "condivisione di immagini che ritraggono abusi sessuali su minori".

Occorre considerare che ci troviamo dinanzi a una norma, introdotta nel codice penale nel 1998[4], concepita originariamente per contrastare la mercificazione, nei circuiti pedofili, di immagini che immortalavano lo sfruttamento sessuale di minori. Tuttavia, nel corso degli ultimi quindici anni, essa è stata chiamata dalla giurisprudenza a disciplinare anche un fenomeno ulteriore e diverso rispetto a quello del mercato pedofilo, ossia la prassi, diffusa in particolare tra gli adolescenti, di realizzare e condividere, mediante strumenti informatici, immagini a contenuto sessuale auto-prodotte o comunque realizzate con il loro consenso nell'ambito di un contesto relazionale, quale nuova pratica di approccio alla sessualità. Faccio riferimento all'ormai noto fenomeno del c.d. "*sexting*", neologismo di origine inglese che deriva dalla congiunzione di "*sex*" (sesso) e "*texting*" (invio di messaggi)[5], e che individua, per quanto qui interessa, la pratica di inviare o postare immagini sessualmente suggestive attraverso il cellulare o internet[6]. Accade non di rado, tuttavia, che, in un secondo momento, queste immagini vengano messe in circolazione nelle *chat* degli amici o conoscenti, o pubblicate sui *social network*, o diffuse in rete. E nel momento in cui le immagini fuoriescono dalla sfera di controllo del soggetto che le ha prodotte e accedono all'ambiente sconfinato della rete, esse si confondo e si mescolano; vengono percepite dall'esterno indistintamente come immagini sessualmente connotate di minorenni e assimilate nella generica e onnicomprensiva categoria della pornografia minorile[7].

Gli interrogativi a cui la giurisprudenza ha cercato di rispondere in seguito all'emersione di questo fenomeno sono stati molteplici. I minori godono di una sfera di autodeterminazione nella gestione della propria immagine sessuale? Così come possono liberamente compiere atti sessuali dopo il compimento dei quattordici anni, possono altrettanto liberamente manifestare la propria sessualità attraverso le immagini, acconsentendo alla loro produzione, auto-producendole, condividendole? E, di conseguenza, chi interagisce con il minore è penalmente responsabile oppure no? È indifferente che il produttore sia un minore oppure un adulto? Il minore può diffondere la propria immagine sessuale? Ancora, il minore può acconsentire a che un altro soggetto la diffonda?

A talune di queste domande è stata data risposta, ad altre, invece, non ancora. Intendo pertanto ripercorrere sinteticamente i più recenti approdi giurisprudenziali, al fine di illustrare gli spazi di liceità o di non punibilità che la giurisprudenza ha delineato

[4] Legge n. 269/1998, recante "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù", nota anche come "Legge antipedofilia" (v., fra i primi commenti, V. Patalano, *Il Ddl anti-pedofilia cerca il consenso ma «chiede troppo» al diritto penale*, in «Guida al diritto», 27 (1998), pp. 9 ss.

[5] M.R. Parker, *Kids these Days: Teenage Sexting and how the Law shoud deal with it*, 2.9.2009, consultabile nel sito http://works.bepress.com/michael_ parker/1/.

[6] C. Calvert, *Sex, Cell Phones, Privacy, and the First Amendment: When Children Become Child Pornographers and the Lolita Effect Undermines the Law*, in «18 Commlaw Conspectus», 1, 2009, p. 30.

[7] V.E. Quayle, C. Gören Svedin, L. Jonsson, *Children in identified sexual images – who are they?: Self and non-self-taken images in the International Child Sexual Exploitation image database (ICSE DB) 2006-15*, in «Child Abuse Review» (2018).

in questo contesto, mettendo in luce i numerosi profili di criticità che caratterizzano l'impostazione attuale.

2. *L'impervio precorso giurisprudenziale*

Come è noto, l'art. 600-*ter* c.p. (pornografia minorile) contempla condotte ordinate secondo una prospettiva scalare, da quella punita più severamente a quella punita meno severamente (produzione, commercio, distribuzione, divulgazione, diffusione, pubblicizzazione, offerta e cessione).

La norma prevede, all'ultimo comma, una definizione di pornografia minorile, ossia: "ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali". Non è, pertanto, richiesta la rappresentazione di un atto di abuso sessuale: l'immagine può consistere, come riconosciuto in alcune pronunce giurisprudenziali, anche in una mera raffigurazione statica della nudità o di parti erogene, quali il seno o i glutei, del minore[8].

La norma, inoltre, non distingue, a differenza del delitto di atti sessuali con minorenne (art. 609-*quater* c.p.), in relazione all'età del minore (infraquattordicenni, infrasedicenni, infradiciottenni), né prevede una causa di esclusione della punibilità nei casi in cui il materiale sia prodotto da minori e tra minori. Diversamente, altri ordinamenti, come quello tedesco e quello austriaco[9], hanno introdotto esplicite cause di non punibilità per la produzione di materiale intimo in un contesto consensuale, recependo quanto indicato dai documenti sovranazionali di riferimento[10], che riservano agli Stati membri un margine di discrezionalità nell'escludere dal perimetro dei reati di produzione e detenzione pornografia minorile ipotesi in cui le immagini siano realizzate senza abuso del minore, che abbia raggiunto l'età del consenso sessuale, con il suo consenso e per uso personale delle persone coinvolte. Il fatto che alcuni ordinamenti abbiano diversificato legislativamente tali ipotesi evidenzia come l'intera materia, sebbene sia disciplinata da una Direttiva europea, presenti notevoli differenze nelle normative interne, circostanza che può ostacolare un'applicazione omogenea del regolamento in questo ambito.

[8] Cfr. Cass., Sez. III, 8.1.2020, n. 9354; Cass., Sez. III, 19.10.2021, n. 6302; Cass., Sez. III, 20.12.2022, n. 16134.

[9] V., per la disciplina in Germania, l § 184c StGBe; per la disciplina in Austria, § 207a StGB. Sul punto v. D. Rosani, *The Increasing Recognition of Child Rights by European Constitutions and its Relevance for the Criminal Regulation of Sexting*, in «European Yearbook on Human Rights» (2020), pp. 349 ss.

[10] Decisione quadro 2004/68/GAI; Direttiva 2011/93/UE; Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale del 25 ottobre 2007, cd. Convenzione di Lanzarote.

2.1. *La non punibilità della produzione di pedo-pornografia domestica*

In questo rigido assetto normativo si è inserita la giurisprudenza, nel tentativo di individuare un punto di equilibrio tra l'esigenza di un intervento paternalistico volto a tutelare tutti i minori, presunti indistintamente incapaci di cogliere i rischi connessi alla condivisione della propria immagine sessualmente connotata, e il riconoscimento di uno spazio di autonomia sessuale del minore, coerente con le modalità attuali attraverso cui gli adolescenti instaurano relazioni ed esprimono la loro sessualità.

Nel corso degli ultimi quindici anni si è progressivamente sviluppato un orientamento giurisprudenziale volto a riconoscere, seppur con molti limiti, un qualche rilievo alla volontà del minore all'interno di tale contesto, attraverso la valorizzazione del presupposto normativo dell'"utilizzazione" del minore nella produzione del materiale pedopornografico, previsto dal primo comma dell'art. 600-*ter* c.p., secondo cui il materiale deve appunto essere prodotto "utilizzando un minore degli anni diciotto". In tale prospettiva, si è cominciato ad affermare che il consenso del minore ultraquattordicenne alla produzione del materiale possa, al ricorrere di specifiche e circoscritte condizioni, escludere l'"utilizzazione" penalmente rilevante, con conseguente insussistenza del reato di produzione di pornografia minorile. In questo quadro, è significativa la pronuncia del GIP del Tribunale di Firenze, che già nel 2015, sempre in un caso di produzione di immagini a contenuto sessuale di una diciassettenne da parte del fidanzato maggiorenne, affermava che ritenere che il consenso, validamente prestato, "non abbia alcun valore nella valutazione del caso concreto, potrebbe in ipotesi limitare fortemente quella stessa libertà sessuale, e le relative manifestazioni della stessa, che l'ordinamento invece vuole riconoscere"[11].

È stato però un fondamentale *obiter dictum*, contenuto in una pronuncia della Corte di Cassazione a Sezioni Unite di qualche anno successivo, a creare uno spazio più definito di non punibilità[12]. La Corte introduce, in poche ma dense pagine, il tema della "pornografia domestica", ossia la «condotta di chi realizza materiale pornografico in cui sono coinvolti minori che abbiano raggiunto l'età del consenso sessuale nei casi in cui tale materiale è prodotto e posseduto con il consenso di tali minori e unicamente a uso privato delle persone coinvolte» e afferma, esplicitamente, l'opportunità di valorizzare il dato dell'appartenenza di tali condotte all'ambito "dell'autonomia privata sessuale" per evitare «"ipercriminalizzazioni" non coerenti con le finalità proprie

[11] Trib. Firenze, 27.1.2015 (dep. 10.2.2015), n. 163, G.I.P., 22, in *archiviodpc.dirittopenaleuomo.org*, 22.4.2015 con nota di A. Verza, *Sulla struttura speculare e opposta di due modelli di abuso pedopornografico. Considerazioni sociologiche e giuridiche a margine di una recente sentenza in materia*.

[12] Cass. pen., Sez. un., 31.5.2018, n. 51815 (su questa pronuncia cfr., L. Picotti, *La pedo-pornografia nel Cyberspace: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa*, in «Diritto di Internet», 1 (2019), pp. 187-192; D. Rosani, «*Send nudes*». *Il trattamento penalistico del sexting in considerazione dei diritti fondamentali del minore d'età*, in «Dir. pen. cont.», 2 (2019), pp. 9-32; M. Bianchi, *Produzione di materiale pedo-pornografico: il nuovo principio di diritto delle Sezioni unite*, in «Arch. pen.», 1 (2019), pp. 1-25).

del diritto penale». Anche in quella sede, si attribuisce rilievo all'imprescindibile presupposto della "utilizzazione del minore", enfatizzandone la portata dispregiativa, in quanto espressiva di una vera a propria "strumentalizzazione" del minore stesso, di una sua trasformazione in strumento per il soddisfacimento di desideri sessuali altrui o per il conseguimento di utilità di vario genere: condotta, questa, che rende invalido anche un eventuale consenso del minorenne. Dalla centralità del requisito dell'utilizzazione del minore deriva che la portata applicativa del reato di produzione di pedo-pornografia sia circoscritta alla produzione "abusiva", ossia quella che si caratterizza o per la posizione di supremazia rivestita dal soggetto agente nei confronti del minore, o per le modalità con le quali il materiale pornografico viene realizzato (ad esempio, con minaccia, violenza, inganno), o per il fine commerciale che sottende la produzione, o per l'età dei minori coinvolti, qualora questa sia inferiore a quella del consenso sessuale[13]. Al contrario "qualora le immagini o i video abbiano per oggetto la vita privata sessuale nell'ambito di un rapporto che, valutate le circostanze del caso, non sia caratterizzato da condizionamenti derivanti dalla posizione dell'autore, ma siano frutto di una libera scelta – come avviene, per esempio, nell'ambito di una relazione paritaria tra minorenni ultraquattordicenni – e siano destinate ad un uso strettamente privato, dovrà essere esclusa la ricorrenza di quella "utilizzazione"". Irrilevante per la Corte, in sintesi, la mancata introduzione, da parte del legislatore, di specifiche cause di esclusione della punibilità in questo contesto, in quanto – da un lato – sarebbe lo stesso concetto di 'utilizzazione' del minore a delimitare l'ambito del penalmente rilevante e – dall'altro – l'estensione del rigoroso trattamento sanzionatorio previsto, sia con riguardo alle pene principali sia alle pene accessorie, anche a tali ipotesi di pornografia minorile non abusiva, si porrebbe in contrasto con il principio costituzionale di ragionevolezza.

2.2. *Ancora sul concetto di "utilizzazione" del minore quale criterio guida per il giudice. La punibilità "senza condizioni" della diffusione di pedo-pornografia domestica*

Questa ricostruzione interpretativa, introdotta in via incidentale dalla Corte, ha lasciato aperti tuttavia molti interrogativi. È davvero ipotizzabile che il minore possa esprimere un consenso validamente rilevante alla produzione di tale materiale in assenza di un esplicito fondamento normativo? Nel caso in cui il produttore non sia un minore, bensì un adulto, si ricadrebbe comunque nell'ambito della cosiddetta pedopornografia domestica, con conseguente insussistenza del reato? E qualora tali immagini vengano successivamente divulgate, può ritenersi integrata la fattispecie di cui all'art. 600-*ter*, comma 3, c.p.; oppure l'assenza del requisito dell'"utilizzazione" del minore – che esclude la punibilità nella cd. pornografia domestica – si estenderebbe anche alla successiva diffusione del medesimo materiale? Infine, come qualificare la condotta del

[13] Questa lettura interpretativa era stata suggerita anche in dottrina, nell'attesa di una presa di posizione del legislatore. Si consenta di rinviare a M. Bianchi, *I confini della repressione penale della pornografia minorile. La tutela dell'immagine sessuale del minore fra esigenze di protezione e istanze di autonomia*, Torino, 2019, pp. 541 ss.

minore che diffonde egli stesso immagini a contenuto sessuale che lo ritraggono, siano esse auto-prodotte o realizzate da terzi?

Ad alcuni di questi interrogativi ha risposto la Corte di Cassazione, nella medesima composizione, pochi anni dopo[14]. In breve, i fatti: un trentenne e una quindicenne si frequentano per circa un anno, durante il quale realizzano consensualmente immagini e video dei loro rapporti sessuali. Al termine della relazione sentimentale, l'uomo invia le immagini al nuovo partner della ragazza, decisione che, secondo le dichiarazioni rilasciate dalla minorenne, sarebbe stata da lei stessa espressamente condivisa (al fine di "mettere alla prova" il nuovo partner).

La Corte ribadisce la atipicità della produzione di pedo-pornografia domestica rispetto alla fattispecie di cui al primo comma dell'art. 600-*ter* c.p., confermando l'interpretazione secondo la quale il discrimine fra il penalmente rilevante e il penalmente irrilevante risiede nella sussistenza o meno dell'utilizzazione del minore per la realizzazione del materiale e che in presenza di tale strumentalizzazione nessun valore scriminante può essere riconosciuto al consenso eventualmente prestato dal minore. In ogni caso, il giudice è chiamato a svolgere un accertamento puntuale e rigoroso del contesto in cui tale consenso è stato manifestato, al fine di verificarne l'effettiva libertà da condizionamenti illeciti. Diventa, pertanto, centrale l'individuazione dei criteri qualificanti l'"utilizzazione" del minore e di conseguenza i limiti della validità del suo consenso alla produzione di immagini che lo ritraggono in un contesto sessualmente connotato. In assenza di indicazioni legislative, il Collegio, in un'ottica di sistema, individua un primo parallelismo con la disciplina prevista per gli atti sessuali con minorenne (art. 609-*quater* c.p.). Quest'ultima norma si presterebbe a fungere da punto di riferimento poiché, dopo il rinvio all'art. 609-*bis* c.p. (applicabile nei casi di consenso viziato da costrizione), contempla ulteriori ipotesi in cui deve essere esclusa la validità del consenso prestato dal minore all'atto sessuale, che bene si attagliano anche al consenso eventualmente espresso alla rappresentazione della propria attività sessuale. Non sarebbe dunque valido il consenso del minore che non abbia compiuto quattordici anni; del minore infrasedicenne, in presenza dei particolari rapporti intercorrenti con l'agente (parentela, convivenza, tutela, affidamento per ragioni di cura, educazione, istruzione, vigilanza o custodia); del minore ultrasedicenne, qualora l'agente abbia abusato dei poteri connessi alla propria posizione, sempre nell'ambito di rapporti di parentela, convivenza, educazione, ecc.; in tutti i casi in cui ricorrano le ulteriori condotte di abuso di fiducia, di autorità o influenza in ragione della qualità dell'agente o dell'ufficio ricoperto o delle relazioni familiari, domestiche, lavorative, di coabitazione o di ospitalità indicate nell'art. 609-*quater* c.p.

[14] Cass., Sez. un., 9 febbraio 2022, n. 4616. Per i commenti alla sentenza si rinvia a S. Bernardi, *Le Sezioni unite chiariscono i limiti della (ir)rilevanza della "pedopornografia domestica" ai sensi dell'art. 600-*ter *c.p.*, in *www.sistemapenale.it*, 25 febbraio 2022; D. Rosani, *L'introduzione giurisprudenziale di una clausola di non punibilità per la "pornografia minorile domestica": pensieri critici*, in *www.sistemapenale.it*, 15 aprile 2022; N. Recchia, *Pregevoli approdi e persistenti criticità nella sentenza delle Sezioni unite sul* sexting, in «Giur. it.» (2022), pp. 1470 ss.

Attraverso un confronto con la fattispecie di prostituzione minorile, di cui all'art. 600-*bis* c.p., la Corte estende poi l'elenco delle ipotesi in cui la volontà del minore non può ritenersi libera da condizionamenti, includendovi anche la dazione o la promessa di denaro quale corrispettivo per l'attività di ripresa o registrazione di immagini a contenuto sessuale, nonché l'approfittamento delle condizioni economiche del minore.

Sulla base di quanto già sostenuto dalle sezioni semplici della Corte di Cassazione[15], il Collegio sottolinea, inoltre, che anche l'istigazione e l'induzione all'auto-produzione delle immagini rientra nel perimetro del reato di cui all'art. 600-*ter*, comma 1, n. 1, c.p.: in altre parole, configura il reato di produzione di pornografia minorile anche la condotta consistente nell'indurre ("quell'attività, coscientemente finalizzata, di persuasione, di convincimento, di determinazione, di eccitamento, di rafforzamento della decisione"[16]) il minore a farsi un autoscatto pedo-pornografico e inviarlo all'agente.

Nel dare indicazioni ai giudici chiamati a verificare la sussistenza o meno dell'"utilizzazione" del minore, la Corte valorizza sia il grado di maturità del minore vittima, sia l'età adulta o meno dell'autore. Si distingue fra vittime infra-sedicenni e ultra-sedicenni, precisando che per le prime è richiesta "un'attenta valutazione in ordine all'abuso del rapporto di fiducia da parte dell'adulto (…) ed alle modalità di convincimento cui lo stesso ha fatto ricorso, parametrando le pressioni e l'insidiosità degli artifici necessari a vincere la resistenza psicologica del minore alla sua limitata capacità di cogliere le situazioni per sé svantaggiose»[17]. Il discorso è diverso, afferma la Corte, quando l'autore è un minorenne, laddove, nel rapporto fra pari, l'accertamento della condizione di "utilizzazione" richiede il "confronto con un contesto necessariamente più fluido, fatto di rapporti più difficilmente inquadrabili", in cui la condotta può essere mossa da motivazioni diverse rispetto a quelle riscontrabili nei rapporti asimmetrici adulto-minore, quali, per esempio, l'esibizionismo o la vanteria; inoltre, in ragione della prossimità anagrafica tra soggetti coinvolti, viene meno la presenza di una figura di riferimento caratterizzata da una posizione di prevalenza o supremazia.

La corte giunge così al primo principio di diritto, secondo il quale «si ha "utilizzazione" del minore allorquando, all'esito di un accertamento complessivo che tenga conto del contesto di riferimento, dell'età, maturità, esperienza, stato di dipendenza del minore, si appalesino forme di coercizione o di condizionamento della volontà del minore stesso, restando escluse dalla rilevanza penale solo condotte realmente prive di offensività rispetto all'integrità psico-fisica dello stesso» (par. 8).

La seconda parte della pronuncia si focalizza sulle cosiddette condotte diffusive, analizzando in particolare il rapporto sistematico tra le fattispecie incriminatrici delineate ai

[15] V. Cass., Sez. III, 18.4.2019, n. 26862.

[16] La Corte richiama in questo passaggio la giurisprudenza formatasi sul reato di prostituzione minorile (Sez. Un. 19.12.2013, n. 16207).

[17] E questo anche qualora adulto e minore siano legati da una relazione affettiva, perché il primo potrebbe aver vinto le «resistenze del minore inducendolo a superare le proprie riluttanze tramite tecniche di manipolazione psicologica e di seduzione affettiva, sfruttando la superiorità in termini di età, esperienza, posizione sociale o la condizione di inferiorità del minore» (par. 5).

commi 2, 3 e 4 dell'art. 600-*ter* c.p. – concernenti la circolazione, diffusione e cessione di materiale pedopornografico – e il primo comma della medesima disposizione, cui tali previsioni normative operano espresso rinvio. Quest'ultimo pone un rilevante quesito interpretativo: tale richiamo deve intendersi come un generico rinvio alla pornografia minorile – così come definita dal settimo comma – oppure implica un riferimento specifico al materiale pornografico realizzato mediante l'utilizzazione del minore, quale elemento costitutivo del reato descritto al primo comma? Il problema, già emerso in precedenti pronunce con esiti non univoci, assume particolare rilievo al fine di chiarire se la messa in circolazione di materiale prodotto in assenza di utilizzazione del minore (c.d. pedopornografia domestica) possa integrare o meno le fattispecie incriminatrici di cui ai commi 2 e seguenti dell'art. 600-*ter* c.p.

La Corte, seguendo l'adagio delle sezioni semplici (Cass., Sez. III, 21.11.2019, n. 5522) afferma che i commi 2, 3 e 4 dell'art. 600-*ter* c.p., nel fare riferimento al 'materiale pornografico di cui al comma 1', non operano un rinvio al reato di produzione di pedo-pornografia, bensì si riferiscono esclusivamente al materiale pedopornografico, come definito al comma 7 della norma. Inoltre, aggiunge il Collegio, il presupposto necessario della "pornografia domestica" è che il materiale realizzato sia destinato a rimanere nella disponibilità esclusiva delle parti coinvolte nel rapporto. Se questo materiale viene messo in circolazione, il minore, anche se non "utilizzato" nella fase iniziale, deve essere ritenuto strumentalizzato nella fase di cessione o diffusione delle immagini. E l'eventuale consenso del minore alla diffusione della propria immagine è da ritenersi giuridicamente irrilevante, in quanto egli deve essere considerato, in via presuntiva, privo di un adeguato livello di maturità tale da consentirgli una valutazione pienamente consapevole delle potenziali implicazioni negative derivanti dalla mercificazione del proprio corpo attraverso la diffusione di proprie immagini erotiche.

L'argomentazione della Corte si basa anche sulla duplice natura del bene giuridico tutelato, che si configura, da un lato, come individuale – volto alla protezione dell'immagine, della dignità e dello sviluppo psico-fisico del singolo minore ritratto – e, dall'altro, come collettivo, concernente la salvaguardia di tutti i minori come gruppo sociale, ossia minori non direttamente coinvolti nella produzione e diffusione di quelle specifiche immagini. In questa seconda prospettiva, la criminalizzazione della circolazione del materiale pedopornografico assume dunque una funzione preventiva, volta a evitare la creazione di condizioni favorevoli a futuri abusi e fenomeni di sfruttamento sessuale di minorenni.

In questa cornice sistematica viene formulato il secondo principio di diritto: «La diffusione verso terzi del materiale pornografico realizzato con un minore degli anni diciotto integra il reato di cui all'art. 600-*ter* c.p., commi 3 e 4, e il minore non può prestare consenso ad essa».

È evidente il tentativo della Corte di individuare un punto di equilibrio tra la tutela dell'autodeterminazione sessuale del minore e la necessità di proteggerlo non solo da forme di coercizione o condizionamento della volontà (ossia dalla c.d. "produzione

abusiva"), ma anche dai rischi derivanti dall'acconsentire alla produzione e alla diffusione di proprie immagini a contenuto sessuale.

2.3. *E se è lo stesso minore a mettere in circolazione proprie immagini intime?*

Prima di pronunciare il secondo principio di diritto, si legge in un passaggio della motivazione molto discutibile che la responsabilità penale sarà in capo al minore se la circolazione del materiale è imputabile esclusivamente alla sua iniziativa. In poche e criptiche righe la Corte ha aperto un varco pericoloso. Una parte della dottrina non ha mancato di esprimere preoccupazione in ordine alla possibile configurazione della responsabilità per cessione di pedo-pornografia, ai sensi dell'art. 600-*ter*, comma 4, c.p., in capo al minore che condivida immagini a contenuto sessuale auto-prodotte nel contesto di una relazione affettiva. Tale ricostruzione rischia infatti di ricondurre il fenomeno del *sexting* nell'alveo della cessione di materiale pedopornografico penalmente rilevante, con evidenti criticità sul piano della coerenza sistematica e della proporzionalità[18]. Si aggiunga che il recente Report del Comitato di Lanzarote sul tema delle immagini pedo-pornografiche auto-prodotte non solo chiede agli stati di non perseguire il minore che condivida le proprie immagini o video sessuali con un altro minore qualora tale condivisione sia volontaria, consensuale e destinata esclusivamente all'uso privato reciproco (Raccomandazione II-8); ma precisa che, anche nel caso in cui il minore decida di distribuire (anche su larga scala) la propria immagine intima, il ricorso al diritto penale deve rappresentare una *extrema ratio* e deve essere data priorità a strumenti più appropriati, come a misure educative e terapeutiche[19].

3. *Quali immagini pedo-pornografiche costituiscono "contenuto illecito"?*

Dall'attuale ricostruzione interpretativa, che abbiamo tentato di sintetizzare in questo contributo, emerge sostanzialmente che qualunque immagine o video a contenuto sessuale ritraente un minore individua, ove messo in circolazione, un contenuto illecito, indipendentemente dalle modalità con cui è stato realizzato, ossia indipendentemente dalla tipologia di produzione che vi è a monte (abusiva, domestica, auto-produzione, etero-produzione).

[18] Cfr. M. Bianchi, *Per una tipizzazione della produzione e diffusione di "pedo-pornografia domestica"*, in «Arch. pen.», 1 (2023), p. 236; D. Rosani, *L'introduzione giurisprudenziale di una clausola di non punibilità per la pornografia minorile domestica: pensieri critici*, in «Sist. pen.», 1 (15.4.2022); S. Bernardi, *La "pornografia domestica" davanti alle Sezioni Unite: alcune riflessioni sulla libertà del minore di disporre della propria immagine sessuale*, in «Riv. it. dir. proc. pen.», 3 (2022), p. 1182; G.M. Caletti, Habeas corpus *digitale. Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Torino, 2024, p. 195.

[19] Lanzarote Committee, Implementation Report, cit., par. 80, ove si richiama l'Opinion del Comitato di Lanzarote del 2019, par. 7 (a)).

Occorre, tuttavia, sottolineare che l'opzione ermeneutica adottata dalla Corte di Cassazione a sezioni unite nel 2022 presenta profili di frizione con il principio di legalità, nella misura in cui opera una riscrittura della norma, sostituendo il rinvio al materiale di cui primo comma con un rinvio al settimo comma, con effetti che si traducono in un'estensione analogica in *malam partem*[20].

Un'interpretazione strettamente aderente al dato testuale dell'art. 600-*ter* c.p. non potrebbe prescindere dalla constatazione che nelle ipotesi di diffusione di materiale a carattere domestico non ricorre il presupposto dell'"utilizzazione" del minore nella fase della produzione dell'immagine. Di conseguenza, in assenza di tale elemento (a cui il comma n. 2 e seguenti fanno esplicito rinvio), non potrebbero ritenersi configurabili le fattispecie incriminatrici di commercio, diffusione o cessione di materiale pedopornografico, e quindi l'autore della divulgazione non dovrebbe essere ritenuto penalmente responsabile ai sensi del reato in esame.

In dottrina ci si è interrogati sull'opportunità di ricondurre tali ipotesi nell'alveo applicativo del delitto di diffusione illecita di immagini o video sessualmente espliciti. Il reato di cui all'art. 612-*ter* c.p., tuttavia, non appare idoneo a disciplinare queste ipotesi per una serie di motivi[21]. Oltre al fatto che si tratta di un reato procedibile a querela di parte, privo di specifiche circostanze aggravanti per il caso in cui la vittima sia minorenne, occorre sottolineare che il suo elemento costitutivo, rappresentato dall'assenza del consenso della persona ritratta alla diffusione, non si adatta all'ipotesi in cui la persona ritratta sia un minore. Ci spieghiamo meglio. La presenza dell'elemento costitutivo dell'assenza di consenso alla diffusione dell'immagine implica che nel caso in cui la persona ritratta acconsenta ad essa il reato non si configura. Ma quando il soggetto ritratto è un minorenne la questione si fa più complessa: non è infatti sostenibile che il consenso espresso dal minore alla diffusione della propria immagine possa assumere efficacia scriminante, in quanto ciò si porrebbe in contrasto sia con i principi affermati nei documenti sovranazionali in tema di diffusione di pedo-pornografia, sia con la chiara posizione della Corte di Cassazione a sezioni unite, che, come abbiamo illustrato, esclude che il minore possa prestare un valido consenso in questo contesto, difettando della maturità necessaria per comprendere le implicazioni e i rischi connessi alla circolazione del materiale.

Occorre tuttavia prestare attenzione alla recente evoluzione normativa in materia di bullismo e cyberbullismo. La legge 17 maggio 2024, n. 70, recante disposizioni in materia di prevenzione e contrasto del bullismo e del cyberbullismo, ha esteso la procedura dell'ammonimento (art. 7, legge n. 71/2017), a cui si può far ricorso per alcuni reati commessi da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, anche al delitto di cui all'art. 612-*ter* c.p. Tale scelta normativa sembra presupporre che nelle ipotesi in cui un minore diffonda immagini sessuali raffiguranti

[20] Recchia, *Pregevoli approdi e persistenti criticità nella sentenza delle Sezioni unite sul* sexting, in «Giur. it.» (2022), p. 1470.

[21] V. Cass., Sez. III, 12 febbraio 2020, n. 5522, par. 9.6.

altri minori, il reato di riferimento sia proprio quello di cui all'art. 612-*ter* c.p. Un simile richiamo rischia tuttavia di creare incertezza interpretativa nella giurisprudenza. In effetti, quest'ultima norma, come abbiamo precisato *supra*, non risulta strutturalmente idonea a disciplinare la circolazione di immagini sessuali ritraenti minorenni.

Una possibile soluzione, sistematicamente più coerente e garantista, potrebbe consistere in una riscrittura dell'art. 612-*ter* c.p., mediante l'introduzione di una sotto-fattispecie *ad hoc* riferita alla diffusione di immagini a contenuto sessuale la cui produzione non integri gli estremi del delitto di produzione di pornografia minorile. Tale intervento, opportunamente coordinato con la disciplina dei delitti previsti dall'art. 600-*ter* c.p., permetterebbe di evitare pericolose sovrapposizioni e garantirebbe forse una risposta più ragionevole e proporzionata per perseguire la diffusione di questa categoria di immagini.

Seguendo infatti l'interpretazione offerta dalle Cassazione a Sezioni unite del 2022 si finisce per ricondurre al medesimo reato condotte profondamente eterogenee: da un lato, la diffusione di immagini che ritraggono atroci abusi sessuali su bambini; dall'altro la messa in circolazione di un'immagine a contenuto sessuale raffigurante la propria fidanzata diciassettenne prodotta con il suo consenso e diffusa con o senza il suo consenso.

Ciò non vuol dire che quest'ultima condotta sia priva di rilevanza penale: essa è comunque connotata da disvalore e offensività e può generare gravi conseguenze sul piano psicologico e sociale per il minore ritratto. Ma può essere qualificato come "pedopornografo" il fidanzato che diffonde l'immagine a contenuto sessuale della propria ex partner diciassettenne? È questo il soggetto cui si riferiva il legislatore del 1998 nel delineare il reato di pornografia minorile? Appare evidente che, sia nella *communis opinio* sia nell'originario pensiero del legislatore, il "pedopornografo" è soggetto pericoloso per i minori, tanto da prevedere l'applicazione di gravissime pene accessorie, quale l'interdizione perpetua da qualunque incarico nelle scuole di ogni ordine e grado, nonché da ogni ufficio o servizio presso istituzioni o strutture frequentate abitualmente da minori (art. 600-*septie*s 2 c.p.).

Non si può ignorare la criticità, sotto il profilo della coerenza sistematica e dei principi fondamentali del diritto penale, di sussumere fatti tipici qualitativamente e criminologicamente così distanti nella medesima fattispecie incriminatrice. Una simile operazione interpretativa appare, a mio avviso, in contrasto con il principio di frammentarietà, di proporzionalità e *fair labelling*[22].

Appare ormai imprescindibile un intervento legislativo in cui si assuma una chiara posizione in ordine al perimetro della non punibilità della cd. pedo-pornografia domestica, in cui si disciplini in modo specifico la diffusione di questo materiale e si rivaluti la cornice sanzionatoria, tanto sul piano delle pene principali[23] quanto su

[22] Si consenta di rinviare a M. BIANCHI, *I confini della repressione penale della pornografia minorile*, cit., p. 45, ove si offre una ricostruzione di questo principio finalizzata a una revisione della disciplina nazionale.

[23] A tale proposito si segnala che, con riferimento al reato di produzione di materiale pornografico realizzato mediante l'utilizzazione di minori di anni diciotto, la Corte costituzionale con sentenza n. 91/2024 ha dichiarato l'illegittimità costituzionale dell'art. 600-*ter*, comma 1, n. 1, c.p., per violazione degli artt. 3 e 27, commi 1 e 3,

quello delle pene accessorie, tenendo in considerazione le specifiche esigenze dell'autore minorenne.

Un simile intervento risulta ancor più urgente alla luce delle più recenti indicazioni sovranazionali. In particolare, merita attenzione il report adottato dal Comitato di Lanzarote sul fenomeno delle *child self-generated sexual images and videos*, che, come già evidenziato, fornisce importanti linee guida orientate alla tutela effettiva dei minori, nonché la proposta di Direttiva del Parlamento europeo e del Consiglio del 2024 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e al contrasto della pedopornografia. Quest'ultima proposta, per esempio, restringe l'ambito della causa di non punibilità, limitandola ai casi in cui il materiale sia stato prodotto e detenuto tra minori o coetanei, escludendo quindi la sua applicazione nell'ipotesi in cui il materiale coinvolga un minore che abbia raggiunto l'età del consenso sessuale e un adulto.

Come già da anni sollecita la dottrina, solo un intervento legislativo puntuale potrà ricondurre la materia a criteri di chiarezza, coerenza sistematica, ragionevolezza e proporzionalità. Tale intervento legislativo diventa ancor più urgente alla luce della necessità di individuare con maggiore precisione il perimetro del cosiddetto "contenuto illecito" che i *providers* sono tenuti a rimuovere.

Cost., nella parte in cui non prevede che nei casi di minore gravità la pena da esso comminata sia diminuita in misura non eccedente i due terzi.

LA PROPAGAZIONE ILLECITA DI MATERIALE SESSUALMENTE ESPLICITO. QUALE TUTELA PENALE?

Monica Tortorelli

1. *Il dato fenomenologico e i presupposti della incriminazione*

La realtà socio-criminale, come non di rado avviene, spinge il legislatore a rivedere il sistema di tutela penale con l'inserimento di nuove ipotesi di reato volte ad abbracciare interessi ritenuti privi di strumenti idonei a garantirne una effettiva protezione.

In tale direzione, tra le diverse novità della l. 19 luglio 2019, n. 69, nota come Codice rosso, si pone la introduzione dell'art. 612 *ter* c.p. in tema di Diffusione illecita di immagini o video sessualmente espliciti[1].

Si tratta della fattispecie che ricomprende il segmento della vita della immagine[2] – quello appunto della sua (illecita) propagazione – più temuto e più grave, in quanto diretto a colpire la riservatezza della persona nella delicata sfera della intimità sessuale e della privatezza del proprio corpo.

[1] L'art. 612 *ter* c.p. (*Diffusione illecita di immagini o video sessualmente espliciti*) dispone che: «1. Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con la multa da euro 5.000 a euro 15.000. 2. La stessa pena si applica a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento. 3. La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici. 4. La pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza».

[2] Le diverse fasi della vita dell'immagine possono ricondursi ad una precisa scansione – ovvero la realizzazione, produzione, creazione, conservazione, condivisione privata e diffusione – come indirettamente suggerita anche dal Regolamento UE 2022/2065 (c.d. "*Digital Services Act*") in materia di responsabilità delle piattaforme digitali: v. G.M. CALETTI, Habeas corpus *digitale, Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Giappichelli, Torino, 2024, p. 286.

Si considerino emblematicamente, nel recente quadro criminologico, i casi, tristemente noti, di Tiziana Cantone, Carolina Picchio e Giulia Sarti[3], i quali attirano l'opinione pubblica e probabilmente smuovono lo stesso legislatore a disciplinare velocemente il fenomeno c.d. di *revenge porn* (sulla questione terminologica v. *infra*, § 4).

Le prime due vicende si sono drammaticamente concluse con il suicidio delle giovani donne, evidenziando ancor di più la necessità di disciplinare a livello normativo misure capaci di contrastare le peculiari condotte che, con le modalità più diverse, nel *cyberspazio*, concretizzano pericolose forme di abusi e violenza, ma anche di scherno, denigrazione, oppure prevaricazione e persino vendetta[4].

Ebbene, in occasione del nostro incontro di studio, è sembrato interessante individuare alcuni profili della norma contenuta nell'art. 612 *ter* c.p. che appaiono più rilevanti.

Si tenterà di offrire qualche spunto di riflessione per giungere essenzialmente ad una considerazione di fondo: siamo dinanzi ad una norma incriminatrice davvero efficace?

Prima ancora di esaminarli, tuttavia, bisogna operare una premessa.

Nel momento in cui ci si chiede – come pare opportuno domandarsi – se occorra il ricorso al diritto penale in questo ambito la risposta è certamente positiva.

Ragionando in termini di sussidiarietà della risposta penale, può affermarsi che la creazione di una norma *ad hoc* sia una scelta necessaria.

La corretta attuazione del canone della sussidiarietà nel nostro caso si evince nel momento in cui, oltre all'intensità del danno psicologico subìto dalle vittime, si considera l'irreversibilità della pubblicazione dei materiali sessualmente espliciti. Si tratta di una diffusione spessissimo virale che, per via del c.d. chiacchiericcio informatico[5], reso ancora più stringente dai *social media* e da piattaforme tecnologiche affini quali applicazioni di messaggistica istantanea, portali *hard*, *peer to peer* o *mailing list*, risulta difficile da arginare, posto che i contenuti immessi e condivisi nella rete diventano inarrestabili[6].

Nei contesti della violenza digitale, però, la piena legittimità in termini di politica criminale dell'intervento penale si giustifica soprattutto dinanzi alla incapacità dei

[3] Si vedano tali casi in G.M. CALETTI, *Can Affirmative Consent Save "Revenge Porn" Laws? Lessons from the Italian Criminalization of Non-Consensual Pornography*, in «VJoLT», 25/3 (2021), p. 117 ss. ("*Tiziana, Carolina and Giulia. Three (Non-) "Revenge Porn" "Italian Stories*") e M. MATTIA, "Revenge porn" e *suicidio della vittima: il problema della divergenza tra 'voluto' e 'realizzato' rispetto all'imputazione oggettiva degli eventi psichici*, in «Legislazione Penale», 18.7.2019, pp. 2 ss.

[4] Per una più approfondita riflessione sulle ricadute devastanti nella sfera reale delle vittime delle condotte di violenza digitale, M.N. CAMPAGNOLI, *Social media e information disorder: questioni di ecologia comunicativa in Rete (Parte Terza – Il* revenge porn), in «Dirittifondamentali.it.», 3 (2020), pp. 302 ss.

[5] Sulla c.d. chiacchiera informatica, A.C. AMATO MANGIAMELI, *Un nuovo bene: l'informazione*, in A.C. AMATO MANGIAMELI, M.N. CAMPAGNOLI (a cura di), *Strategie digitali. #diritto_educazione_tecnologie*, Torino, 2020, in part. p. 39; M.N. CAMPAGNOLI, *Social media e information disorder: questioni di ecologia comunicativa in Rete (Parte Terza – Il* revenge porn), cit., p. 317.

[6] Precipuamente sul tema e su quello connesso della negazione del diritto all'oblio, perchè «*Internet never forgets*», P.J. LARKING, *Revenge Porn, State Law and Free Speech*, in «Loyola of Los Angeles Law Review» (2014-2015), pp. 62 ss.

preesistenti presidi normativi e rimedi extrapenali, ad esempio di natura inibitoria, ma anche strumenti di controllo sulla rete Internet e sui *social networks*[7], di offrire efficace protezione alle vittime degli abusi sessuali tramite immagini, nei cui confronti l'offesa ai summenzionati beni giuridici può estendersi smisuratamente.

Pare pertanto del tutto condivisibile, a fronte anche della inefficienza di preesistenti norme penali (v. *infra*, § 2), la scelta del legislatore di autonomizzazione della tutela per mezzo della fattispecie *ex* art. 612 *ter* c.p., che fissa il baricentro della protezione penale sul contenimento delle pericolose conseguenze della "digitalizzazione" della propria o altrui intimità sessuale, capace di diffondersi velocemente quale nuova forma di manifestazione della libertà sessuale, ma che va certamente fronteggiata sul versante degli effetti dannosi che produce.

Siamo dinanzi a bisogni di tutela che intercettano il senso profondo della riservatezza, che custodisce la sfera più intima della vita umana e, una volta constatata pure l'insufficienza di agenzie diverse di controllo sociale (scuola, famiglia, associazionismo), al diritto penale sembra spettare un ruolo di primo piano nell'azione di contrasto a tali pratiche, potendosi ragionevolmente fare affidamento sulla sua capacità di deterrenza, che – più in particolare – si indentifica nella prevenzione della prima pubblicazione delle immagini sconvenienti[8].

C'è da sottolineare altresì l'attitudine della risposta penale a mostrarsi, in questa ipotesi, quale mezzo di orientamento culturale e di stabilizzazione collettiva del giudizio di disvalore delle condotte di "*revenge porn*", le cui conseguenze pregiudizievoli rischiano di essere minimizzate proprio per il fatto che vengono realizzate online, ossia in una dimensione apparentemente diversa da quella 'reale'.

Cionondimeno, in prospettiva, l'auspicio è che l'impegno dell'ordinamento si indirizzi al recupero di un modello integrato di contrasto e prevenzione[9], nella consapevo-

[7] Si legge nella stessa ordinanza del Tribunale di Napoli Nord con riferimento al 'caso Cantone' che in capo al *provider* non si ravvisa alcun obbligo di controllo preventivo nei confronti dei contenuti pubblicati e che la responsabilità del *provider* è successiva e sorge soltanto a seguito dell'avvenuta segnalazione da parte dell'interessato. Cfr. Tribunale Di Napoli Nord, 03.11.2016, con commento, di R. BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in «Giurisprudenza italiana», 3 (2017), pp. 629 ss.: ordinanza, questa, che richiama la Direttiva europea sul commercio elettronico (2000/31/CE), recepita nel nostro ordinamento con il d. lgs. 9 aprile 2003 n. 70. Sarà, tuttavia, utile valutare in proposito l'incidenza del Regolamento UE 2022/2065 sui servizi digitali operativo dal 17 febbraio 2024 e delle disposizioni della l. 7 ottobre 2024 n. 143 (Conversione in legge con modificazioni del c.d. *Decreto Omnibus*) in tema di obblighi di segnalazione e comunicazione (e relative omissioni) previsti per il *provider* stesso.

[8] Approfonditamente, P. BECCARI, G.M. CALETTI, *La diffusione di immagini sessualmente esplicite*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), *Cybercrime*, UTET Giuridica, Milano, II ed., 2023, p. 648.

[9] Occorrerebbe, in sinergia tra le diverse agenzie di controllo sociale, progettare ed attivare interventi pure sul fronte preventivo, volti anzitutto alla sensibilizzazione circa l'utilizzo responsabile e consapevole della rete e dei *social networks*, così da promuovere programmi di alfabetizzazione digitale e di sicurezza online, oltre che di educazione di genere, coinvolgendo strutture amministrative, ma anche didattiche ed accademiche. Inoltre, tra le varie misure ipotizzabili, solo per fare qualche altro esempio, sembra necessario attivare forme di assistenza psicologica e di supporto tecnico a protezione della sicurezza informatica e ideare strumenti capaci di reintegrare efficacemente la dignità violata delle vittime.

lezza che l'utilizzo dello strumento punitivo, quello più invasivo in termini di compromissione dei diritti individuali e di stigmatizzazione sociale, da solo non basta, e che in ogni caso il suo intervento richiede, di per sé, particolare rigore nella sua graduazione, così come particolare attenzione nella valutazione tecnica circa la funzionalità delle norme incriminatrici.

2. *Il vecchio contesto normativo e una voce fuori dal coro:* «Cautions against Criminalization»

Nella prassi applicativa, precedentemente alla introduzione della norma *ad hoc*, alcune fattispecie preesistenti – *in primis*, *ex* artt. 595, 615 *bis*, 617 *septies* c.p., art. 167 d. lgs. n. 196/2003 – venivano utilizzate per punire le condotte di abusi sessuali tramite immagini ma, benché se ne operasse una dilatazione operativa, le stesse si rilevavano spesso inidonee ad abbracciare le esigenze di tutela legate alla trasformazione telematica della vita di relazione.

In particolare, prendendole brevemente in considerazione, è evidente come il limite essenziale all'operatività della figura di interferenze illecite nella vita privata, come disciplinata dall'art. 615 *bis* c.p., risiedesse nella sua capacità di ricomprendere solo le ipotesi di diffusione riconducibili alle pratiche di *voyerismo* in cui l'immagine sia carpita mediante una intrusione dall'esterno nella sfera domiciliare, con un raggio di azione della tutela indubbiamente troppo ristretto[10].

La figura di diffusione di riprese e registrazioni fraudolente *ex* art. 617 *septies* c.p. – introdotta dall'art. 1 del d.lgs. 29 dicembre 2017, n. 216, in occasione della riforma

Allo stato, si badi, le stesse misure extrapenali e preventive, al pari delle tutele processuali, previste dal c.d. Codice rosso in favore delle vittime di violenza di genere (su cui v. L. ALGERI, *Il c.d. Codice rosso: tempi rapidi per la tutela delle vittime di violenza domestica e di genere*, in "Diritto penale e processo", n. 10/2019, pp. 1363 ss.), non sono purtroppo applicabili alle vittime della diffusione illecita di contenuti sessuali: nessuna norma di coordinamento tra queste diverse forme di abusi è stata contemplata nel testo della legge.

[10] Salvo qualche isolata pronuncia in senso contrario (vedi Cass. pen., Sez. V, 20 dicembre 2018, n. 13384: «la captazione di immagini di un atto della vita privata anche del co-protagonista della ripresa – che non si accompagni ad una manifestazione di volontà implicita od esplicita alla ripresa da parte di quest'ultimo – rende tale ripresa indebita, violando il suo diritto di riservatezza, pur risultando filmato un atto di coppia condiviso»), l'orientamento prevalente della giurisprudenza di legittimità può racchiudersi nel seguente principio di diritto: «non integra il reato di interferenze illecite nella vita privata (art. 615-*bis* c.p.) la condotta di colui che, mediante l'uso di strumenti di ripresa visiva, in un'abitazione in cui sia lecitamente presente, filma scene di vita privata, in quanto l'interferenza illecita normativamente prevista è quella realizzata dal terzo estraneo al domicilio che ne violi l'intimità, mentre il disvalore penale non è ricollegato alla mera assenza del consenso da parte di chi viene ripreso»: cfr. Cass. pen., Sez. V, 2 maggio 2018, n. 27160. Per completezza espositiva si segnalano nondimeno le decisioni che hanno operato una lettura estesa della nozione di privata dimora, riconducendovi – quali luoghi a metà strada tra la dimensione pubblica e privata – ad esempio l'ambulatorio di un ospedale (Cass. pen., Sez. III, 24 maggio 2018 n. 47123), lo spogliatoio di un circolo sportivo (Cass. pen., Sez. V,1° novembre 2014, n.12180) e un bagno ad utilizzo di più persone, quantunque non indiscriminato (Cass. pen., Sez. III, 30 aprile 2015, n. 2784). *Contra* si rimanda all'orientamento dominante come avallato nella ancora attuale pronuncia circa la nozione ristretta di privato domicilio: Cass. pen., Sez. un., 28 marzo 2006, n. 26795.

della disciplina delle intercettazioni – è invece calibrata su di una casistica completamente diversa da quella che ci riguarda, ovvero contempla le ipotesi della ripresa di incontri privati compiuta con modalità fraudolente (dunque opererebbe solo per i casi di pubblicazione di contenuti creati senza il consenso della persona ritratta), peraltro riguardanti contenuti audio (diversi dalle immagini).

Ad ogni modo, alla introduzione dell'art. 617 *septies* c.p. ha fatto immediatamente seguito l'inserimento nel sistema della fattispecie "dedicata", ovvero quella *ex* art. 612 *ter* c.p., e dunque si potrebbe forse ipotizzarne l'applicabilità, in un'ottica futura, alle ipotesi nelle quali l'assenza del requisito della destinazione privata dei contenuti richiesto dalla norma sul c.d. *revenge porn* (v. i*nfra*, § 3.2.1) può paralizzare l'operatività del reato. In dottrina, si è fatto riferimento ad esempio ai casi in cui vi sia la diffusione di un incontro amoroso filmato di nascosto da uno dei protagonisti; fattispecie che non può configurare l'ipotesi *ex* art. 615-*bis* c.p.[11].

La figura di illecito trattamento di dati di cui art. 167 del Codice della *privacy*, talvolta utilizzata[12] attraverso la equiparazione della immagine a qualsiasi altro dato personale, viene messa definitivamente fuori campo dalla riforma del 2018 (d.lgs. 10 agosto n. 101) che rende la norma non più applicabile alle ipotesi di distribuzione delle immagini: la condotta è punita solo in quanto (comma 2) posta in essere in violazione delle disposizioni di cui agli artt. 2 *sexies* e 2 *octies*, o delle misure di garanzia di cui all'art. 2 *septies*, ossia operando in violazione delle misure adottate ai sensi dell'art. 2 *quinquiesdecies*: ipotesi, queste, che hanno ad oggetto tutt'altre situazioni rispetto a quelle che qui trattiamo[13].

Ma, più di tutto, nel vecchio contesto normativo, le problematiche maggiori riguardavano il reato di diffamazione, disciplinato all'art. 595 c.p., a cui più frequentemente si faceva ricorso nella prassi applicativa[14].

[11] G.M. Caletti, Habeas corpus *digitale*, cit., p. 229.

[12] Cass. pen., Sez. III, 10 settembre 2015, n. 40356; Cass. pen., Sez. III, 14 giugno 2017, n. 29549.

[13] La stessa Cassazione ha negato la continuità normativa tra la vecchia e la nuova formulazione della norma in ordine alla illecita diffusione di contenuti intimi, prospettando la eventualità di ricercare detta continuità rispetto ad altre disposizioni vigenti, come l'art. 612 *ter* c.p. Si considera in particolare il secondo comma dell'art. 167, assumendo che è certo che i dati relativi alla vita sessuale rientrino nel richiamato art. 9 del regolamento UE, ma è altrettanto vero che la condotta è punita solo in quanto posta in essere in violazione delle suddette disposizioni di cui agli artt. 2-*sexies* e 2-*octies*, o delle misure di garanzia di cui all'art. 2-*septies* ossia operando in violazione delle misure adottate ai sensi dell'art. 2-*quinquiesdecies*: Cass. pen., Sez. V, 17 dicembre 2020, n. 3050. In senso critico circa la opzione di non inquadrare la illiceità penale della propagazione di materiale intimo all'interno del Codice Privacy, come illecito trattamento di dati, P. Troncone, *La tutela penale della riservatezza e dei dati personali*, ESI, Napoli, 2020, p. 19 e pp. 179 ss. Ma ancora, l'Autore pare avallare la possibilità di ricondurre questi comportamenti anche oggi nello spazio operativo della ipotesi *ex* art. 167 del Codice Privacy, pur in presenza delle modifiche legislative.

[14] «Anche il prestato consenso alla pubblicazione di un dato contenuto su un sito *web* o su *social networks* potrebbe non "salvare" dal reato di diffamazione, qualora il materiale di cui si era autorizzata la pubblicazione dovesse essere divulgato in contesti o per finalità completamente differenti da quelle che avevano indotto la vittima a prestare il suddetto consenso». In particolare, «potrebbe configurare il reato di diffamazione anche la pubblicazione in un sito internet di immagini fotografiche (nel caso di specie le fotografie ritraevano una persona in atteggiamenti pornografici), in un contesto e per destinatari diversi da quelli in relazione ai quali era stato precedentemente prestato il consenso alla pubblicazione»: Cass. pen., Sez. III, 19 marzo 2019, n. 19659. Nello

Eppure non è chi non veda come la fattispecie di diffusione illecita di materiale intimo non abbia ad oggetto una propagazione di notizie, ovvero la comunicazione di una informazione, ma la propagazione di una immagine quale dato esperienziale 'materiale', quantunque posta in essere in una dimensione apparentemente diversa da quella reale.

L'applicazione del reato di diffamazione non poneva solamente, in verità, un problema di *quantum* di pena, considerando peraltro che in vari casi, come quello della condivisione sui *social media*, il trattamento sanzionatorio poteva essere potenziato dal riconoscimento della circostanza aggravante integrata dal mezzo di pubblicità[15].

Si trattava invece di un reato inidoneo a recepire la tipologia di offesa insita nella condotta di diffusione illecita di immagini intime, attraverso cui non si realizza solo una lesione della reputazione della persona, ma prima di tutto essa viene infranta nell'ambito della privatezza e autodeterminazione del proprio corpo[16].

Per meglio dire, l'offesa al decoro qui si mostra più che altro come incidentale, in quanto la vittima potrà ricevere la disapprovazione sociale per la formazione di materiali a contenuto sessuale.

Di talché, la trasposizione, con la nuova norma, del fulcro della tutela dall'interesse reputazionale al bene della riservatezza contribuisce proprio ad arginare pericolosi meccanismi di *victim blaming*[17].

Ciò che si vuole intendere, in altre parole, è che, in una diversa e più corretta prospettiva, debba considerarsi come pregiudicato il decoro di una persona non in ragione della propagazione di sue immagini sessualmente esplicite (dal momento che non è il comportamento diffusivo, punito per altri scopi, a toccarne la reputazione), ma a causa della reazione della società ad una siffatta azione.

Nella dottrina americana[18], portando tale tematizzazione a più radicali sviluppi, è stato evidenziato che la stessa incriminazione della condotta di diffusione di immagini

stesso senso, Cass. pen., Sez. V, 19 giugno 2008, n. 30664. Approfonditamente, anche per più ampi riferimenti giurisprudenziali, v. S. SORGATO, Revenge Porn. *Aspetti giuridici, informatici e psicologici*, Milano, Giuffrè, 2019, pp. 20 ss. Più in generale, per una ricostruzione della giurisprudenza sulle "vecchie" fattispecie applicate, G. PANEBIANCO, *La diffusione illecita di immagini o video sessualmente espliciti: tra carenze della fattispecie incriminatrice e coadiuvanti extrapenali*, in «Genius», 16 novembre 2022, pp. 5 ss.

[15] Per un approfondimento in chiave critica circa la tendenza della giurisprudenza dominante a presumere la suddetta aggravante nei casi di diffamazione commessa su *Internet* si rimanda a F.P. LASALVIA, *Diffamazione via* web *nell'epoca dei* social network, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), *Cybercrime*, cit., pp. 345 ss.

[16] Parlava di una tutela che si risolveva in una «montagnola di sabbia» T. PADOVANI, *L'assenza di coerenza mette a rischio la tenuta del sistema*, in «Guida al Diritto», 37 (2019), p. 54.

[17] In questo senso si pongono anche le considerazioni di G.M. CALETTI, Habeas corpus *digitale*, cit., p. 230. Più in generale, la locuzione «*victim blaming*» – traducibile letteralmente come «colpevolizzazione della vittima» – è tratta dalla nota opera *Blaming the victim* del 1971, New York, Pantheon Books, del sociologo William Ryan, che la definisce come la tendenza ad ascrivere alla vittima, in virtù di un comportamento ritenuto sconveniente e superficiale, la situazione di danno subìto.

[18] V. la interessante prospettazione di A. GRUBER, *Cautions against Criminalization*, in G.M. CALETTI, K. SUMMERER (a cura di), *Criminalizing Intimate Image Abuse. A Comparative Perspective*, Oxford University Press, Oxford, 2024, pp. 94-95.

intime possa incorrere in un rischio analogo, dal momento che le politiche di contrasto al *revenge porn* sottenderebbero una idea di sessualità e di nudità femminile come preoccupante tabù, le quali diventano oggetto di stigmatizzazione sulla base dell'assunto che condividere foto di nudo sia giocoforza deturpante per la vittima.

In forza di questa teoria (identificabile con la perifrasi «*Cautions against Criminalization*») si rimarca, cioè, il rischio di divulgazione, in tal modo, del messaggio secondo cui la sessualità pubblica sia totalmente biasimevole e perciò le donne dovrebbero rifuggirla.

Ora, a riguardo c'è da osservare come si tratti di una prospettazione senza dubbio interessante, ma oggigiorno appare molto difficile da percorrere la strada della mancata criminalizzazione di abusi di questo tipo, ravvisandosi a monte (il problema è anzitutto e *ancora* culturale) la necessità di mutare – questo sì – obsolete concezioni sociali alla stregua delle quali le donne la cui immagine di nudo per qualsiasi motivo diventa pubblica devono per ciò solo subire lo sdegno e la condanna pubblica.

3. *La introduzione di una norma penale* ad hoc*: dalla opportunità della scelta legislativa ad alcuni profili problematici*

3.1. *La collocazione sistematica e una lettura in prospettiva*

Il nostro legislatore penale, dal canto suo, in seno alla legge 19 luglio 2019, n. 69, introduttiva di diverse modifiche al codice penale e al codice di procedura penale in materia di tutela delle vittime di violenza domestica e di genere[19], è intervenuto a ragione con la previsione di una specifica fattispecie criminosa, volta a fronteggiare più efficacemente i fenomeni di violenza digitale realizzati mediante la diffusione di contenuti sessualmente espliciti.

Nondimeno, come spesso accade, quando dal piano astratto degli intenti si passa a quello delle scelte concrete, sul fronte cioè della funzionalità delle norme, vediamo che lo stesso legislatore nel mettere mano alla disposizione cade in vecchi errori, dovuti a logiche di cattiva semplificazione.

In particolare, venendo ai profili di maggiore rilievo del reato, il primo tema di interesse è quello che attiene alla collocazione sistematica della norma e quindi al bene giuridico tutelato, quale elemento – ci pare – (ancora) importante di interpretazione della fattispecie, al fine di comprenderne i limiti, i confini e la interazione con altre figure, anche in una visione in prospettiva.

Nell'ipotesi di specie, un'auspicabile opzione legislativa potrebbe, a monte, identificarsi in una revisione più generale delle coordinate di sistema degli illeciti posti a tutela dei beni che qui trattiamo, ruotanti intorno alla reputazione e riservatezza della persona.

[19] Per tutti, in merito, L. Russo, *Emergenza "Codice Rosso"*, in «Sistema penale», 9 gennaio 2020; F. Basile, *La tutela delle donne dalla violenza dell'uomo: dal Codice Rocco… al Codice Rosso*, in «Diritto Penale e Uomo», 20 novembre 2019.

Sul punto avremo modo di tornare più avanti, valutando la possibilità che una riforma di questa materia *sub specie* dell'inquadramento sistematico della figura di diffusione illecita di contenuti intimi veda la luce.

Ad oggi, a fronte dell'attuale collocazione del delitto nel capo dedicato ai delitti contro la libertà morale[20], vi è chi diversamente dal legislatore individua nella "riservatezza" il bene leso dalla condotta diffusiva. Ma al tempo stesso, considerando l'impronta più grave del comportamento diffusivo rispetto ad altri reati che riguardano dati personali, non mancano aperture circa la possibilità di una collocazione diversa, dedicata alla tutela della libertà e autodeterminazione sessuale[21].

Ora, è pur vero che, allo stato – ovvero con una visione *de lege lata* –, la discussione circa l'inquadramento sistematico del reato non andrebbe acuita: è chiaro che si tratta di una fattispecie plurioffensiva, che abbraccia un intreccio di interessi, ove il bene della riservatezza è prodromico alla tutela di altri interessi[22].

La stessa giurisprudenza di legittimità ha avuto occasione, nel ricomporre i diversi profili di tutela sottesi alla figura, di sottolineare che: «il reato è inserito tra quelli a tutela della libertà morale individuale e si rivolge alla sfera di intimità e della *privacy*,

[20] In senso favorevole alla collocazione attuale, T. PADOVANI, *L'assenza di coerenza mette a rischio la tenuta del sistema*, cit., p. 54.

[21] Cfr. G.M. CALETTI, *La prima pronuncia di legittimità sull'art. 612* ter *c.p.*, in «Sistema penale», 10 (2023), p. 166, il quale osserva che in ragione della natura plurioffensiva del reato (cfr. per tutti M. BIANCHI, *L'incriminazione del "revenge porn": il nuovo delitto di "diffusione illecita di immagini o video sessualmente espliciti"*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Diritto penale*, t. III, UTET Giuridica, Milano, 2022, p. 6568 s.) «le possibili soluzioni "topografiche" erano molteplici, spaziando ad esempio dalla annessione tra i delitti sessuali – che avrebbe trovato giustificazione nel requisito del carattere "sessualmente esplicito" dei materiali diffusi – fino alla creazione di un nuovo titolo dedicato alla tutela dell'intimità o privacy sessuale» (lo si veda da ultimo in ID., Habeas corpus *digitale*, cit., p. 29 ss.); ed ancora G.M. CALETTI, *Libertà e riservatezza sessuale all'epoca di Internet. L'art. 612* ter c.*p. e l'incriminazione della pornografia non consensuale*, in «Rivista italiana di diritto e procedura penale», 4 (2019), p. 2064, quando rileva che «il riferimento al carattere "sessualmente esplicito" delle immagini contenuto nell'art. 612-*ter* c.p. fa pensare ad un'aggressione anche ad altri valori, quali l'intimità, la riservatezza, talvolta la fiducia prestata nei confronti dell'agente e, più in generale, la libertà di determinarsi in ambito sessuale». V. altresì, tra gli altri, B. ROMANO, *L'introduzione dell'articolo 612*-ter *del codice penale in materia di diffusione di immagini o video sessualmente espliciti (art. 10, l. 19 luglio 2019, n. 69)*, in B. ROMANO, A. MARANDOLA (a cura di), *Codice Rosso. Commento alla l. 19 luglio 2019, n. 69, in materia di tutela delle vittime di violenza domestica e di genere*, Pacini Giuridica, Pisa, 2020, p. 106, secondo cui «è indubbio che con il delitto […] si intenda tutelare la libertà della persona, gravemente vulnerata sul piano della vita di relazione poiché violata nella propria sfera sessuale». Inoltre, nella proposta di riforma dei reati sessuali redatta dall'Associazione italiana dei Professori di diritto penale, un reato corrispondente era collocato tra i delitti contro l'autodeterminazione sessuale. Il gruppo, coordinato dal Prof. Sergio Seminara, si componeva dei Proff. Giuliano Balbi e Marta Bertolino e delle dottoresse Malaika Bianchi, Sofia Braschi e Lara Ferla: v. S. SEMINARA (a cura di), *Reati contro la libertà e l'autodeterminazione sessuale*, in *www.aipdp.it*. Infine, l'Unione Camere penali italiane aveva proposto, in sede di audizione in Commissione Giustizia del Senato con riguardo al c.d. "Codice Rosso", la creazione di un titolo *ad hoc* riservato alla tutela della riservatezza sessuale (la si vada su *www.senato.it*). In quest'ultimo senso anche G. PANEBIANCO, *op. cit.*, p. 7 s.

[22] Sul tema, in generale, S. FIORE, voce *Riservatezza (diritto alla) (diritto penale)*, in «Enciclopedia giuridica», vol. XXVII, Treccani, Roma, 1998, p. 1 ss.

intesa quale diritto a controllare l'esposizione del proprio corpo e della propria sessualità, in un'ottica di autodeterminazione della sfera sessuale individuale»[23].

Tuttavia, c'è da evidenziare un profilo, che appare significativo: dal dibattito assai vario sul tema della collocazione sistematica del reato emerge un atteggiamento molto cauto della dottrina nell'assimilarlo *tout court*, in ordine ai profili lesivi, ai reati sessuali.

Eppure, in un'analisi di questo tipo, diretta a delineare l'offensività del delitto, andrebbe senz'altro accolta la prospettiva della vittima come punto di riferimento importante della valutazione (la quale del resto costituisce una fondamentale conquista in tema di evoluzione dei reati sessuali[24]), così da considerare gli effetti dell'ipotesi *de qua* quali conseguenze lesive del tutto parificabili a quelle dei reati sessuali.

In ragione di questo assunto, sul piano della tutela, allora, non appare corretto concentrarsi esclusivamente sulla dimensione privata del soggetto leso, ma il raggio di protezione della incriminazione andrebbe ricalibrato sugli interessi dell'intimità sessuale stessa, della libertà di scegliere come palesarla, sia che si tratti della creazione di immagini e video ovvero della negazione alla creazione di tali materiali, sia che si tratti di una condivisione con terzi[25].

Difatti, l'immagine (quale oggetto di diffusione) è un dato esperienziale, non un mero supporto di esso: se il corpo diventa "esperienza", ovvero partecipa ad una dimensione materiale (e non meramente ideale), è chiaro che possa essere violato anche attraverso atti (virtuali, appunto) che non ne investono l'integrità fisico-materiale.

Pertanto, la considerazione della *corporeità* della vittima comunque lesa dalla sua diffusione giustificherebbe, in una prospettiva *de lege ferenda*, la collocazione del reato all'interno di in un capo autonomo delle aggressioni sessuali, rivolto così alla tutela della sfera sessuale *tout court*.

3.2. *I problemi legati alla tecnica normativa: due esempi e un'auspicabile rivisitazione*

3.2.1. *Il requisito della «privatezza» dei contenuti*

Le problematicità della disposizione, non senza errori e vizi di merito, palesa l'approssimazione di un intervento normativo, il primo in tema di "abusi per immagine" della *privacy* sessuale, licenziato di fretta e furia nella sede legislativa e privo del benché minimo approfondimento anzitutto di tipo criminologico sul fenomeno, a discapito dei canoni di precisione, che invece dovrebbero guidare sempre la mano del legislatore penale.

Ancorché, in via preliminare, occorra considerare con molto rispetto la dimensione tragica degli eventi che, come sopra richiamati (§ 1), hanno mosso il legislatore

[23] Cass. pen., Sez. V, 22 febbraio 2023, n. 14927.

[24] Sul tema, anche per un approfondimento in chiave comparatistica, M.L. MATTHEUDAKIS, *Un'indagine comparatistica sulla configurazione dei reati sessuali per colpa (grave) sui profili di consenso della vittima*, in «Revista de Direito Brasileira», Florianópolis, SC, v. 25, n. 1072020, pp. 280 ss.

[25] In questo stesso senso, B. PANATTONI, *Violazioni "incorporee" della sfera sessuale. Possibili evoluzioni ed insidie nell'ambito dei reati sessualmente connotati*, in «Archivio penale», 2-3/2022, p. 28 s.

all'approvazione del c.d. Codice rosso, non può non evidenziarsi, quale conseguenza della rapidità con cui in quell'occasione (con emendamento al testo poi approvato della l. 69/2019) l'art. 612 *ter* è stato inserito nel codice penale[26], qualche palese difetto della formulazione normativa, che invero si sarebbe potuto evitare attraverso la predisposizione di un intervento più ponderato.

Sul versante precipuo della tecnica normativa, l'elemento della fattispecie che desta maggiori incertezze è fuor di dubbio quello della *destinazione privata* dei materiali descritti dalla norma.

Nello statuire che la diffusione delle immagini deve avere ad oggetto contenuti «destinati a rimanere privati» e avvenire «senza il consenso delle persone rappresentate», il legislatore – avvalendosi di una costruzione sintattica alquanto approssimativa – parrebbe in verità creare una endiadi[27] con la indicazione dei due requisiti della 'privatezza' e della 'mancanza di consenso', cosicché il primo potrebbe ritenersi una mera duplicazione del secondo. Eppure, la giurisprudenza di merito – quantunque agli albori della riflessione sulla tematica – esclude una tale prospettazione, rilevando che è proprio il primo limite l'aspetto caratterizzante della disposizione, oltre che quello più critico, e ne riconosce «una propria autonomia semantica e giuridica».

Il riferimento è alla decisione del GUP di Reggio Emilia, tra i primi chiamati a pronunciarsi sul tema, relativamente ad un caso di "*revenge porn*" contestato a due imputati che, utilizzando uno *smartphone*, dapprima formavano e poi diffondevano il video di un rapporto sessuale consumato da una coppia di fidanzati nel bagno maschile di una discoteca[28].

Il Giudice, nel caso di specie, ha fondato la propria decisione – con esito assolutorio – proprio su di una espressa valorizzazione del requisito in questione, evidenziando che l'inciso «destinati a rimanere privati» abbia la funzione di conferire «valore penale solo a quelle ipotesi in cui l'invio, la consegna, la cessione, la pubblicazione o la diffusione concernano materiale sessualmente esplicito, precedentemente condiviso o realizzato dalla coppia all'interno del contesto relazionale, realizzato consensualmente in un contesto connotato da reciproca fiducia, per cui al momento della cessazione del rapporto di fiducia stesso, essendo elevato il pericolo di utilizzo del materiale consensualmente realizzato a scopo ritorsivo, il legislatore ha deciso di introdurre una mirata sanzione per arginare tale fenomeno sociale e prevenire la diffusione di video, o immagini siffatte, soprattutto online».

[26] La disposizione *de qua* è stata inserita nel corpo normativo del c.d. Codice rosso con l'Emendamento 1.500 presentato dalla Commissione all'Assemblea della Camera e da questa approvato con il voto unanime dei presenti nella seduta del 2 aprile 2019.

[27] In questo senso anche P. Beccari, *Le prime difficoltà applicative della nuova fattispecie di "*revenge porn*" in caso di diffusione del materiale da parte di soggetti estranei al rapporto sessuale*, in «Sistema penale», 6 (2020), p. 12.

[28] Trib. Reggio Emilia, Sez. GIP/GUP, sent. n. 528/2021 (ud. 09/11/2021, dep. 22/11/2021): la si veda in «Sistema penale», n. 6/2020, con nota di P. Beccari, *op. cit.*, pp. 5 ss.; in «disCrimen», con note di D. Micheletti, "L'*interversio pubblicationis* quale elemento costitutivo della fattispecie di *revenge porn*", 7 gennaio 2022, pp. 1 ss. e C. Paonessa, *Ai confini del c.d.* Revenge porn. *Tessere di un mosaico* normativo, 8 marzo 2022, pp. 1 ss.

Da qui, ha ritenuto penalmente irrilevanti le condotte contestate agli imputati, le quali, benché deplorevoli e pregiudizievoli per le persone offese, non si reputano sussumibili nella fattispecie *ex* art. 612 *ter* c.p. per assenza di tipicità, dato che non si trattava di immagini realizzate con il consenso degli attori e destinate a rimanere private[29].

Pertanto, così interpretata, la fattispecie si limiterebbe ad incriminare solo la diffusione delle immagini sessualmente esplicite condivise «dalla coppia all'interno del contesto relazionale», con lo scopo di apprestare tutela alla riservatezza della relazione stessa lesa da una grave forma di abuso capace di rendere molesto ciò che in origine era oggetto di un rapporto intimo.

Un tale lettura, secondo alcuni Autori, giustificherebbe la controversa collocazione del delitto (privo dei requisiti di violenza e minaccia) tra quelli contro la libertà morale, nel senso che, in assenza di una condotta costrittiva, lo *specificum* del reato risiederebbe proprio nella interruzione del patto fiduciario – la c.d. *interversio pubblicationis* – che legava gli autori dell'atto sessuale consensualmente ripreso, con la conseguente violazione dell'autodeterminazione della vittima nell'ambito della propria sfera sessuale[30].

In verità, a noi sembra che alla base della scelta del legislatore di inserire la nuova fattispecie incriminatrice tra i delitti contro la libertà morale vi sia più che altro la contiguità criminologica tra la diffusione di immagini sessualmente esplicite e lo *stalking*, così da ritenere opportuno collocarla proprio immediatamente dopo gli atti persecutori (*ex* art. 612 *bis* c.p.), dalla cui disciplina peraltro non si manca di attingere anche per alcuni aspetti di contenuto (si pensi *in primis* al profilo delle circostanze aggravanti). Nondimeno, l'incongruenza della predetta soluzione interpretativa è evidente laddove si consideri che, a fronte di un disposto normativo tutt'altro che univoco, si andrebbe a convalidare la opzione di riservare la tutela penale alle ipotesi dotate di una minore carica offensiva, perché concernenti la diffusione di contenuti consensualmente formati (all'interno del *menage* di coppia), ma si escluderebbe per contro la rilevanza penale delle condotte maggiormente lesive, aventi cioè ad oggetto il materiale formato all'insaputa della vittima, al di fuori di una specifica dinamica relazionale.

C'è da prospettare allora una diversa lettura, in forza della quale, invece, la nozione di privatezza dovrebbe qualificarsi in senso «soggettivo»[31], così da esprimere la direzione che consensualmente i protagonisti degli atti sessuali imprimono alle immagini che li rappresentano.

[29] Il giudice, al pari, esclude nel caso di specie la configurabilità del reato di interferenze illecite *ex* art. 615 *bis* c.p., pure contestato dalla pubblica accusa con riguardo alla fase di *captazione* dei materiali stessi, ritenendo anche qui insuperabile un *deficit* di tipicità del fatto concreto dato dalla mancata integrazione del requisito del «domicilio», il cui riferimento nella norma, come noto, fonda il carattere «indebito» delle riprese e porta ad escludere dal perimetro applicativo della fattispecie la creazione di contenuti intimi fuori da un'abitazione, da una privata dimora o dalle relative pertinenze.

[30] Così D. Micheletti, *op. cit.*, p. 6.

[31] N. Amore, *La tutela penale della riservatezza sessuale nella società digitale. contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612*-ter *c.p.*, in «La Legislazione Penale», 20.1.2020, pp. 21 ss.

Questo significa richiedere in seno all'art. 612 *ter* c.p. la verifica di una duplice manifestazione di volontà: una, nel momento della formazione dei materiali, quale autorizzazione oppure negazione della loro diffusione (il che integrerebbe il requisito della «destinazione»); l'altra, all'atto di concretizzazione della propagazione, in termini di approvazione o meno di quello che inizialmente si era negato (ciò che costituirebbe l'elemento del «consenso»). Pertanto, ove il consenso alla diffusione sia dato contestualmente alla formazione dei contenuti, la propagazione non necessiterà di successivi e ulteriori permessi. Se questo non accade, la fruizione dei materiali riguarderà solo i soggetti originariamente individuati quali destinatari e la eventuale diffusione dovrà essere autorizzata.

Si tratta, invero, di una soluzione interpretativa che si giustifica per ragioni di ordine sistematico, considerando che attraverso la disciplina di cui agli artt. 615-*bis*, 617 *septies* c.p. e 96 l. 633/1941 l'ordinamento vieta ogni pratica diffusiva di materiali visivi avvenuta senza l'assenso di tutti i soggetti coinvolti.

Ma soprattutto questa opzione pare esprimere le finalità di tutela sottese alla incriminazione, posto che nell'attuale realtà digitale il diritto alla riservatezza e alla autodeterminazione sessuale si identifica soprattutto nella possibilità di scegliere a chi mostrarsi[32].

Resta ovviamente da comprendere, in questo caso, come il requisito dell'assenza di consenso alla diffusione debba essere verificato in sede giudiziale. Invero, la formulazione della norma – nel riferirsi per l'appunto alla «mancanza di consenso» – non sembra richiedere la manifestazione di un espresso dissenso alla divulgazione delle immagini, ovvero quella «volontà contraria» della vittima presente invece in altre disposizioni (una per tutte, quella di cui all'art. 614 c.p.) pure incentrate sulla non consensualità. Va detto che il consenso alla stessa propagazione debba essere esplicito[33], in termini cioè di preventiva autorizzazione: pertanto, c'è da concludere che l'imputato deve farsi carico della prova dell'assenso della persona ritratta alla diffusione del materiale che la rappresenta, dal momento che il reato si realizza ove la propagazione operi senza che l'autore abbia preliminarmente conseguito una manifestazione di volontà espressa alla diffusione[34]. Tutto questo, si badi, pur in presenza di consenso prestato dalla persona offesa alla condivisione iniziale delle immagini (c.d. *sexting*)[35].

[32] *Ibidem*.

[33] In questo senso gran parte della dottrina: per tutti, P. Beccari, G.M. Caletti, *op. cit.*, pp. 655 ss.; N. Amore, *op. cit.*, pp. 24 ss.; G. Panebianco, *op. cit.*, p. 10 s. *Contra*, tra gli altri, ritiene che l'assenza di consenso possa essere presunta G. De Santis, *"Codice Rosso". Le modifiche al codice penale (Prima parte)*, in «Studium iuris», 1 (2020), p. 5.

[34] Sulla scia d'altronde del parametro interpretativo recentemente adottato dalla giurisprudenza in tema di consenso nel reato di violenza sessale: per una ricostruzione di tale prospettiva ermeneutica e per un approfondimento sul tema del *consenso* nell'ambito del contesto più generale della violenza sessuale, cfr. G.M. Caletti, *Dalla violenza al consenso nei delitti sessuali. Profili storici, comparati e di diritto vivente*, Bologna University Press, Bologna, 2023, pp. 21 ss. Per la dottrina angloamericana si veda, *ex multis*, D.K. Citron, A.M. Franks, *Criminalizing Revenge Porn*, in «Wake Forest L Rev», 49 (2014), p. 354.

[35] Sul tema del *sexting*, su cui la dottrina angloamericana è sterminata, nella letteratura nazionale, si rimanda per tutti al lavoro monografico di M. Bianchi, *I confini della repressione penale della pornografia minorile. La tutela dell'immagine sessuale del minore tra esigenze di protezione e istanze di autonomia*, Giappichelli, Torino, 2019.

Ora, è chiaro però, tornando alla 'privatezza', che, a fronte di un elemento di fattispecie che inserito così ambiguamente nella costruzione del reato produce difficoltà interpretative, occorrerebbe – in prospettiva – una rivisitazione del significato che l'inciso attualmente assume. Potrebbe ipotizzarsi, auspicando una riforma della norma, di trasformare la locuzione «destinati a rimanere privati» nella perifrasi «destinati a rimanere riservati», da coordinarsi con il requisito dato dalla natura «sessualmente esplicita» degli stessi contenuti non consensualmente propagati: l'elemento della «*riservatezza*» delle immagini oggetto di diffusione, in luogo di quello della privatezza, porrebbe inequivocabilmente la fattispecie al di fuori della troppo restrittiva logica di coppia[36]. Sarebbe invece da conservare la previsione della «relazione affettiva» tra reo e vittima come circostanza aggravante (attuale comma 3) la quale si mostrerebbe anche più coerente (in quanto elemento realmente accidentale) all'interno di un più ampio contesto di disciplina del reato-base.

Si avrebbe, in questo modo, una figura criminosa idonea a cogliere a sufficienza le possibili e più attuali forme di manifestazione del fenomeno e capace di recuperare efficacia in termini di prevenzione generale e di prevenzione speciale rispetto anche a più gravi ipotesi di pornografia non consensuale.

In effetti, si può facilmente negare la destinazione privata ai contenuti sessualmente espliciti laddove il reato si realizzi in ambiti per loro natura esposti al pubblico (si fa l'esempio degli stabilimenti balneari o delle spiagge per cc.dd. "nudisti" o di spettacoli erotici aperti al pubblico)[37]. Di natura riservata, invece, potrebbero considerarsi i materiali divulgati in contesti non privati ma che avrebbero comunque dovuto rimanere "protetti" per volere dei soggetti coinvolti, come nell'ipotesi affrontata dalla surrichiamata decisione del GUP emiliano, ove il rapporto avveniva non platealmente, ma nel bagno di una discoteca, nel quale «si appartavano» le persone offese, che «ne chiudevano debitamente la porta a chiave»[38], come ricostruito in sentenza, che pur nega la privatezza dei contenuti necessaria ad integrare il delitto.

Ad ogni modo, fatte queste considerazioni in una prospettiva *de iure condendo*, nella speranza che il legislatore quanto prima intervenga a chiarire la portata appli-

[36] C'è chi *de lege lata* ritiene di doversi «rileggere» la nozione di 'privatezza' in termini di "intimità" (P. BECCARI, *op. cit.*, p. 16) oppure chi parla di intimità con riguardo all'inciso, rilevando però immediatamente dopo che la relazione intima «non potrebbe comunque compiersi senza tenere in debito conto della volontà di chi l'ha formata. È proprio la volontà dei componenti del *menage* […] più che "il contesto" in cui si svolge, a rappresentare l'elemento decisivo per fargli assumere una caratterizzazione privata» (N. AMORE, *op. cit.*, pp. 21 ss.). Ciò evidentemente crea il rischio di un accavallamento tra i due requisiti del carattere privato delle immagini e del consenso. Per la rivisitazione *de lege ferenda* nel senso della "riservatezza" dei contenuti sia consentito il rimando a M. TORTORELLI, *Gli abusi sessuali tramite immagini. Limiti applicativi e prospettive di riforma dell'art. 612* ter *c.p.*, in «Diritto Penale Contemporaneo» – Rivista trimestrale, 1 (2024), p. 215.

[37] L'esempio è riportato da P. BECCARI, *op. cit.*, p. 16.

[38] Di diverso avviso quella parte della dottrina secondo cui «chi si apparta maldestramente in preda a furore amoroso, senza premunirsi di non essere visto, non può che imputare a sé stesso l'eventuale cattura e diffusione di immagini che lo riguardino»: D. MICHELETTI, *op. cit*., p. 7. Così pure C. PAONESSA, *op. cit.*, p. 13 s.

cativa del delitto (magari in vista di prossimi lavori parlamentari[39]), riteniamo invece che, *de lege lata*, la riflessione debba necessariamente rimanere ancorata ad un epilogo esegetico obbligato.

È prospettabile la soluzione che rimanda ad un "annullamento" del carattere di privatezza delle immagini, nel senso di riconoscerne la inoperatività laddove sia accertata l'assenza del consenso delle persone coinvolte.

In tal modo, è chiaro, la portata applicativa della fattispecie verrebbe estesa sino ad abbracciare ogni ipotesi di diffusione di materiali sessualmente espliciti, realizzati e acquisiti da un terzo, estraneo al contesto relazionale.

Questa opzione dovrebbe per contro necessariamente essere esclusa laddove si ritenesse di non potersi prescindere dal requisito, così da preservarne l'autonomia di significato, considerando che l'elemento della mancanza di consenso è invece esplicitato dal legislatore[40].

In tal senso la decisione del GUP emiliano segna una direttrice importante e, senza per questo sminuire il carattere «ampiamente censurabile» della condotta posta in essere dagli imputati nel caso di specie, ritiene che l'ipotetica lacuna punitiva potrebbe essere colmata in futuro solo da un intervento del «legislatore ampliando la sfera di penale rilevanza».

3.2.2. *Il riferimento (troppo) vincolante alla diffusione di materiale «reale»*

L'art. 612 *ter* c.p. – incentrato sui due perni operativi della creazione "lecita" di video o immagini a connotazione sessuale all'interno di un contesto relazionale e della non consensuale pubblicizzazione del medesimo materiale – non sembra in grado, nemmeno nell'ipotesi aggravata della commissione del fatto con strumenti informatici o telematici (comma 3 seconda parte)[41], di contenere "nuove" forme di abusi sessuali tramite immagini, mostrandosi pertanto non completamente idoneo ad assolvere al compito che il legislatore, almeno in termini di intenzioni, ha voluto affidargli.

Le forme di pornografia non consensuale, nell'attuale società digitale, risultano assai più estese rispetto alla casistica considerata dal legislatore.

[39] Mai ritirati risultano i numerosi progetti di legge in materia pendenti in Parlamento: durante la XVII Legislatura, v. quello del 27 settembre 2016 (Atto Camera 4055) ed il disegno di legge presentato al Senato il 5 dicembre 2017 (Atto Senato n. 2994) e riproposto alla Camera nella successiva Legislatura il 2 luglio 2018 (Atto Camera n. 839). Durante la XVIII Legislatura si vedano: la proposta di legge presentata alla Camera il 9 gennaio 2019 (Atto Camera n. 1488); i disegni di legge comunicati alla Presidenza del Senato il 19 febbraio 2019 (Atto Senato n. 1076) e il 12 marzo 2019 (Atto Senato n. 1134); il disegno di legge presentato al Senato il 25 marzo 2019 (Atto Senato 1166); la proposta di legge presentata alla Camera il 7 maggio 2019 (Atto Camera 1828).

[40] Per questa lettura v. anche C. Paonessa, *op. cit.*, p. 12.

[41] Possibilista in tal senso ma dubbiosa per ragioni di tassatività della norma penale, in quanto il testo della disposizione non fa riferimento a contenuti non reali, C. Corridori, *Il fenomeno del deep-fake e il diritto penale tra tutela dell'immagine e autodeterminazione sessuale*, in «Giudicedonna.it», 1-2 (2023), p. 5.

Tra le "nuove" ipotesi (V*oyeurismo* digitale, sabotaggio di dispositivi informatici, "pornografia estrema": v. *infra*, § 4), cresciute in maniera esponenziale negli ultimi anni, vi è quella – che si presta particolarmente bene a rappresentare la esigenza di un allargamento della definizione di violenza digitale ai sensi dell'art. 612-*ter* c.p. – del '*deep sex fake*'.

Può dirsi, in estrema sintesi, per quel che qui più interessa, che tale fenomeno consiste in una tecnica basata sull'intelligenza artificiale per manipolare immagini e video già esistenti, atta a sovrapporre, tramite algoritmi di apprendimento automatico, il volto o altre parti della vittima a figure intente a compiere atti sessuali, con la diffusione poi di tali contenuti in Rete[42].

A fronte di questa pericolosa modalità di compromissione della riservatezza e della intimità sessuale, utenti donne di *Twitch*, *Youtube* e *Tik Tok* si sono trovate coinvolte in video pornografici con la loro faccia; ma la cronaca narra di vicende avvenute nelle scuole, lanciando l'allarme anche tra gli studenti. Successivamente l'impiego dell'app "*Deep Nude*" ha consentito di 'denudare' artificialmente qualsiasi donna manipolandone l'immagine vestita: si tratta di un programma che lavora prevalentemente su immagini femminili (perché di più facile reperibilità), con l'effetto di creare delle foto di nudo dal contenuto assolutamente realistico. Lo strumento si è diffuso addirittura su *Telegram*, in cui le immagini femminili divengono "denudabili" attraverso i cc.dd. *BOT*[43] e altresì passibili di una diffusione estrema perché reperibili molto agevolmente da chiunque acceda ad una chat con il '*BOT Deep Nude*'[44].

Così è evidente come, a pochi anni dalla riforma del c.d. Codice rosso, viene in rilievo una nuova forma di estrinsecazione della pornografia non consensuale, poiché se è vero che i contenuti di *deep-porn* sono realizzati in maniera artificiale, è altrettanto vero che essi appaiono assolutamente verosimili[45], tanto da costituire una forma molto

[42] V. per un'ampia disamina sul tema i contributi di N. Ordonselli, *"*Porno Deepfake*": profili di diritto penale. Quando l'intelligenza artificiale incontra la pornografia*, in «CyberLaws.it», 18 gennaio 2021, e di C. Corridori, *Il fenomeno del deep-fake*, cit.

[43] Programmi *software* che eseguono attività automatizzate, ripetitive e predefinite, congegnati per imitare o sostituire le azioni umane.

[44] Per un approfondimento pure sui dati statistici di ciò che identifica non un semplice problema, ma una vera e propria emergenza, anche e soprattutto tra i giovanissimi, si rimanda a G. Canè, *Studenti «spogliano» le compagne con l'intelligenza artificiale: sempre più* deepfake *nelle scuole (anche in Italia?)*, in *Corriere.it*, 7 novembre 2023, il quale richiama le fonti internazionale del *Washington Post* (ove si citano gli sudi dell'analista del settore *Genevieve Oh*) e di *Sensity AI*, una società che ha monitorato i video *deepfake online* a partire dal dicembre 2018; D. Giancipoli, *Deepnude: i contenuti pornografici creati con l'AI sono fuori controllo?*, in *Alley Oop. L'altra metà del Sole* (*de Il Sole24ore*), 11 dicembre 2023; D. Harwell, *Scarlett Johansson on fake AI-generated sex videos: 'Nothing can stop someone from cutting and pasting my image'*, in *washingtonpost.com*, 31.12.2018; G. Giacobini, *Storia dell'app che genera(va) false foto di nudo femminile*, 29 giugno 2019, su https://www.wired.it/mobile/app/2019/06/28/app-deepnude-fake-donne/.

[45] Judge Herbert B. Dixon Jr., *Deepfakes: More Frightening Than Photoshop on Steroids, The Judges' Journal, American Bar Association*, 12 agosto 2019, su https://www.americanbar.org/groups/judicial/publications/judges_journal/2019/summer/deepfakes-more-frightening-photoshop-steroids/.

pericolosa di violenza che infrange irreversibilmente la sfera personale della vittima e che quindi necessita di assumere rilevanza penale[46].

Allora, collocando pure qui la riflessione in una prospettiva *de iure condendo*, anche alla luce della recentissima Direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica che impone la criminalizzazione della diffusione di immagini artefatte, ci pare ipotizzabile – come nuovo modello di incriminazione *ex* art. 612 *ter* c.p. – una fattispecie volta ad inglobare specificatamente, in un apposito comma, accanto alle condotte diffusive di contenuti reali, l'ipotesi di *deep sex fake*, nella forma della manipolazione di contenuti sessualmente espliciti con l'inserimento artificiale di soggetti terzi e/o della diffusione di tali materiali manipolati[47].

Va nondimeno rimarcata la opportunità, in siffatta direzione, che la modifica contempli, in seno alla previsione della punibilità della diffusione di immagini false, il requisito del loro *realismo*[48].

La espressa tipizzazione di detto fenomeno criminale, quale parte di un sistema di tutela integrato con le altre agenzie di controllo sociale[49], ne consentirebbe una più compiuta emersione, indirizzando davvero l'intervento penale alla sua funzione di utilità sociale, in termini di idoneità preventiva e non solo di funzione simbolica.

Il diritto penale, «oltre a dover strutturare incriminazioni fedeli ai suoi principi fondamentali», è chiamato qui «più che in ogni altro campo dell'agire delittuoso ad interpretare l'evoluzione del sentire sociale, a confrontarsi nel profondo con i costumi sessuali della sua epoca, a comprendere il reale peso di alcuni stereotipi culturali radicatisi nel tempo»[50].

[46] Sulla sicura rilevanza penale del fenomeno N. ORDONSELLI, *"*Porno Deepfake*"*, cit.; N. AMORE, *op. cit.*, p. 30 s.

[47] Per questa proposta v. anche N. AMORE, *op. cit.*, p. 36 s. Aveva peraltro contemplato la dimensione dei nuovi *media* l'emendamento n. 01.017, proposto dai deputati Boldrini e Conte (LEU) e bocciato pochi giorni prima dell'approvazione del testo dell'art. 612 *ter* c.p. da parte della Camera dei deputati. La proposta versione del reato di «Divulgazione non consensuale di contenuti intimi» considerava pure le ipotesi delle «immagini virtuali realizzate utilizzando immagini di persone senza il loro consenso, create con tecniche di elaborazione grafica non associate in tutte o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali», inglobando perciò le pratiche di *deepfake*. Cfr. sul punto P. BECCARI, *op cit.*, p. 22.

[48] In questa prospettiva anche G.M. CALETTI, Habeas corpus *digitale*, cit., p. 172.

[49] Si consideri, tra le varie misure ipotizzabili sul piano extrapenale, quella che, a livello sovranazionale, si è sostanziata nell'accordo sul regolamento europeo per l'intelligenza artificiale, raggiunto nel dicembre 2023 con il nome di *AI Act*, il quale si compone, tra gli altri, di provvedimenti relativi a strumenti come *ChatGpt* o *LaMDA*, laddove viene in rilievo la pratica di manipolazione di immagini, e quindi la responsabilità che i sistemi di AI dovrebbero avere in termini di trasparenza, tutela e legalità. Sul fronte preventivo, nel nostro sistema, si segnala l'iniziativa intrapresa dal Garante dell'Infanzia della Regione Lazio in seguito al noto caso romano degli adolescenti che hanno utilizzato l'app *Bikinioff* per creare immagini di nudo delle loro compagne (v. G. GIACOBINI, *Storia dell'app che genera(va) false foto di nudo femminile*, cit.): sono stati organizzati incontri formativi nelle scuole, nelle parrocchie e nei gruppi sportivi con il progetto "*Genitori al centro, missione adolescenza*". Si consideri inoltre il progetto contro la violenza digitale «*Donneconloscudo*» ideato dalla informatica forense Federica Bertoni nel 2019 al fine di sensibilizzare l'opinione pubblica sui temi della sicurezza informatica e dell'informatica forense e di rappresentare le esigenze delle vittime delle "realtà digitale": per un approfondimento può leggersi il pezzo di D. AMERI uscito sul numero 1.254 di D – *la Repubblica delle donne*, del 4 settembre 2023.

[50] Così, con riguardo al generale contesto dei reati sessuali, G.M. CALETTI, *Dalla violenza al consenso nei delitti sessuali*, cit., p. 23. Può richiamarsi altresì la ancora più generale riflessione di G. FORNASARI, *L'evoluzione*

In quest'ottica, la esplicita incriminazione della pratica di *deep sex fake* offrirebbe agli operatori del settore, alle Forze dell'ordine e alla magistratura *in primis*, uno strumento in grado di contrastare condotte offensive di beni rilevanti – l'intimità e dignità della vittima, comunque lese attraverso la forzata esibizione, quantunque artefatta ma verosimile, della sua sessualità – che oggi non si riesce a fronteggiare con delle fattispecie (oltre alla ipotesi *de qua*, la diffamazione *ex* art. 595 c.p., l'estorsione *ex* art. 629 c.p., lo *stalking*, di cui all'art. 612-*bis* c.p.) le quali o contemplano soltanto alcuni profili del fenomeno oppure, in definitiva, non sono state pensate per tale scopo di tutela[51].

4. *Una conclusione: in ogni caso, «non chiamatelo* revenge porn»

I brevi cenni appena riportati restituiscono l'immagine di una disciplina ancora fortemente disarticolata e sguarnita di un sufficiente livello di approfondimento del fenomeno che si deve fronteggiare.

Ora, se è evidente che si tratta di un contesto nel quale risulta molto difficile rimanere ancorati ai canoni di razionalità rispetto a vicende umane estremamente drammatiche, è d'altro canto vero che il rispetto del principio di effettività diventa comunque la condizione perché il diritto penale possa davvero funzionare.

Il legislatore dovrebbe preoccuparsi di creare incriminazioni puntuali e quanto più possibile accurate nella descrizione del dato criminologico che intende contrastare, per guadagnare autorevolezza e credibilità sul piano general preventivo (sia positivo che negativo), e non solo su quello repressivo.

Su questa linea, in ordine alla fattispecie che trattiamo, ai fini della corretta attuazione degli interventi modificativi come quelli sopra auspicati, l'attenzione, in prospettiva, andrebbe concentrata su di una migliore comprensione di alcuni punti di riferimento anche terminologici, così da convergere verso un approccio più preciso alle esigenze di tutela della riservatezza corporea.

della comparazione giuridica in ambito penalistico, in «www.robertotoniatti.eu» (2020), secondo il quale «se è vero che le norme giuridiche e la loro interpretazione seguono l'evoluzione del mondo che devono regolare, oggi quel mondo è globalizzato e vive di interrelazioni».

[51] Diversamente, i casi di immagini porno *deepfake* ritraenti soggetti minorenni potrebbero farsi rientrare nel reato di pornografia virtuale posto che in forza dell'art. 600 *quater*1 c.p. si considerano integrati i reati di pornografia minorile (art. 600 *ter* c.p.) e di detenzione di materiale pornografico (art. 600 *quater* c.p.) anche quando le immagini sono virtuali, cioè «realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali». Tuttavia, in aggiunta a tale norma (in cui, al di là della complessità che notoriamente la accompagna, parrebbe potersi leggere in verità più una generale *voluntas legis* di prevenire e scoraggiare la pratica in sé della pedopornografia), onde garantire una risposta adeguata al fenomeno di *deep sex fake*, sarebbe (anche per questo) augurabile un intervento legislativo che, con la previsione di una specifica ipotesi rivolta a tale scopo, possa apprestare una più efficace tutela alle persone offese, pure quelle minori di età – in tal caso con una misura rafforzata data dall'aggravante disciplinata già all'attuale comma 4 dell'art. 612-*ter* c.p. in cui auspicabilmente sarebbe da inserire il precipuo ed espresso riferimento al soggetto minore – in conseguenza di azioni lesive che costituiscono una pericolosa degenerazione della corrispondenza a sfondo sessuale. Per un approfondimento sul punto sia consentito rinviare a M. TORTORELLI, *op. cit.*, p. 223 s.

La nozione, in particolare, di "*revenge porn*" – diffusamente utilizzata per definire il reato – risulta fuorviante[52], poiché essenzialmente essa si riferisce, in maniera molto limitante, ai contesti di coppia, rimandando ad una finalità di vendetta, mentre di fatto le motivazioni che spingono all'illecito possono essere assai differenti[53].

La stessa dottrina angloamericana ha inteso rivederne l'originario significato prospettando locuzioni alternative, in ragione anzitutto della ritenuta necessità di incentrare il sistema di protezione penale sull'assenza di consenso della vittima: la specifica condotta di diffusione di immagini è oggi indicata con la locuzione "distribuzione non consensuale di immagini intime" ("*non-consensual distribution of intimate images*")[54].

Ma, al fine di definire il fenomeno in maniera più ampia, la dicitura senza dubbio prevalente nella comunità scientifica, specialmente a livello internazionale, è quella di "*Image-based sexual abuse*" ("IBSA")[55], che appare neutra e sufficientemente estesa da ricomprendere le diverse manifestazioni di questo reato.

A proposito, infatti, della profonda eterogeneità di tale fenomenologia criminale, si considerino, accanto al già richiamato fenomeno del *deep sex fake*, le ipotesi, tra le altre, di sabotaggio di dispositivi informatici cui consegue la pubblicazione dei materiali sessualmente espliciti che essi racchiudono, spesso realizzate ai danni di personaggi famosi, oppure la "pornografia estrema", laddove a monte la non consensualità riguarda lo stesso rapporto sessuale. Ma soprattutto vanno segnalate le ipotesi in cui la compromissione del diritto alla riservatezza si determina al momento della *realizzazione* del materiale sessualmente esplicito, perché indebitamente formato, già prima della conseguente diffusione. É il caso, ad oggi sguarnito di una effettiva risposta penale[56], del '*Voyeurismo* digitale', ovvero la pratica di osservare segretamente le vittime, nelle loro parti intime, attraverso mezzi digitali, senza il loro consenso, decidendo in seguito eventualmente di condividere il materiale sulla rete[57].

Alla luce di tali considerazioni, occorrerà ampliare anche in questa direzione il dato testuale dell'art. 612 *ter* c.p.

[52] In merito v. l'interessante intervista di K. SUMMERER, *"Non chiamatelo* revenge porn*"*, su https://salto.bz/de/article/20032024/non-chiamiamolo-revenge-porn.

[53] Quale, ad esempio, l'intento di recare danno alla vittima per rovinarne l'immagine pubblica, a prescindere dalla sussistenza di un legame di coppia. La condotta tipica potrebbe inoltre essere innescata da ragioni di natura estorsiva. Dalle cronache giornalistiche emerge tra l'altro la pratica in uso a diverse categorie di soggetti, giovani e meno giovani, di diffondere contenuti intimi dei propri *partners* tra gli amici, per finalità di scherzo, di vanto o solo vilmente per acquisire notorietà.

[54] M. AIKENHEAD, *Image-based Abuse in Intimate Partnerships in Canada: Lessons from the Criminal Case Law*, in G.M. CALETTI, K. SUMMERER (a cura di), *Criminalizing Intimate Image Abuse. A Comparative Perspective*, cit., p. 322 s.

[55] Cfr. i contributi di C. MCGLYNN, E. RACKLEY, *Image-based Sexual Abuse*, in «Oxford Journal of Legal Studies», 37/3 (2017), p. 534 ss. e N. HENRY, C. MCGLYNN, A. FLYNN, K. JOHNSON, A. POWELL, A.J. SCOTT, *Image based Sexual Abuse. A Study on the Causes and Consequences of Non consensual Nude or Sexual Imagery*, Abingdon Oxon-New York, Routledge, 2021.

[56] Considerate anche le già richiamate limitazioni applicative del delitto di interferenze illecite *ex* art. 615 *bis* c.p. (v. *supra*, § 2).

[57] Su queste "nuove" forme di pornografia non consensuale, N. AMORE, *op. cit.*, p. 6 s. e p. 30 s.

Il legislatore italiano, invero, si è attenuto ad una definizione piuttosto neutrale della fattispecie nella specificazione della rubrica della norma (*Diffusione illecita di immagini o video sessualmente espliciti*), idonea potenzialmente a ricomprendere ipotesi ulteriori rispetto a quelle realizzate nella dimensione privata della relazione di coppia. Sarebbe tuttavia opportuno che vi uniformasse anche il suo contenuto, che pare invece, come visto, legittimare l'angusto significato di *porno-vendetta* (troppo incentrato, com'è, sul punto di vista dell'autore), così da creare una incriminazione a contenuto più esteso, davvero capace di fronteggiare la violenza virtuale e recuperare una visione d'insieme e una reale prospettiva di effettività, contemplando la complessa e sfaccettata dimensione odierna della pornografia non consensuale, in una società sempre più interconnessa, ove si determina una inarrestabile propagazione di contenuti da ogni dove e per le più diverse finalità creati.

Attraverso una tale inversione, recuperandosi seriamente la norma alle ragioni della effettività, si riorienterebbe la fattispecie, in un'ottica di maggiore efficacia, sul riconoscimento della prospettiva della vittima, cui potrebbe aggiungersi la valorizzazione del requisito del consenso, «unico discrimine […] il quale può esserci o no indipendentemente dal contesto, dalla situazione, dagli attori implicati»[58], anche con riguardo alla fase della *creazione* dei contenuti a sfondo sessuale.

Invero, la enfatizzazione della finalità vendicativa dell'autore dell'illecita diffusione non permette di considerare a tutto tondo la condizione delle vittime, che spesse volte risultano loro malgrado, come già detto, assoggettate a cattive pratiche di c.d. *victim blaming* per aver concesso il proprio iniziale consenso alla creazione di materiali sessualmente espliciti[59]. Invece, i due piani – quello del consenso alla formazione e quello del consenso alla propagazione delle immagini – non andrebbero mai confusi, vale a dire che non è in alcun modo ammissibile una interpretazione che desuma il consenso alla diffusione dal fatto che la vittima abbia scelto (legittimamente) di condividere contenuti intimi con una persona, in circostanze di fiducia, quale estrinsecazione della propria libertà sessuale.

La soluzione in prospettiva potrebbe essere, allora, anche quella di esplicitare nel testo della norma una ulteriore specificazione dei contenuti oggetto della condotta di diffusione quali immagini o video *pure consensualmente formati*.

Ben vero, ci pare fondamentale prendere le distanze da ogni forma di minimizzazione di queste pratiche di violenza, diretta conseguenza di un modello culturale inveterato, ma da rifuggire ed osteggiare, attraverso anche l'utilizzo di schemi linguistici, oltre

[58] In questi termini, con riguardo alla violenza sessuale, T. PITCH, *Violenza sessuale*, in *Un diritto per due*, Il Saggiatore, Milano, 1998, p. 169, come richiamata, in tema *de quo*, da P. BECCARI, *op. cit.*, p. 20 s. Sul tema v. altresì P. BECCARI, G.M. CALETTI, *op. cit.*, pp. 647 ss.

[59] Sulla mancanza di una 'cultura del consenso' («*a missing culture of consent*») in svantaggio delle persone offese dalle pratiche di pornografia non consensuale, nelle letteratura angloamericana, v. N. HENRY ET AL., *Imaged-based sexual abuse*, cit., pp. 113 ss., anche per la evidenziazione dell'esigenza di una maggiore prevenzione sulla tematica: «*[…] efforts to respond victim-survivors and to work with perpetrators towards preventing imaged-based sexual abuse need to take account of this dual reality of victims-survivors' life*».

che cognitivi, che siano appropriati e consoni, in sostituzione di vecchi codici culturali e stereotipi (uno per tutti i miti legati alla *rape culture*)[60] che forgiano in modo falsato la percezione e l'interpretazione degli episodi di violenza stessa.

Chiaramente non si può pensare di far fronte ad un tale problema nella sede penale se prima non si attivano interventi preventivi di sensibilizzazione generalizzata a tutti i livelli e in tutti i settori di competenza, ma un mutamento di prospettiva già sul piano della 'cura' nella scelta dei registri comunicativi riguarda anche il ruolo e la funzione delle norme incriminatrici[61], le quali dovrebbero riuscire a descrivere i precetti attraverso una puntuale raffigurazione del volto reale del fatto vietato, così che quel rapporto "metaforico" che si crea tra ciò che la norma prescrive e la dimensione illecita che vi è sottesa riesca davvero a restituire una immagine veritiera del fatto punito, oltre che visibile e pienamente riconoscibile[62].

[60] Per tutti, L.K. THACKER, *Rape culture, Victim blaming, and the role of media in the criminal justice system*, in «Kentucky Journal of Undegraduate Scholarship», vol. 1, Issue 1, Maggio 2017.

[61] Per un attuale contributo sul tema concernente il "linguaggio del diritto penale" ed il suo rapporto con le esigenze di effettività del sistema, C. DE MAGLIE, *Linguaggio del diritto penale e principio di effettività: spunti di riflessione*, in «disCrimen», 31 marzo 2023.

[62] Sulla esigenza di riconoscibilità, storicamente, Corte Cost., 8 giugno 1981, n. 96, in «Giurisprudenza costituzionale» (1981), p. 802. Cfr. altresì Corte cost., 22 aprile 1992, n. 185, in «Cassazione penale» (1993), p. 5.

LA DIFFUSIONE DI CONTENUTI ILLECITI ONLINE. OBBLIGHI DI INCRIMINAZIONE E CONTRASTO DEL "*DEEPFAKE*" NELLA DIRETTIVA (UE) 2024/1385

Caterina Paonessa

SOMMARIO: 1. Una preliminare contestualizzazione. – 2. Le direttrici di tutela penale. In particolare: il caleidoscopio della dignità umana. – 3. Il fenomeno "*deepfake*". – 4. L'attuale assetto della regolamentazione nazionale. – 5. La condivisione non consensuale di materiale intimo o manipolato nella prospettiva europea e il suo possibile impatto sull'art. 612-*ter* c.p. – 6. Gli ulteriori risvolti attuativi. – 7. Postilla.

1. *Una preliminare contestualizzazione*

L'allestimento, tramite direttive, di articolati programmi di tutela che si estendono fino a comprendere specifiche istanze di natura repressiva è un tratto ormai ricorrente dell'*acquis* europeo, espressamente legittimato dall'art. 83 TFUE. Anche la recente direttiva (UE) 2024/1385, «sulla lotta alla violenza contro le donne e alla violenza domestica», si colloca in questo tracciato, rendendo, di riflesso, necessarie alcune premesse sistemiche per poterne cogliere appieno tanto il contenuto precettivo, quanto le potenziali ricadute applicative.

Su un piano generale, è utile, innanzitutto, ricordare che gli obblighi di incriminazione evocano una precisa "tecnica" di evoluzione del diritto penale: al vincolo sovraordinato, espressivo di valutazioni anticipate sulla meritevolezza e sul bisogno di pena, fa da *pendant*, infatti, la limitazione della libertà di scelta politica del legislatore. Questo schema si ripete quale che sia la fonte impositiva del vincolo di tutela: sia essa la Costituzione oppure il diritto sovranazionale, segnatamente il diritto dell'Unione europea. Se, nella forma, il *modus operandi* è sempre lo stesso, nella sostanza emergono, però, differenze piuttosto significative tra obblighi costituzionali ed obblighi europei di penalizzazione.

Allocata nella Costituzione, la tutela penale obbligatoria è servente alla piena attuazione di diritti e libertà fondamentali[1], da presidiarsi anche (e soprattutto) contro il rischio di possibili degenerazioni dell'esercizio del potere punitivo. Si tratta di ipotesi, per il vero assai circoscritte, che hanno visto coagulare intorno a sé un naturale consenso, non solo perché contenutisticamente collimanti con il complesso dei valori delineato nella fonte che li ospita, elemento fondativo dello stesso diritto penale, ma anche

[1] Per una disamina dell'assiologia dei valori tutelati nell'esperienza costituzionale italiana, europea e internazionale, sia consentito il rinvio a C. PAONESSA, *Gli obblighi di tutela penale. La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari*, Edizioni ETS, Pisa, 2009, p. 65 ss., p. 119 ss.

e, specificamente, per la precipua funzione di garanzia da essi assolta. Emblematica, in proposito, è l'unica clausola di incriminazione presente nel nostro ordinamento – l'art. 13, comma 4, Cost. – che pone l'obbligo di reprimere penalmente «ogni violenza fisica e morale sulle persone comunque sottoposte a restrizioni di libertà»[2]: il valore rispetto al quale si trova a soccombere la riserva di legge è la libertà personale, ovvero la stessa garanzia che è alla base della legalità penale[3].

Ad una visione per così dire "riduzionistica" degli obblighi di tutela, si è affiancata nel tempo una corrente di segno opposto, segnata dalla crescita esponenziale delle richieste di presidio penale di fonte sovranazionale, al cui rispetto l'ordinamento è tenuto a norma dell'art. 117 Cost. Formalmente gli *input* europei di penalizzazione sono ossequiosi della riserva di legge; per poter funzionare, essi necessitano, invero, della loro traduzione in leggi dello Stato e, quindi, della collaborazione del legislatore nazionale. Ma affiorano anche significative peculiarità, che meritano di essere rimarcate. Simmetrica all'amplificazione numerica di questa tipologia di vincoli è, infatti, la variabilità contenutistica degli stessi, a sua volta funzionale ad assicurare, in chiave utilitaristica, l'effettività della politica unionista nei settori di competenza[4]. Si è al cospetto di richieste spesso stringenti in ordine all'*an* e al *quantum* di pena, le quali, nell'esigere dagli Stati membri la punizione di determinati fatti, si spingono, non di rado, a descrivere le connotazioni strutturali della fattispecie incriminatrice e la cornice sanzionatoria, con una marginalizzazione di fatto del legislatore nazionale, che – complice una lettura talvolta cieca dell'obbligo di fedeltà e di leale collaborazione – ne vede fortemente menomata la sua autonomia disciplinare e politico-criminale. Con ciò dimenticando, però, che si tratta del solo soggetto abilitato a produrre norme penali e che l'Unione europea non ha, allo stato, una competenza penale diretta[5].

[2] Imprescindibile è il rimando allo studio di D. Pulitanò, *Obblighi costituzionali di tutela penale?*, in «Riv. it. dir. proc. pen.», 2 (1983), p. 484 ss. Sul carattere «eccezionale e isolato» della tutela penale obbligatoria assicurata dalla disposizione costituzionale, attestato anche dai lavori dell'Assemblea costituente, v., altresì, da ultimo, N. Zanon, *Violenza ai danni delle persone private della libertà: i lavori preparatori dell'articolo 13, comma 4, della Costituzione*, in «Riv. it. dir. proc. pen.», 3 (2024), p. 917 ss. e, parimenti, E. Mazzanti, *Il problema degli obblighi convenzionali di tutela penale. Gli effetti espansivi della penalità derivanti dalla protezione dei diritti umani*, Giappichelli, Torino, 2025, p. 160 ss.

[3] Volendo, ancora, *amplius* C. Paonessa, *Gli obblighi di tutela penale*, cit., p. 26 ss. e, segnatamente, p. 32, nonché Ead., *Vincoli costituzionali e tutela penale: l'occasione per fare il punto, a partire da alcune recenti vicende giurisprudenziali*, in «Leg. pen.», 1 (2021), p. 251.

[4] È sufficiente menzionare, a titolo meramente esemplificativo, la direttiva (UE) 2024/1226 relativa alla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673, quest'ultima relativa alla lotta al riciclaggio mediante il diritto penale; la direttiva (UE) 2017/1371 sulla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale; la direttiva (UE) 2014/57 concernente le sanzioni penali in caso di abusi di mercato; si veda pure la direttiva (UE) 2024/1203 sulla tutela penale dell'ambiente, che sostituisce le direttive 2008/99/CE e 2009/123/CE, con le criticità relative all'imputazione della responsabilità per colpa, su cui cfr. C. Larinni, *Obblighi europei di incriminazione e responsabilità colposa*, in «Riv. pen.», 5 (2020), p. 458 ss. (consultabile anche in *disCrimen*).

[5] Va da sé che, più si assottiglia la discrezionalità legislativa nell'adattamento delle richieste sovranazionali al diritto interno, più si finisce per accreditare, surrettiziamente, una competenza penale diretta del diritto europeo,

Ferma questa inquadratura di sistema tra obblighi costituzionali ed europei di tutela penale, a cui si affianca – come si è detto – l'ulteriore distinzione tra obblighi valoriali (che hanno dietro la tutela della persona) e obblighi improntati all'efficientismo eurounitario, che certamente non stanno sullo stesso piano, va, nondimeno, evidenziata l'eccezione rappresentata dalla direttiva (UE) 2024/1385 in esame. Emerge qui un volto dell'Unione diverso da quello che si è palesato, per esempio, all'ombra delle note vicende delle false comunicazioni sociali[6] o, più di recente, della sentenza Taricco[7]. A profilarsi è l'immagine di una Europa che si preoccupa di proteggere dei valori e che, per farlo, ambisce a disegnare un'ampia strategia di contrasto al riprovevole fenomeno della «violenza contro le donne» e della «violenza domestica», seguendo un triplice piano di intervento: preventivo, di supporto e assistenza alle vittime, e, appunto, di carattere repressivo.

Sia detto per inciso. La logica efficientista, in realtà, neppure in tale occasione, è completamente oscurata. La direttiva attecchisce come risposta alle difficoltà di ratifica della Convenzione di Istanbul del Consiglio d'Europa[8], di cui ne riprende parzialmente i contenuti. Ma è un efficientismo – si potrebbe dire – "a fin di bene", che punta ad armonizzare a livello europeo, la disciplina di temi oltre modo delicati, che attingono sfere della persona particolarmente sensibili richiedendo – e il dato non manca di essere evidenziato nella stessa direttiva – un approccio "globale". Non è un caso che il testo spinga per l'adozione di una serie di misure che toccano anche il piano processuale (dal potenziamento dell'accesso alla giustizia al rafforzamento di misure protettive e risarcitorie, passando per limitazioni probatorie finalizzate alla salvaguardia di aspetti della vita privata delle vittime) e parimenti investono l'approccio culturale al fenomeno della violenza di genere e domestica (segnatamente con la promozione di campagne o programmi educativi e di sensibilizzazione, volti, tra l'altro, a contrastare gli stereotipi di genere e a promuovere parità e rispetto reciproco).

Un'impostazione, dunque, almeno in linea di principio, olistica quella fatta propria dalla direttiva europea, che non manca di confrontarsi, come si vedrà a breve, anche con dinamiche complesse, quali la violenza (intesa in senso lato) online, che non trovano invece adeguato spazio di riconoscimento entro l'apparato convenzionale.

allo stato inesistente; in questi termini, F. GIUNTA, *Europa e diritto penale. Tra linee di sviluppo e nodi problematici*, in «Criminalia» (2019), p. 289.

[6] Per una ricognizione delle censure di illegittimità sollevate, v., per tutti, E. MUSCO, *I nuovi reati societari*, 3ª ediz., Giuffrè, Milano, 2007, p. 119 ss.

[7] Sulla vicenda, definitivamente chiusa dalla Corte costituzionale con la sentenza n. 115/2018, nell'ambito di un ampio dibattito, cfr., *ex plurimis*, i contributi raccolti nel volume *Dal giudice garante al giudice disapplicatore delle garanzie. I nuovi scenari della soggezione al diritto dell'Unione europea: a proposito della sentenza della Corte di giustizia Taricco*, a cura di C. Paonessa e L. Zilletti, Pacini Giuridica, Pisa, 2016, nonché F. GIUNTA, *La Consulta riafferma la tradizione culturale del diritto penale costituzionale: una sentenza davvero "rivoluzionaria"*, in «Giur. cost.», 3 (2018), p. 1311 ss.

[8] B. PEZZINI, *Una Direttiva in materia di lotta alla violenza contro le donne e alla violenza domestica*, in *Quad. cost.*, 2024, fasc. 3, p. 731 ss. Diffusamente, sulla Convenzione di Istanbul, cfr. l'analisi contenuta nel volume *Against Women and Domestic Violence. A Commentary on the Istanbul Convention*, a cura di S. De Vido e M. Frulli, Edward Elgar Publishing, Cheltenham, 2023.

2. *Le direttrici di tutela penale. In particolare: il caleidoscopio della dignità umana*

Nell'approfondire le richieste di presidio penale avanzate dalla direttiva, colpisce, in prima battuta, la loro aggregazione sotto la comune etichetta «Reati di sfruttamento sessuale femminile e minorile e criminalità informatica». Un'etichetta, a ben guardare, alquanto imprecisa, se rapportata ai contenuti che ne sono ricompresi, la quale si spiega in ragione della necessità di agganciare le previsioni europee alla cornice normativa di riferimento per provvedimenti di questo tipo. Come noto, il Trattato di Lisbona consente, infatti, l'adozione di «norme minime relative alla definizione dei reati e delle sanzioni» alla condizione che esse riguardino «sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni»; tra queste, sono indicate nominativamente proprio lo «sfruttamento sessuale delle donne e dei minori», da un lato, e la «criminalità informatica», dall'altro (art. 83, par. 1, TFUE). Il loro richiamo testuale vale, quindi, a fugare ogni possibile dubbio – che pure non si è mancato di manifestare[9] – sulla correttezza della base giuridica utilizzata per il varo del testo normativo.

Lo spettro di tutela è oltre modo ampio; sullo sfondo della repressione del contrasto della violenza contro le donne e della violenza domestica sono posti vari diritti fondamentali: il diritto all'uguaglianza e alla parità di trattamento (considerando n. 2), «il diritto alla dignità umana, il diritto alla vita e all'integrità della persona, la proibizione di pene o trattamenti inumani o degradanti, il diritto al rispetto della vita privata e familiare, il diritto alla libertà e alla sicurezza, il diritto alla protezione dei dati di carattere personale, il diritto alla non discriminazione, compresa quella basata sul sesso, e i diritti del minore» (considerando n. 3).

Ciononostante, l'impressione è che la protezione giuridica che si intende approntare fatichi ad affrancarsi dalle tradizionali cornici della libertà sessuale e della libertà morale. Il dato è evidente specialmente con riguardo al primo filone di obblighi che attiene alla necessità di sanzionare penalmente, anche in forma tentata (art. 9, par. 3, della direttiva (UE) 2024/1385), le condotte di «mutilazioni genitali femminili» e di «matrimonio forzato», peraltro già contemplate dalla Convenzione di Istanbul. Si tratta di *input* – merita evidenziarlo – ad "impatto zero" sul nostro ordinamento, da tempo adempiente sul punto. Alle indicazioni contenute negli artt. 3 e 4 della direttiva (UE) 2024/1385 fanno da *pendant*, infatti, le previsioni incriminatrici dell'art. 583-*bis* c.p. e dell'art. 558-*bis* c.p., rispettivamente inserite nel codice penale dalla l. 9 gennaio 2006, n. 7 («Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile») e dalla l. 19 luglio 2019, n. 69 (c.d. Codice Rosso). La prima delinea una autonoma figura di lesioni personali particolarmente gravi, secondo la logica tipica del

[9] E. Bergamini, *Combating Violence against Women and Domestic Violence from the Istanbul Convention to the EU Framework: The Proposal for an EU Directive*, in «Freedom, Security & Justice: European Legal Studies», 2 (2023), p. 28 ss.

diritto penale simbolico, valendo a stigmatizzare non solo il fatto in sé, ma anche le sue radici culturali, incompatibili con la concezione della persona come portatrice di diritti inalienabili, tra cui quello all'integrità e alla vita sessuale[10]. E lo stesso può dirsi per l'art. 558-*bis* c.p. Prima della sua introduzione, per la repressione penale di queste condotte si poteva attingere a diverse fattispecie nelle quali contestualizzare simili vicende (es. gli artt. 572, 605, 610, 609-*bis*, 609-*quater* c.p.). L'inserimento di una disposizione apposita è valso, ad ogni modo, a valorizzare precipuamente la libertà di autodeterminarsi sulla propria vita sentimentale e matrimoniale; è su questo, infatti, che si appunta lo specifico disvalore della fattispecie, nel quadro di un fenomeno comunque complesso, che può assumere forme diverse a seconda del contesto in cui ha luogo[11]. Anche tenuto conto di tali fattori, il tentativo di costringere o indurre taluno al matrimonio ai sensi dell'art. 558-*bis* c.p. sembra apparire una misura di per sé sufficiente a soddisfare l'ulteriore indicazione europea di sanzionare penalmente il fatto di «attirare un adulto o un minore nel territorio di un paese diverso da quello in cui risiede allo scopo di costringerlo a contrarre matrimonio» (art. 4, lett. *b*, della direttiva (UE) 2024/1385); diversamente si consentirebbe ad un eccessivo arretramento della tutela rispetto al bene giuridico protetto[12], senza considerare le difficoltà sul versante probatorio.

Più articolato il secondo filone di obblighi che comprende la repressione di plurime forme di "violenza digitale", tra cui la «condivisione o manipolazione non consensuale di materiale intimo o manipolato», lo «stalking online» e le «molestie online», l'«istigazione alla violenza o all'odio online» (artt. 5-8 della direttiva (UE) 2024/1385). Le condotte – accomunate tutte dal necessario impiego di «tecnologie dell'informazione e della comunicazione (TIC)», ossia da quell'insieme di tecniche che permettono di ricevere, elaborare, trasformare e trasmettere informazioni (dati digitali) – prendono in considerazione profili diversi: alcune attengono al momento genetico, altre a quello della diffusione, altre ancora all'uso strumentale di determinati "contenuti" veicolati online.

Ad emergere in modo preponderante è, per lo più, l'esigenza di salvaguardare la tranquillità psichica e la libertà di autodeterminazione della vittima in ordine alle modalità di conduzione della propria vita privata. Si tratta di istanze di tutela, anche queste, che trovano già, in larga misura, una risposta sul versante interno. La fattispecie incriminatrice degli atti persecutori (art. 612-*bis* c.p.), segnatamente l'ipotesi aggravata del secondo comma, che fa riferimento alla commissione del fatto «attraverso strumenti informatici o telematici», appare, infatti, in grado di dare copertura sia all'*input* di punire l'impiego – ripetuto e continuativo – di strumenti di monitoraggio dei movimenti e delle attività della vittima, anche all'insaputa della stessa («senza il suo

[10] F. GIUNTA, *Le mutilazioni genitali femminili*, in *Sussidiario di diritto penale, Parte speciale*, a cura di F. Giunta, in «disCrimen» (sezione "Testi e iper-testi"), agg. 2 maggio 2023, cap. XVI, § 5; cfr., altresì, C. DE MAGLIE, *I reati culturalmente motivati. Ideologie e modelli penali*, Edizioni ETS, Pisa, 2010, p. 41 ss.

[11] In tema, C. RIGONI, *I matrimoni forzati: una prospettiva europea*, in «Foro it.», 3 (2023), V, c. 135 ss.

[12] Rileva questa criticità anche A. MASSARO, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica: il possibile impatto sull'ordinamento italiano*, in «Sistema penale», 3 (2025), p. 117.

consenso o un'autorizzazione legale a tal fine»), qualora tali condotte possano arrecarle «un danno grave»[13] (art. 6 della direttiva (UE) 2024/1385, «stalking online»), sia, nella sostanza, a talune situazioni rientranti nelle «molestie online» (art. 7 della direttiva (UE) 2024/1385). Sotto quest'ultimo profilo, sorvolando sulla non ineccepibile formulazione linguistica degli obblighi in questione, il citato disposto dell'art. 612-*bis* c.p. consentirebbe di inglobare, invero, tanto il fatto di «assumere, in modo ripetuto o continuativo, comportamenti minacciosi nei confronti di una persona, almeno qualora tali comportamenti comportino il rischio di commettere reati, tramite TIC, se tali comportamenti possono indurre la persona in questione a temere seriamente per la propria incolumità o per l'incolumità delle persone a carico» (lett. *a*), quanto quello di «adottare pubblicamente, insieme ad altre persone, tramite TIC, comportamenti minacciosi o ingiuriosi nei confronti di una persona, qualora tale comportamento possa arrecare un grave danno psicologico alla persona in questione» (lett. *b*)[14]. Non c'è dubbio che, astrattamente, le condotte anzidette potrebbero ricadere, a seconda delle circostanze concrete, anche sotto altre previsioni incriminatrici già esistenti; il ventaglio delle possibilità, tuttavia, deve tenere conto del *quantum* sanzionatorio delineato, in proposito, dalla direttiva, che fissa, in effetti, la soglia minima della punibilità all'applicazione della «reclusione non inferiore nel massimo a un anno» (art. 10, par. 4, della direttiva (UE) 2024/1385). Ciò renderebbe plausibile, per fare un esempio, la loro attrazione eventualmente nella diffamazione aggravata *ex* art. 595, comma 3, c.p., ma non nella minaccia, pure se grave, la cui previsione di pena massima è «fino a un anno» (art. 612, comma 2, c.p.), a meno di non procedere ad un ritocco del trattamento punitivo della fattispecie.

Con riguardo alle restanti ipotesi di «molestie online» la cui incriminazione è sollecitata in sede europea, esse fotografano, da un lato, la pratica del c.d. *cyberflashing*, ossia l'invio – non richiesto – di «un'immagine, un video o altro materiale analogo raffigurante i genitali», dall'altro lato, quella del c.d. *doxing*, concernente la diffusione di «materiale contenente i dati personali di una persona». L'orizzonte della tutela non guarda al fatto in sé, ma alle sue ripercussioni pregiudizievoli sulla persona offesa: nel primo caso, infatti, la condotta deve essere tale da poterle arrecare «un grave danno psicologico» (art. 7, lett. *c*, della direttiva (UE) 2024/1385); nel secondo, in termini ancora più pregnanti, è richiesta la finalità di «istigare altre persone ad arrecare un danno fisico o psicologico grave» (art. 7, lett. *d*, della direttiva (UE) 2024/1385). Se è vero che non si dispone di incriminazioni *ad hoc*, basta prestare mente alla casistica

[13] Nel considerando n. 21 della direttiva (UE) 2024/1385 si evidenzia che «di solito l'autore del reato fa un uso improprio della tecnologia per rendere più pressante un comportamento coercitivo e controllante, la manipolazione e la sorveglianza, aumentando così la paura, l'ansia e il graduale isolamento della vittima da amici e familiari e dal contesto professionale», lasciando intendere, pur nell'ambiguità del testo dell'art. 6, che il danno non sia, dopotutto, slegabile dalla condotta.

[14] Sottolinea S. Braschi, *La nuova direttiva sulla lotta alla violenza contro le donne e alla violenza domestica e le sue ricadute nell'ordinamento nazionale*, in «Dir. pen. proc.» (2024), p. 1375 che l'obbligo di incriminazione si indirizzerebbe a quegli Stati membri che non dispongono già di fattispecie precipuamente volte a sanzionare lo *stalking*, con un impulso quindi ad armonizzare la disciplina nel contesto europeo.

più frequente che coinvolge situazioni di questo tipo per avvedersi che non si tratta di esigenze sguarnite di protezione nel contesto nazionale, potendo ricadere, in ipotesi, nella fattispecie contravvenzionale dell'art. 660 c.p. (la quantificazione sanzionatoria minima di cui si è detto non comprende, infatti, il *cyberflashing* di cui alla lett. *c* dell'art. 7 della direttiva) oppure, ancora, nelle norme volte a reprimere l'illecita diffusione di dati personali ai sensi del c.d. Codice della *privacy*, sempre che, va da sé, non ricorrano i presupposti operativi di fattispecie più gravi.

C'è, infine, anche dell'altro da considerare. Tra le pieghe delle richieste di penalizzazione sembrano ritagliarsi uno spazio autonomo, infatti, istanze di tutela esorbitanti il grande contenitore della libertà morale, che pure le include, strettamente legate alla necessità di proteggere il valore identitario della persona, inteso sia come percezione soggettiva di sé, sia come immagine sociale proiettata all'esterno. Alcuni sviluppi della normativa europea parrebbero, in particolare, mettere in luce forme di offesa che, degradando profondamente l'umanità della persona, tendono a configurarsi come autentiche lesioni della dignità. Siffatto valore, che innegabilmente manifesta molteplici sfaccettature nel campo della tutela dei beni personali[15], opererebbe, dunque, come criterio di legittimazione dell'intervento punitivo. Sennonché, la sua forte connotazione etica, da un lato, e il relativismo ideologico che lo contraddistingue, dall'altro, ne rendono l'impiego alquanto controverso, con il rischio concreto che tale parametro finisca per impattare negativamente sulla reale consistenza dell'offesa. Da qui l'esigenza di definire con chiarezza quali aspetti della dignità umana siano meritevoli di effettiva protezione giuridica, sì da evitare di tramutare in oggetto di repressione penale impostazioni ideologiche del tutto legittime e innocue, che andrebbero, però, ad alimentare una visione esclusivamente vittimocentrica della materia.

Nel contesto della direttiva (UE) 2024/1385, la questione si pone specificamente per il vincolo a punire l'istigazione alla violenza o all'odio nei confronti di un gruppo di persone o di un membro di detto gruppo «definito con riferimento al genere» (art. 8). Sebbene il testo normativo non offra alcuna precisazione in ordine al suo significato, il concetto rimanda, implicitamente, alla disciplina internazionale, identificandosi con l'insieme di «ruoli, comportamenti, attività e attributi socialmente costruiti che una determinata società considera appropriati per donne e uomini» (art. 3, lett. *c*, della Convenzione di Istanbul, ratificata in Italia con la l. 27 giugno 2013, n. 77). Il problema di fondo, in tale ambito, è distinguere tra necessità del diritto penale e spinta meramente moralizzatrice di comportamenti assistita dal diritto penale, al quale verrebbe riconosciuta, in altre parole, una sorta di funzione palingenetica, ma sulla cui efficacia, tuttavia, si ha più di un buon motivo per dubitare[16]. Se questo è il crinale, va da sé che la carica offensiva andrebbe selettivamente cercata non nella semplice manifestazione di opinioni o ideologie, bensì in atti che ledono concretamente aspetti ben

[15] F. Giunta, *Il valore della dignità*, in «Sussidiario di diritto penale», cit., cap. XIV, § 9.

[16] G. Fiandaca, *Prima lezione di diritto penale*, Laterza, Bari-Roma, 2017, pp. 49-50, 135; F. Giunta, *Ghiribizzi penalistici per colpevoli. Legalità, "malalegalità", dintorni*, Edizioni ETS, Pisa, 2019, p. 179.

definiti della dignità, centrata su principi costituzionali e universalmente riconosciuti, perché largamente condivisi e culturalmente non divisivi, in linea con quanto previsto, ad esempio, per l'istigazione ad atti di violenza per motivi di discriminazione razziale, etnica e religiosa (art. 604-*bis* c.p.)[17].

Non mancano, ad ogni modo, situazioni in cui la dimensione offensiva è più facilmente apprezzabile in ragione della natura stessa della condotta. Così per quelle forme di «condivisione non consensuale di materiale intimo o manipolato» consistenti nel «produrre, manipolare o alterare e successivamente rendere accessibile al pubblico tramite TIC immagini, video, o analogo materiale in modo da far credere che una persona partecipi ad atti sessualmente espliciti, senza il consenso della persona interessata, qualora tali condotte possano arrecare un danno grave a tale persona» (art. 5, par. 1, lett. *b*, della direttiva (UE) 2024/1385). Il *background* di questo specifico obbligo di incriminazione risiede nella pratica del c.d. *deepfake*, dalla cui perimetrazione occorre, pertanto, partire per una corretta valutazione delle sue implicazioni giuridiche.

3. *Il fenomeno "*deepfake*"*

Sul piano linguistico, *deepfake* è classificabile come "parola macedonia": il neologismo «mette insieme», infatti, «più parole maciullate» – la locuzione *deep learning*, contratta al solo aggettivo – «con una parola intatta» – il sostantivo *fake* –[18]. La sincrasi è presa in prestito direttamente dall'inglese e, come tale, riversata nella lingua corrente.

La scelta risponde ad una logica, evidentemente, di sintesi espressiva. Il primo segmento – *deep learning* – reca in sé una complessità esplicativa che la semplice trasposizione linguistica – "apprendimento profondo" o, se si preferisce, "approfondito" – non è in grado di rendere. L'espressione, che è gergale, allude ad un tipo di apprendimento automatico, identificativo di un insieme di tecniche che, tra le altre cose, «permettono all'intelligenza artificiale di imparare a riconoscere le forme»[19], utilizzando plurime stratificazioni di dati, fondamentalmente imitandone l'elaborazione da parte del cervello umano[20]. Meno problematico il secondo segmento: *fake* ha una portata concettuale ben definita; indica ciò che è falso, finto, non rispondente al vero.

[17] Viene comunque lasciata agli Stati membri la possibilità di «decidere di configurare come reato soltanto le condotte atte a turbare l'ordine pubblico o che sono minacciose, offensive o ingiuriose»; così l'art. 8, par. 2, della direttiva (UE) 2024/1385, che porterebbe nel nostro ordinamento a valorizzare l'istigazione a delinquere di cui all'art. 414 c.p. Sul punto, A. Massaro, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., p. 122.

[18] In questi termini B. Migliorini, *Uso ed abuso delle sigle*, in Id., *Conversazioni sulla lingua italiana*, Le Monnier, Firenze, 1949, p. 89.

[19] Così la voce *Deepfake*, inserita nel 2018 nella sezione *Neologismi* dell'Istituto dell'Enciclopedia Italiana Treccani: https://www.treccani.it/vocabolario/deepfake_(Neologismi)/.

[20] I.H. Sarker, *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*, in «SN Computer Science», 420 (2021), p. 2 ss.

Altrove si è provato a sperimentare la strada di composti autoctoni: *ultrasuplantación* in Spagna[21], *hypertrucage* in Francia[22], ad esempio. Ma si tratta di tendenze allo stato isolate, che non sono state in grado di scalzare *in toto* l'impiego in purezza dell'anglicismo, anche perché la sua resa traduttiva, pur nella fedeltà all'originale delle varianti proposte, perde in termini di descrittività, non consentendo quell'automatica correlazione all'aspetto tecnologico che è il tratto maggiormente caratterizzante l'espressione *deepfake*. L'accento sulla qualificazione della falsificazione finisce per offuscare, invero, proprio la modalità che dà corso alla stessa, che, come si vedrà a breve, con i suoi automatismi, è esattamente ciò che rende tale attività particolarmente pervasiva e perniciosa. Si spiega così come mai, anche da noi, formule sostanzialmente analoghe – "falso profondo", pure nella versione "profondo falso"[23], contenente una implicita suggestione cinematografica, o, ancora, l'impiego di traducenti quali "ultrafalso", "iperfalsificazione", "falso iperrealistico", "ipermanipolazione"[24] – non hanno mai attecchito.

Tutto ciò, ad ogni modo, non deve sorprendere. L'universalità del dato linguistico, in fondo, è il riflesso della globalità delle manifestazioni che esso riassume. Il *deepfake* si inquadra, segnatamente, nel complesso di quelle tecniche che consentono di operare *collage* di realtà per mistificare la realtà stessa, identificandone l'ultima frontiera: la forma più evoluta e sofisticata, ma, ad un tempo, alla portata di tutti. Il suo funzionamento si basa, in estrema sintesi, su reti neurali che esaminano ampi *set* di dati per apprendere come replicare le espressioni facciali, i manierismi, la voce e le inflessioni di una persona e ciò consente agli utenti, pure a quelli con scarse competenze tecniche e pressoché privi di capacità artistica, di modificare video, scambiare volti (*face swapping*), alterare espressioni e sintetizzare il parlato con una precisione quasi perfetta[25].

Proprio questa attitudine a toccare nel profondo, in modo deliberato e intenzionale, l'identità della persona, nelle manifestazioni che la contraddistinguono come un *unicum*, ha finito per determinare una torsione ermeneutica dell'espressione *deepfake*. Se, riguardato nel suo significato etimologico, l'intreccio tra *deep learning* e *fake* è "neutro", perché indica niente più che una tecnica molto raffinata di falsificazione che sfrutta le amplissime possibilità messe a punto dalle applicazioni dell'intelligenza artificiale, va dato atto che l'espressione – quasi subito dall'esordio – ha visto sempre più

[21] E. Simó Soler, *Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho*, in «InDret», 2 (2023), p. 496; M. Santisteban Galarza, *La criminalización de las ultrafalsificaciones (con especial atención a las implicaciones de la normativa europea de servicios digitales e inteligencia artificial)*, in «Revista de derecho penal y criminología», 31 (2024), p. 211 ss.

[22] S. Renaudin, *Le deepfake ou l'hypertrucage. Connaitre la règlementation et s'en prémunir*, in «Village de la Justice», 19 febbraio 2025.

[23] M. Gramellini, *Profondo falso*, in *Corriere della sera*, 26 settembre 2019.

[24] Vedi il *topic* sull'individuazione di un possibile traducente dell'espressione *deepfake* nello spazio di discussione sulla lingua italiana (*Cruscate*) aperto su *Achyra* (https://www.achyra.org).

[25] M. Westerlund, *The Emergence of Deepfake Technology: A Review*, in «Technology Innovation Management Review», 9 (2019), p. 40. V. anche G.M. Caletti, Habeas corpus *digitale. Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Giappichelli, Torino, 2024, p. 160 ss.

polarizzare il suo significato sul prodotto distillato, ossia sul contenuto creato, che altro non è se non un "falso convincente"[26], giungendo, in pratica, ad identificarsi con esso.

L'associazione più immediata che è invalsa nella prassi è quella che salda il *deepfake* con il materiale audiovisivo. Non è un caso che uno tra i più noti dizionari della lingua italiana spieghi l'espressione come il «filmato che presenta immagini corporee e facciali catturate in Internet, rielaborate e adattate a un contesto diverso da quello originario tramite un sofisticato algoritmo»[27]. La categoria, in realtà, è più ampia. Di questo se ne ha piena contezza in ambito giuridico, tant'è che il recente regolamento UE 2024/1689 (*AI Act*) considera *deepfake* – con un'evidenza anche plastica della sineddoche che fonde la tecnologia nel suo *output* – «un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona» (art. 3, par. 1, n. 60)[28].

La fenomenologia del *deepfake*, come si può intuire, è oltre modo varia. Si passa dal materiale artatamente creato a scopo di *divertissement* e, in generale, "innocuo" a quello, invece, ben più "compromettente", dove frasi mai pronunciate e situazioni mai vissute, possono avere fortissimi riverberi sul piano relazionale e sociale di un individuo, attribuendo o facendo equivocare modi di essere della sua persona, che ne minano nel profondo l'aspetto identitario. Il grado di verosimiglianza del prodotto finale è elevato: esso è facilmente confondibile con ciò che potrebbe essere autentico, perfino (anzi verrebbe quasi da dire soprattutto) quando è incredibile.

Molteplici ne sono gli impieghi. La *misinformation* passa anche per l'utilizzo di questi strumenti altamente decettivi, agevolmente strumentalizzabili al fine di convogliare consensi sul piano politico[29], manipolare strategicamente un determinato pubblico o creare ulteriori fratture nelle divisioni già esistenti[30], finanche pregiudicare, in certi contesti, la sicurezza nazionale e il regolare svolgersi della vita democratica[31]. Pur in assenza di dati esaustivi o pienamente attendibili sulla diffusione delle diverse tipologie di *deepfake*, è difficile negare, però, che una componente significativa del fenomeno, sin dalle sue prime manifestazioni, riguardi le alterazioni che toccano la sfera dell'intimità

[26] G.F. Lendvai, G. Gosztonyi, Deepfake *y desinformación. Qué puede hacer el derecho frente a las noticias falsas creadas por* deepfake*?*, in «IDP. Revista de Internet, Derecho y Política», 41 (2024), p. 3.

[27] In questi termini, ancora, la voce *Deepfake*, cit.

[28] Per una contestualizzazione dell'approccio legislativo europeo che, sul piano della disciplina, si limita a prevedere obblighi di trasparenza per i fornitori e i *deployers* di determinati sistemi di IA (segnatamente, considerando n. 134 e art. 50, par. 4), sanzionandone l'inosservanza in via amministrativa (art. 99), cfr. A. Orlando, *La regolamentazione del* deepfake *in Europa, Stati Uniti e Cina*, in «MediaLaws», numero speciale 1 (2024), p. 311 ss.

[29] T. Guerini, Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020, p. 45 ss.

[30] G.F. Lendvai, G. Gosztonyi, Deepfake *y desinformación*, cit., p. 4.

[31] D.K. Citron, R. Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, in «California Law Review», 107 (2019), p. 1776 ss., pp. 1783-1784; G.M. Caletti, Habeas corpus *digitale*, cit., p. 159.

sessuale. Questo tipo di prodotto – si rileva[32] – ha anche un altro triste primato: quello di coinvolgere in prevalenza donne, perpetrando, con forme tecnologicamente avanzate, quella tendenza alla reificazione del corpo femminile – eredità anche di un ancestrale paradigma culturale – che ha da sempre contraddistinto, purtroppo, se pure non in via esclusiva, la pornografia.

4. *L'attuale assetto della regolamentazione nazionale*

Sul piano giuridico, va considerato che, ad oggi, il mero allestimento di *deepfake*, ossia di materiale non veritiero ancorché realistico, non ha di per sé rilevanza penale. Il fenomeno non sfugge, comunque, completamente alle maglie punitive.

La diffamazione (per lo più nella forma aggravata del terzo comma, che fa riferimento all'impiego di qualsiasi mezzo di pubblicità) è certamente in grado di dare una cornice legale a tale tipologia di contenuti, nella misura in cui la loro diffusività si riverberi sulla reputazione dei soggetti coinvolti.

Ancora, i *deepfake* potrebbero acquisire una rilevanza strumentale nel contesto della realizzazione di fattispecie ben più gravi: l'estorsione (art. 629 c.p.), gli atti persecutori già menzionati (art. 612-*bis* c.p.), la pedopornografia (se sono coinvolti minori), ne sono alcune esemplificazioni.

Meno plausibile appare, invece, l'applicabilità della fattispecie di sostituzione di persona (art. 494 c.p.), la quale rasenta il parossismo implicando che sia lo stesso autore del *deepfake* a dover sostituire illegittimamente la propria all'altrui persona, per indurre taluno in errore. Ipotesi che, va da sé, non può escludersi *a priori* (si pensi al caso di chi, intrattenendo una relazione con persona già coniugata, altera un video che ritrae se stesso in atteggiamenti intimi con persona diversa dall'amante, sostituendone poi il suo volto con quello dell'amante; il materiale così confezionato viene successivamente reso pubblico affinché il coniuge dell'amante, vedendolo, decida di interrompere il rapporto chiedendo la separazione), ma che di certo non fotografa la casistica più frequente.

Con riferimento specifico al deplorevole fenomeno dei *deepfake* pornografici, il dato che più di ogni altro viene enfatizzato è l'impossibilità di ricondurlo alla fattispecie deputata alla repressione della diffusione illecita di materiale (immagini o video) «sessualmente espliciti» (art. 612-*ter* c.p., c.d. *revenge porn*). A tale norma, come noto, nel nostro ordinamento è affidato il contenimento degli effetti perversi legati alla "digitalizzazione" (auto o eteroprodotta) dell'intimità sessuale, quale nuova modalità di estrinsecazione della libertà sessuale[33], con la previsione di un trattamento sanzionatorio assai

[32] J. Bailey, S. Dunn, *Recurring Themes in Tech-Facilitated Sexual Violence Over Time. The More Things Change, the More They Stay The same*, in *Criminalizing Intimate Image Abuse: A Comparative Perspective*, a cura di G.M. Caletti e K. Summerer, Oxford University Press, Oxford, 2024, 50.

[33] C. Paonessa, *Ai confini del c.d.* Revenge porn. *Tessere di un mosaico normativo*, in «Criminalia» (2021), p. 285.

rigoroso (reclusione da 1 a 6 anni e multa da 5.000 a 15.000 euro), facilmente incrementabile se il fatto è commesso «attraverso strumenti informatici o telematici».

Per come è stata congegnata, tale fattispecie incriminatrice ha un ambito di operatività piuttosto stringente. Non deve esserci, ovviamente, il consenso alla diffusione da parte delle persone «rappresentate», ma è richiesta altresì la «destinazione privata» delle immagini o dei video in questione. Come a dire: la fattispecie ha quale retroterra inespresso – e quindi come presupposto – la formazione "intra-relazionale" del materiale "a contenuto sessualmente esplicito", ossia la formazione del materiale ad opera degli stessi soggetti che ivi sono ritratti, sia essa condivisa o meno da tutti: tanto nel caso in cui il materiale venga realizzato in modo consensuale – senza inganno, alla luce del sole – tra i soggetti coinvolti, quanto nel caso in cui sia realizzato da parte di uno (o di alcuni) soltanto dei soggetti coinvolti all'insaputa dell'altro (o degli altri)[34]. Il bersaglio della tutela, come non si è mancato di mettere fin da subito in evidenza, è la fuoriuscita di quel particolare tipo di materiale dal circuito ristretto (confidenziale) nel quale doveva rimanere confinato[35], che – giova sottolinearlo – non implica necessariamente un legame affettivo, né una determinata forma di manifestazione "giuridica"; tali situazioni ove ricorrenti, fanno scattare semmai l'aggravante speciale del terzo comma, che determina un aumento di pena là dove la condotta sia stata realizzata dal «coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa».

Ne consegue che il *mashup* digitale, quale combinazione (generalmente) di volti, corpi e voci di persone reali con corpi che possono essere altrettanto reali o creati artificialmente, sfugge all'ambito operativo della fattispecie. E non solo perché il *deepfake* prescinde dall'allestimento "lecito" del materiale oggetto di divulgazione. Ma anche perché il peculiare perimetro dell'art. 612-*ter* c.p., per come disegnato dal legislatore, non può che guardare unicamente al materiale che abbia un contenuto sessualmente esplicito "genuino".

Così pure deve dirsi, per completare il quadro, a proposito delle interferenze illecite nella vita privata (art. 615-*bis*, comma 2, c.p.) e del delitto di riprese e registrazioni fraudolente (art. 617-*septies* c.p.). Le due fattispecie potrebbero sì fornire tutela nel caso della diffusione di materiale realizzato e formato da un terzo all'esterno di un contesto relazionale, ma solo se l'atto sessualmente esplicito è quello ritratto o ripreso in un luogo di privata dimora o in un contesto comunque riservato, ossia, anche qui, se è "autentico". Nessuna delle due norme consente, all'evidenza, di porre l'accento sull'attività manipolativa che è il tratto qualificante del *deepfake*.

[34] C. Paonessa, *Ai confini del c.d.* Revenge porn, cit., p. 288 ss.; cfr., altresì, D. Micheletti, *L'*interversio pubblicationis *quale elemento costitutivo della fattispecie di* Revenge porn, in «disCrimen», 1 (2022), p. 246.

[35] Trib. Reggio Emilia, 22 novembre 2021, n. 528, in «disCrimen», 7 gennaio 2022, richiamata da D. Micheletti, *L'*interversio pubblicationis *quale elemento costitutivo della fattispecie di* Revenge porn, cit., secondo cui l'inciso «destinati a rimanere privati» si presta a circoscrivere l'oggetto materiale del reato solo alle immagini sessualmente esplicite condivise o volontariamente realizzate «dalla coppia all'interno del contesto relazionale», in un ambito quindi «connotato da reciproca fiducia».

5. *La condivisione non consensuale di materiale intimo o manipolato nella prospettiva europea e il suo possibile impatto sull'art. 612-*ter *c.p.*

Come accennato, nuovi scenari parrebbero dischiudersi sulla scia della direttiva (UE) 2024/1385, segnatamente per effetto degli obblighi finalizzati alla repressione della «condivisione non consensuale di materiale intimo o manipolato» (art. 5), la cui attuazione, sotto vari profili, andrebbe ad intersecarsi con l'assetto di tutela già definito dall'art. 612-*ter* c.p.

La disposizione interna risulterebbe in linea di massima conforme alla prospettiva regolativa ora assunta dall'Europa. Quest'ultima, invero, limita l'oggetto della tutela soltanto al materiale «ritraente atti sessualmente espliciti o le parti intime di una persona», in luogo di quello «a contenuto sessualmente esplicito» della disposizione nazionale[36], agganciando la punibilità sempre al potenziale «danno grave» arrecato alle persone ritratte (art. 5, par. 1, lett. *a*), là dove, invece, il «nocumento», nell'art. 612-*ter* c.p., configura unicamente il dolo specifico della condotta dei c.d. secondi distributori (comma 2), ossia di chi abbia ricevuto o acquisito il materiale senza averlo realizzato o sottratto (c.d. primi distributori, di cui al comma 1).

Una maggiore incisività potrebbe, ad ogni modo, discendere dalla mancanza, nella direttiva europea, di qualsivoglia riferimento alla "destinazione privata" del materiale diffuso. Ciò potrebbe portare, di risulta, a ritenere inoperativa l'attuale limitazione situazionale dell'art. 612-*ter* c.p. di cui si è detto in precedenza (cfr. *retro* § 4), consentendo l'applicazione della previsione incriminatrice anche ai casi in cui è il terzo "estraneo" al contesto relazionale a realizzare o acquisire il materiale (che poi diffonde) in cui sono ritratti o ripresi altri soggetti. L'eventuale estensione permetterebbe di abbracciare, di conseguenza, tutte quelle situazioni, particolarmente riprovevoli, di coartata formazione delle immagini sessualmente esplicite; si pensi alla diffusione di immagini a contenuto sessualmente esplicito rappresentative di fatti di reato (ad esempio, quelle realizzate nell'ambito di una violenza sessuale). Sennonché sotto il rigore sanzionatorio dell'art. 612-*ter* c.p. dovrebbero farsi ricadere parimenti le condotte diffusive di immagini sessualmente esplicite, formate da terzi, che abbiano come protagonisti soggetti sì inconsapevoli delle riprese, ma che si sono esposti volontariamente o inavvertitamente alla possibile visibilità altrui. Rispetto a tali vicende – può essere utile

[36] Nella lettura giurisprudenziale, la locuzione normativa «non rimanda evidentemente e necessariamente alla diffusione di video o immagini di un organo proprio dell'apparato sessuale-riproduttivo in senso medico-scientifico, né tantomeno allude ad un solo atto sessuale vero e proprio (sulla cui nozione, complessa, molto ci si interroga ai fini dell'integrazione delle diverse fattispecie penali nelle quali essa viene inserita)», ma può riguardare «anche altre parti erogene del corpo umano, come i seni o i glutei, nudi o in condizioni e contesto tali da evocare la sessualità»; in questi termini Cass. pen., Sez. I, 28 marzo-28 agosto 2024, n. 33230, in «Diritto e giustizia», 29 agosto 2024; analogamente cfr. Cass. pen., Sez. V, 5 marzo-27 giugno 2024, n. 25516, in *Ced* rv. 286566-1; Id., 29 marzo-26 luglio 2023, n. 32602, in «Diritto e giustizia», 27 luglio 2023; Id., 22 febbraio-7 aprile 2023, n. 14927, in *Ced* rv. 284576-03. In dottrina, cfr. G. Panebianco, *La diffusione illecita di immagini o video sessualmente espliciti: tra carenze della fattispecie incriminatrice e coadiuvanti extrapenali*, in «GenIUS», 16 novembre 2022, p. 10.

ricordarlo – il vuoto punitivo conseguente all'attuale formulazione dell'art. 612-*ter* c.p. non è stato ritenuto del tutto insensato in dottrina: la non punibilità sarebbe, infatti, la contropartita della depenalizzazione delle fattispecie di atti osceni in luogo pubblico *ex* art. 527, commi 1 e 3, c.p.[37]. Nell'assetto definito dalla direttiva, l'unico limite alla punibilità, in pratica, parrebbe essere quello – in sé scontato – che fa salvi «i principi fondamentali connessi alla libertà di espressione e di informazione e alla libertà delle arti e delle scienze, quali recepiti nel diritto dell'Unione o nazionale» (art. 5, par. 2, della direttiva (UE) 2024/1385 e, parimenti, il considerando n. 20).

Per ciò che più interessa in merito al *deepfake*, al di là di tali aspetti, che comunque non inficerebbero il presupposto – sotteso all'art. 612-*ter* c.p. – della necessaria genuinità del materiale sessualmente esplicito in diffusione, la novità di maggiore rilievo risiede nella espressa apertura della direttiva alla punibilità della diffusione di materiale fasullo, ma tale da poter essere scambiato per vero (art. 5, par. 1, lett. *b*, della direttiva (UE) 2024/1385)[38].

Non si tratta, va subito precisato, di un *passpartout* per la criminalizzazione indistinta del complesso fenomeno. L'obbligo sancito in sede europea riguarderebbe, infatti, soltanto la diffusione non consensuale di materiale prodotto, manipolato o alterato «in modo da far credere che una persona partecipi ad atti sessualmente espliciti».

Non è chiaro, inoltre, se l'obbligo di incriminazione includa o meno i *deepfake* "audio". L'oggetto materiale del reato, per come delineato dalla direttiva, comprende immagini, video e «altro materiale analogo». Se non v'è dubbio che l'audio possa essere assimilato alle immagini e ai video quando viene utilizzato in combinazione o in modo complementare con essi, la mera creazione o manipolazione di tracce audio in modo che suonino come se fossero pronunciate da una persona specifica, sì da far credere che essa «partecipi ad atti sessualmente espliciti», quando in realtà ciò non è mai accaduto, si pone al limite. L'estensione del «materiale analogo» in chiave funzionale, guardando cioè all'esperienza percettiva nel suo complesso, non risulterebbe immune di criticità, in assenza di un'esplicita menzione.

Sebbene la formulazione della previsione normativa non brilli per nitidezza espressiva[39], l'obbligo di incriminazione in esame parrebbe, invece, tagliare fuori – compren-

[37] D. Micheletti, *L'*interversio pubblicationis *quale elemento costitutivo della fattispecie di* Revenge porn, cit., p. 247.

[38] Per G.M. Caletti, Habeas corpus *digitale*, cit., p. 172, il requisito del realismo sarebbe la condizione dell'estensione della punibilità dell'art. 612-*ter* c.p.: «è l'impossibilità (o la grande difficoltà) di distinguere se si tratti di un'immagine vera o falsa, infatti, a fondare la lesione della riservatezza e, dunque, a giustificare l'incriminazione nella più severa cornice della diffusione di immagini sessualmente esplicite. All'opposto, quando l'immagine è evidentemente falsa, sembra prevalere la lesione dell'onore e della reputazione della persona»; in quest'ultimo caso «le ipotesi di "*photoshopping*" grossolani» dovrebbero conseguentemente ricadere «nel perimetro della diffamazione, come peraltro già avviene».

[39] E lo stesso potrebbe dirsi per il considerando n. 19 della direttiva in esame che dovrebbe avere una funzione esplicativa: «Tale reato dovrebbe comprendere anche la produzione, la manipolazione o l'alterazione non consensuale (ad esempio l'editing di immagini), anche mediante l'uso dell'intelligenza artificiale, di materiale in modo da far credere che una persona partecipa ad atti sessuali, purché detto materiale sia successivamente reso

sibilmente – i *deepfake* esclusivamente "virtuali", i cui contenuti cioè non coinvolgono in alcun modo persone reali. Il riferimento, da un lato, al «far credere che una persona partecipi ad atti sessualmente espliciti» e, dall'altro lato, alla mancanza di consenso «della persona interessata», così come l'esplicita richiesta, ai fini della punibilità, che le condotte «possano arrecare un danno grave a tale persona», inducono a ritenere non solo che gli innesti debbano coinvolgere parti corporee di persone "effettivamente esistenti", reali, ma anche che queste parti, una volta composte nell'immagine, nel video o nell'analogo materiale menzionato, siano in grado di consentire la riconoscibilità e l'identificazione del soggetto a cui appartengono. Non ci sarebbe spazio, dunque, per una previsione analoga a quella (per il vero assai discussa) della pedopornografia virtuale (600-*quater*.1 c.p.), che si configura allorché «il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse». Come noto, infatti, anche alla luce della precisazione contenuta nel comma 2 di ciò che si intende per «immagini virtuali», la fattispecie, non senza perplessità, troverebbe applicazione pure nel caso di figure di minori interamente «realizzate con tecniche di elaborazione grafica», nelle quali difetta «in tutto» l'associazione «a situazioni reali»[40]. Si tratta di ipotesi prive di offensività, dirette più che altro a sanzionare la perversione dell'agente, prescindendo da una lesione effettiva del bene tutelato. Con riferimento agli adulti varrebbero gli stessi rilievi critici.

6. *Gli ulteriori risvolti attuativi*

Sulla punibilità del *deepfake*, la direttiva europea muove – è evidente – in una cornice di prudenza, verosimilmente nella consapevolezza delle difficoltà che, su questo terreno, si riscontrano sul versante probatorio e, verrebbe da dire, anche in mancanza, come si è visto, di una definizione unitaria del fenomeno, che non si sottrae, in linea di principio, a rischi di estremizzazione.

Resta irrisolto, in particolare, il nodo della formulazione dell'ipotetica figura di reato: l'*input* dato dalla normativa sovranazionale parrebbe compatibile, infatti, sia con una conformazione della tutela in termini di pericolo concreto che di danno.

Nel nostro ordinamento, l'*iter* di recepimento è iniziato (A.C. 2280)[41], sebbene, per una singolare contingenza temporale, risulta parimenti pendente alla Camera

accessibile al pubblico tramite TIC, senza il consenso dell'interessato. Nel concetto di produzione, manipolazione o alterazione dovrebbe rientrare anche la fabbricazione di video fasulli ma realistici ("deepfake") con persone, oggetti, luoghi o altre entità o eventi molto simili a quelli realmente esistenti, che ritraggono una persona mentre compie atti sessuali, risultando falsamente autentici o veritieri agli occhi altrui».

[40] Cfr., a tal proposito, Cass. pen., Sez. III, 13 gennaio-9 maggio 2017, n. 22265, in *DeJure*, relativa al possesso di cartoni animati *hard*, raffiguranti personaggi con caratteristiche fisiche e comportamentali riconducibili a soggetti minorenni, coinvolti in attività sessuali.

[41] Si tratta del disegno di legge recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2024», il cui testo, già approvato dal Senato (A.S. 1258), è consultabile in https://temi.camera.it.

anche un altro percorso normativo (A.C. 2316), relativo alla discussione del disegno di legge recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»[42], che pure tocca la questione. In quest'ultimo caso, la scelta regolativa del *deepfake* – che, lo si ribadisce, è qui solo occasionalmente interferente con la direttiva europea, non costituendone la diretta attuazione – va nel senso di una criminalizzazione generalizzata del fenomeno e nella sua configurazione come delitto di danno. Si propone, infatti, di inserire nel codice penale una previsione incriminatrice *ad hoc* – l'art. 612-*quater* c.p. – volta a punire, con la reclusione da uno a cinque anni, l'«illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale», ossia la condotta di «chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità»[43]. Non è facile individuare il confine con ciò che rimane fuori dalla sfera della punibilità, che è innegabilmente più ampia di quella fatta propria dalla direttiva (UE) 2024/1385. Gli scenari regolativi restano, dunque, aperti, anche a soluzioni che potranno prescindere da un ritocco diretto, almeno sul punto specifico del *deepfake*, della fattispecie in tema di diffusione di immagini e video a contenuto sessualmente esplicito.

Il legislatore – è questo l'aspetto che merita valorizzare – ha un ruolo molto importante nella fase recettiva dei vincoli sovranazionali, che si concretizza anche nel modo di vedere l'attualizzazione di simili richieste, dando loro, per esempio, quella luce su cui la direttiva non dà indicazioni. Un'attuazione "cieca" del vincolo di fedeltà eurounitaria, assistita dall'obbligo conformativo derivante dall'art. 117 Cost., potrebbe finire per avvalorare, invece, squilibri sanzionatori e scelte che si allontanano dai principi consolidati nella nostra tradizione giuridica.

D'altra parte, neppure sul versante più arato delle prescrizioni obbliganti di matrice costituzionale, il vincolo di penalizzazione è mai stato inteso in chiave meccanicistica, ossia in modo tale da elidere totalmente la discrezionalità legislativa. Anche quando espresso dalla Carta fondamentale, l'obbligo in questione fissa il limite minimale della tutela, che spetta al legislatore concretizzare[44], in conformità con l'assetto penale

[42] Anche tale disegno di legge, presentato dal Presidente del Consiglio dei ministri e dal Ministro della Giustizia, risulta già approvato dal Senato (A.S. 1146); il relativo testo è reperibile sempre in https://temi.camera.it.

[43] Diversa, per fare un raffronto, la soluzione francese dettata dalla l. 21 maggio 2024, n. 449, sulla «messa in sicurezza e regolamentazione dello spazio digitale», che ha introdotto nel *Code pénal* la sezione «Della lesione alla rappresentazione della persona»; nello specifico, l'«*infraction de montage*» (art. 226-8 *Code pénal*), anche a carattere sessuale (art. 226-8-1 *Code pénal*), prescinde dal requisito del danno, punendo «il fatto di rendere noto al pubblico o a terzi» un «*montage*» realizzato con le parole o l'immagine di una persona oppure un «contenuto visivo o sonoro generato da un trattamento algoritmico» che rappresenti sempre l'immagine o le parole di una persona senza il suo consenso, alla condizione che non risulti chiara o non sia fatta menzione di tale natura.

[44] L. Grossi, *I "nuovi" obblighi costituzionali di tutela penale: dall'*an *al* quomodo *dell'incriminazione*, in «Leg. pen.», 1 (2024), p. 238, sottolinea, al riguardo, che «è sul piano del *quomodo* dell'incriminazione che è destinato a trovare composizione il difficile bilanciamento tra i vincoli di tutela penale derivanti da una fonte

dell'ordinamento, in particolare tenendo conto della proporzionalità dell'impiego della pena rispetto al bene giuridico da assicurare, nonché della stessa coerenza della scelta punitiva con le altre previsioni criminose presenti.

Da questa angolazione, guardando agli interventi futuri, può risultare allora utile il parallelismo con la diffamazione, attesa la tendenza dell'onore a formalizzarsi nel bene-immagine. Con una significativa differenza, però, che va rimarcata: la lesione dell'onore, che allude alla stima sociale, può essere, infatti, di per sé giustificata dall'interesse pubblico alla manifestazione del pensiero, quella dell'immagine(-dignità), che identifica il valore identitario della persona in sé e rispetto agli altri, può essere giustificata solo dal consenso scriminante (che rispetto alla diffamazione è un'ipotesi di scuola e inverosimile).

È innegabile che almeno una specifica categoria di *deepfake* – quella a contenuto sessuale – sia offensiva di per sé, quand'anche fosse strumento di critica o di satira. Il fenomeno assume tratti di straordinaria lesività con l'eteroesposizione della propria immagine decontestualizzata, sia nelle fattezze (combinazione con corpo altrui), sia nell'ambientazione (compromettente nella misura in cui interessa la sfera della propria intimità). Si tratta, comunque, di un'offesa disponibile, che dovrebbe proiettare fisiologicamente verso la perseguibilità a querela.

7. *Postilla*

Nelle more della pubblicazione del presente volume, è stata definitivamente approvata la l. 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»[45], per effetto della quale è stato inserito nel codice penale il nuovo art. 612-*quater*, a cui si è fatto riferimento nel paragrafo precedente. Si tratta di un intervento normativo indipendente dall'*iter* di recepimento della direttiva (UE) 2024/1385, allo stato fermo al conferimento di una apposita delega al Governo (l. 13 giugno 2025, n. 91, c.d. Legge di delegazione europea 2024), collocato nell'ambito di una serie di misure volte a promuovere «un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale» (art. 1 l. n. 132/2025).

L'obiettivo perseguito dal legislatore con la nuova previsione di reato – che ne spiega anche la collocazione topografica tra i delitti contro la libertà morale – è quello di offrire «una tutela rafforzata della persona, incentrando l'offensività della condotta sul pregiudizio all'autodeterminazione ed al pieno svolgimento della personalità derivante dalla diffusione di immagini, video, voci falsificati o alterati mediante sistemi di intelligenza

sovraordinata e l'apporto discrezionale connaturato all'esercizio del potere legislativo», delineandosi «un modello incrociato in cui vengono a saldarsi le indicazioni derivanti dalla fonte di rango superiore e le valutazioni discrezionali compiute dal legislatore nel rispetto dei principî costituzionali».

[45] Per un inquadramento d'insieme, cfr. B. FRAGASSO, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura*, in «Sistema penale», 16 ottobre 2025.

artificiale»[46]. Il raggio operativo dell'«illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale», per certi aspetti, va oltre l'*input* dell'art. 5, par. 1, lett. *b*, della direttiva (UE) 2024/1385, per altri, invece, risulta più stringente.

Per un verso, infatti, non opera qui la restrizione all'effetto comunicativo o percettivo prevista dalla normativa sovranazionale, la quale, come si è detto, richiede che l'oggetto materiale del reato – «immagini, video o materiale analogo» – sia tale «da far credere che una persona partecipi ad atti sessualmente espliciti». Nel contesto della nuova incriminazione, se c'è stata una falsificazione o una alterazione effettiva del materiale oggetto di diffusione, ossia un intervento tecnico sulla forma del contenuto rappresentato da «immagini, video o voci» che lo lascia percepire come genuino, ciò basta a conferirgli rilevanza penale, quale ne sia la natura, e, dunque, anche se non riguarda i *deepfake porn*.

Per altro verso, in stretta correlazione a tale aspetto, occorre rilevare che la disposizione nazionale, a differenza di quella europea, non polarizza l'attenzione sul mezzo di comunicazione e diffusione dei contenuti alterati o falsificati – vale a dire sul canale attraverso cui essi sono resi accessibili al pubblico, da identificarsi negli strumenti digitali e telematici in senso ampio (TIC) – bensì esclusivamente sulla modalità tecnica impiegata per la loro manipolazione, ossia sulla tecnologia di intelligenza artificiale utilizzata per generarli. Si allude, evidentemente, all'uso di sistemi particolarmente evoluti e sofisticati, come comprova, del resto, il rimando espresso dell'intervento di riforma (art. 2, comma 1, lett. *a*, l. n. 132/2025) alla definizione di «sistema di intelligenza artificiale» dell'*AI Act*, che, all'art. 3, punto 1, considera tale «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

In sostanza, affinché la nuova fattispecie possa ritenersi integrata, sarà decisivo accertare – attraverso un'indagine di natura essenzialmente informatica – l'avvenuta manipolazione compiuta mediante tali strumenti. È un'operazione questa, però, tutt'altro che agevole, anche perché la stessa norma definitoria europea, con la quale occorrerà confrontarsi, non è priva di profili di ambiguità che sollevano dubbi circa la precisa delimitazione del suo ambito applicativo[47]. Senza contare che la disposizione non richiede una stretta simbiosi tra l'autore della condotta diffusiva e il soggetto che realizza materialmente il contenuto *deepfake*: quest'ultimo può anche essere un terzo, purché consapevole delle specifiche modalità di falsificazione o alterazione impiegate. Parimenti, sarà determinante la verifica della capacità decettiva del prodotto così ottenuto, che dovrà risultare credibile quanto alla sua genuinità.

[46] *Relazione illustrativa* al testo del disegno di legge approvato dal Senato (A.S. 1146), reperibile in https://www.senato.it/.

[47] B. Fragasso, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura*, cit., § 4.

Nel complesso, la fattispecie di nuovo conio abbraccia, in via potenziale, la messa in circolazione di qualsiasi combinazione artefatta tramite intelligenza artificiale di rappresentazioni visive o sonore della persona offesa, qualora ciò avvenga senza il suo consenso, nonché cagionandole, come conseguenza diretta e immediata della diffusione, un danno ingiusto, anche solo di natura non patrimoniale[48]. Se, da un lato, l'art. 612-*quater* c.p. si presta ad offrire, quindi, una tutela aggiuntiva rispetto a quella assicurata dall'art. 612-*ter* c.p., non rientrando, attualmente, i *deepfake* pornografici nel perimetro di tipicità di quest'ultima fattispecie (cfr. *retro* § 4), dall'altro lato, però, non si può trascurare come tale delitto, per la sua ampiezza applicativa, rischi di sovrapporsi ad altre previsioni incriminatrici nelle quali la diffusione di *deepfake* potrebbe già assumere rilievo quale modalità esecutiva del reato (si pensi, soprattutto, alla diffamazione). Ne consegue la necessità di operare un'attenta distinzione tra concorso reale o apparente di norme, in un quadro interpretativo, peraltro, reso ancora più complesso da un ulteriore elemento. La l. n. 132/2025, infatti, in aggiunta al nuovo reato e ad alcune aggravanti speciali per gli attentati contro i delitti politici dei cittadini (art. 294 c.p.), l'aggiotaggio (art. 2637 c.c.) e la manipolazione dei mercati finanziari (art. 185 d.lgs. 4 febbraio 1998, n. 58), quando tali fatti siano commessi «mediante l'impiego di sistemi di intelligenza artificiale», ha introdotto un'aggravante comune, di portata trasversale, che determina un incremento di pena ogniqualvolta il fatto sia stato commesso, sempre «mediante l'impiego di sistemi di intelligenza artificiale», allorché, però, tali strumenti «per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato» (art. 61, n. 11-*undecies*, c.p.)[49]. Nel caso dei *deepfake*, la connessione con l'aggravante appare quasi tautologica: si tratterebbe, infatti, di un'associazione pressoché naturale attesa la loro intrinseca capacità di simulare – specie in assenza di *disclaimer* o filigrane – l'autenticità dei contenuti, anche sfruttando, eventualmente, la fiducia o la buona fede della vittima.

[48] F. Consulich, *Il diritto penale al tempo dell'intelligenza artificiale. Prospettive punitive nazionali dopo l'AI Act*, in «Diritto di difesa», 17 dicembre 2024, § 5. Nella *Relazione illustrativa*, cit., si osserva che «la centralità del consenso, in uno alla previsione della procedibilità a querela, esprimono la cautela della proposta di legge rispetto al tema dell'utilizzo dei sistemi di intelligenza artificiale, non penalizzati in quanto tali, ma nella proiezione offensiva derivante da impieghi che pregiudicano la libertà di autodeterminazione della persona e la sua proiezione nel mondo reale».

[49] L'aggravante è stata aggiunta con numerazione già presente (art. 61, n. 11-*decies* c.p., in precedenza inserito dall'art. 11, comma 1, d.l. 11 aprile 2025, n. 48, conv. in l. 9 giugno 2025, n. 80, c.d. decreto sicurezza, per i reati commessi «all'interno o nelle immediate adiacenze delle stazioni ferroviarie e delle metropolitane o all'interno dei convogli adibiti al trasporto di passeggeri») ed è stata successivamente rettificata con il *Comunicato* pubblicato in *G.U.*, *Serie generale*, 17 ottobre 2025, n. 242.

CYBERSTALKING E CYBERBULLISMO: LE FATTISPECIE "ANALOGICHE" DI FRONTE ALLE ESIGENZE DI TUTELA "DIGITALE"

Antonella Massaro

1. *L'irruzione della realtà digitale e la risposta del diritto penale*

Il diritto penale degli ultimi decenni è stato chiamato più volte a confrontarsi con le esigenze di tutela (im)poste dalle nuove tecnologie, specie quando queste ultime costituiscono lo strumento che si presta alla realizzazione di condotte penalmente rilevanti.

Il legislatore potrebbe optare per diversi modelli di criminalizzazione, a seconda dell'*an* e del *quomodo* di una esplicita valorizzazione delle nuove tecnologie.

Quanto all'*an* di un riferimento esplicito alla realtà digitale, secondo una certa classificazione, dovrebbe distinguersi tra reati cibernetici in senso ampio e reati cibernetici in senso stretto[1].

Nei reati cibernetici in senso ampio, il legislatore prevede elementi di tipizzazione solo implicitamente compatibili con la concreta realizzazione nel *cyberspace*. L'esempio più comune sarebbe offerto dal delitto di diffamazione, posto che l'art. 595 c.p. non contiene alcun riferimento esplicito alle nuove tecnologie, ma la diffamazione online è chiaramente compatibile con gli elementi costitutivi della fattispecie. Secondo questo primo modello, quindi, il legislatore si affida a fattispecie "tecnologicamente neutrali", descritte attraverso elementi costitutivi astrattamente compatibili tanto con una realizzazione "tradizionale" quanto con l'impiego delle nuove tecnologie.

[1] La distinzione tra reati cibernetici in senso stretto e in senso ampio cui si fa riferimento nel testo è quella proposta da L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in «Cybercrime», diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, UTET, Torino, 2019, pp. 87 ss.

I reati cibernetici in senso stretto, invece, si riferirebbero ai casi nei quali la singola fattispecie incriminatrice contiene un elemento essenziale o circostanziale che richiama esplicitamente la realtà cibernetica.

Nell'ambito di questo secondo modello, poi, potrebbero configurarsi (almeno) due diverse soluzioni, relative al diverso modo di valorizzare gli elementi "digitali" della fattispecie.

La prima strada, che è anche quella fino a questo momento prevalente nell'ordinamento italiano, consiste nell'adattamento delle fattispecie incriminatrici tradizionali ai contesti e alle dinamiche della realtà cibernetica. L'uso di strumenti informatici o telematici, in effetti, costituisce spesso una modalità (eventuale) di realizzazione di una condotta che, di per sé, già sarebbe penalmente rilevante: si muove dalla fattispecie offline e, ragionando secondo lo schema basilare della specialità in astratto, si "aggiunge" l'uso di strumenti informatici o telematici, spesso considerato come circostanza aggravante. Questa è, per esempio, la tecnica utilizzata per la fattispecie di atti persecutori (art. 612-*bis*, terzo comma c.p.), ma anche per quella immediatamente successiva di diffusione illecita di foto o video a contenuto sessualmente esplicito (art. 612-*ter* c.p.)[2].

La seconda strada possibile, nell'ambito dei reati cibernetici in senso stretto, muove dalla premessa per cui la realtà digitale e/o virtuale non si riduce a mera "forma di manifestazione" della realtà analogica: quello che spesso viene trattato come elemento specializzante (l'uso di strumenti informatici o telematici), in effetti, produrrebbe implicazioni più "strutturali" sulla descrizione della fattispecie incriminatrice, rendendo opportuno un intervento diverso e ulteriore rispetto al mero ampliamento dell'ambito applicativo di reati già esistenti[3]. La fisionomia e la pervasività assunti dalle nuove tecnologie imporrebbe, detto altrimenti, di ragionare sulla criminalizzazione di offese "nuove": gli strumenti informatici o telematici, lungi dal rappresentare mezzi materiali che, in via meramente eventuale, possono rendere più grave un fatto, potrebbero e dovrebbero incidere in maniera più significativa sulla descrizione della modalità di lesione che caratterizza l'offesa tipica.

[2] L'aggravante relativa all'uso di strumenti informatici o telematici nell'art. 612-*ter* c.p. non manca di suscitare perplessità. La realizzazione del reato descritto dall'art. 612-*ter* c.p. attraverso questi strumenti, in effetti, è la regola: proprio la maggiore insidiosità derivante dall'uso delle nuove tecnologie, semplici da usare e in grado di assicurare una rapida diffusione delle immagini, ha posto l'esigenza di una tutela penale specifica. Il rischio, dunque, è quello di configurare in ogni caso la fattispecie aggravata, con la conseguente applicazione di limiti edittali particolarmente severi: G.M. Caletti, *Libertà e riservatezza sessuale all'epoca di internet. l'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale*, in «Riv. it. dir. proc. pen.», 4 (2019), pp. 2086 ss.

[3] L. Picotti, *Diritto penale e tecnologie informatiche*, cit., p. 53, evidenzia, più in generale, l'esigenza di delineare criteri e regole di imputazione della responsabilità penale adeguati alla nuova realtà, definendo con maggiore chiarezza i connotati dei comportamenti e dei datti penalmente rilevanti, quando gli stessi si commettono o manifestano nel *Cyberspace*.

2. *Il cyberstalking nel codice penale italiano: da reato cibernetico in senso ampio a reato cibernetico in senso stretto*

L'art. 612-*bis* c.p., al secondo comma, prevede che la pena del delitto di atti persecutori è aggravata se, tra l'altro, «il fatto è commesso attraverso strumenti informatici o telematici»[4].

La circostanza aggravante dell'uso di strumenti informatici o telematici, come noto, non compariva nel testo originario dell'art. 612-*bis* c.p., ma è stata introdotta dal d.l. 14 agosto 2013, n. 93 convertito dalla l. 15 ottobre 2013, n. 119. Non sussisteva alcun dubbio, ad ogni modo, sul fatto che la fattispecie di atti persecutori potesse applicarsi anche in presenza di condotte commesse avvalendosi di strumenti digitali[5].

Se, quindi, nella sua versione originaria il delitto di atti persecutori assumeva la fisionomia di un reato cibernetico in senso ampio, per effetto della modifica del 2013 lo stesso è venuto a configurarsi come un reato cibernetico in senso stretto, attraverso lo schema del reato circostanziato.

3. *Le criticità della circostanza aggravante del cyberstalking nell'art. 612-*bis *c.p.*

a) il maggior disvalore riconosciuto in astratto all'uso di strumenti informatici o telematici

L'introduzione della nuova aggravante in riferimento agli atti persecutori non era scontata e, in effetti, non ha mancato di suscitare perplessità.

Le argomentazioni che "giustificano" un aggravamento di pena in caso di condotte commesse avvalendosi delle nuove tecnologie sono sufficientemente note. La rete *Internet* è progressivamente divenuta una tecnologia poco costosa e semplice da utilizzare, garantendo l'anonimato di chi la utilizza e consentendo di raggiungere la vittima in ogni momento, superando altresì una eventuale distanza geografica[6]. A ciò si aggiunge la difficoltà di difesa della vittima, a sua volta conseguenza di una maggiore invasività della condotta che si avvale delle nuove tecnologie[7].

[4] Per un più generale inquadramento del concetto di cyberstalking, anche prendendo in esame ordinamenti diversi da quello italiano, si rinvia a G. Ziccardi, *Cyberstalking e molestie portate con strumenti elettronici: aspetti informatico-giuridici*, in «Rassegna Italiana di Criminologia», 3 (2012), pp. 161 ss.

[5] Cass., sez. VI, 16 luglio 2010, n. 32404, per esempio, precisava che le molestie reiterate potessero concretizzarsi non solo in telefonate e lettere, ma anche in messaggi inviati tramite *Internet* e nell'invio, tramite *Facebook*, di un video a contenuto sessuale.

[6] M.L. Pittaro, *Cyber stalking: An Analysis of Online Harassment and Intimidation*, in «International Journal of Cyber Criminology», 1 (2007), pp. 80 ss.

[7] Così, per esempio, C. Minnella, in *Atti persecutori dopo la separazione coniugale: inquadramento giuridico e tutela cautelare*, in «Il diritto di famiglia e delle persone», 4 (2012), p. 1602, il quale osserva che il cyberstalking può essere più invasivo dello *stalking* tradizionale, specie in ragione della più ampia e incontrollata diffusione tramite meccanismi informatici e della maggiore possibilità di controllo della vittima resa possibile dalle nuove tecnologie.

A fronte, però, della formulazione generale e "tecnologicamente neutrale" dell'art. 612-*bis* c.p., che consentiva senza difficoltà di comprendere nell'ambito applicativo della fattispecie anche condotte di c.d. cyberstalking, non erano mancate voci favorevoli all'omessa indicazione esplicita delle nuove tecnologie da parte del legislatore penale. Si era rilevato, per esempio, il rischio di demonizzare le nuove tecnologie o quello di introdurre norme penali obsolete, incapaci di tenere il passo dell'evoluzione tecnologica[8]. Più in generale, si erano espresse perplessità sulla scelta di criminalizzare in via autonoma, sia pur attraverso una circostanza aggravante, condotte già chiaramente riconducibili alla fattispecie di atti persecutori[9].

La premessa per cui lo *stalking* commesso avvalendosi di strumenti informatici o telematici sia espressione, per il solo utilizzo del mezzo digitale, di un maggiore disvalore rispetto ad altre forme di molestia o minaccia reiterate, in effetti, rischia di provare troppo. Il cyberstalking può rivelarsi, in concreto, maggiormente invasivo nella sfera personale della vittima e, sempre in concreto, può accrescere le difficoltà della persona offesa di arginare la sequenza di condotte moleste o minacciose. Il mero riferimento, in astratto, all'uso di strumenti informatici o telematici, al contrario, non sembrerebbe in grado di offrire una ragionevole selezione delle condotte da cui deriva un aggravamento sanzionatorio.

La sequenza persecutoria non necessariamente si caratterizza per condotte interamente offline o, per contro, esclusivamente online, con l'ulteriore conseguenza per cui l'aggravante del secondo comma dell'art. 612-*bis* c.p. ben potrebbe ritenersi integrata anche a fronte di condotte digitali "di minima importanza", se non altro perché inserite in un contesto fattuale "dominato" da molestie o minacce commesse in modalità analogica.

Potrebbe porsi una questione interpretativa nel caso in cui solo una molestia o una minaccia risulti commessa attraverso strumenti informatici o telematici. Si tratta di chiarire se, ai fini dell'applicazione della circostanza aggravante, le condotte digitali debbano, da sole, integrare il requisito dell'abitualità o se, per contro, l'aggravante possa contestarsi anche a fronte di una sequenza di atti di cui uno solo si avvalga delle nuove tecnologie. Qualora si ritenesse che, nell'espressione «se il fatto è commesso attraverso strumenti informatici o telematici», il concetto di "fatto" si riferisca agli elementi costitutivi che integrano la fattispecie del primo comma, l'aggravante potrebbe trovare applicazione solo in caso di condotte digitali reiterate, sia pur congiunte a condotte "tradizionali". Questa, in effetti, sembrerebbe la lettura più conforme alla lettera della legge, sebbene la stessa non riuscirebbe a superare del tutto la criticità cui si è fatto cenno.

[8] G. Ziccardi, *Cyberstalking e molestie*, cit., p. 167.

[9] Corte Suprema di Cassazione, Ufficio del Massimario e del Ruolo, Relazione n. III/01/2013, 22 agosto 2013, in riferimento all'aggravante introdotta nel secondo comma dell'art. 612-*bis* c.p.: «se dunque la nuova previsione conferma la rilevanza di campagne di *stalking* "a distanza", qualche perplessità genera la scelta di riconnettere a tale circostanza natura aggravante, non risultando evidente perché tale modalità consumativa del reato debba effettivamente sempre ritenersi più grave rispetto ad altre invero potenzialmente anche più invasive come i pedinamenti ossessivi, le sistematiche minacce portate di persona ecc.». Sul punto v. anche F. Macrì, *Il Cyberstalking*, in «Cybercrime», cit., p. 585.

L'impressione è che la circostanza aggravante del cyberstalking sia pensata in riferimento ad atti persecutori commessi in modalità esclusivamente digitale. Qualora, invece, vengano in considerazione condotte eterogenee, in assenza di qualsiasi indicazione che, sul piano quantitativo e qualitativo, valga a selezionare l'incidenza delle condotte online rispetto a quelle offline, il mero uso di strumenti informatici o telematici non sembrerebbe espressione, di per sé, di un disvalore tale da sostenere la ragionevolezza della previsione di una circostanza aggravante.

b) il coordinamento con il reato di molestie, con particolare riguardo all'utilizzo di social network

Uno degli strumenti messi a disposizione dalle nuove tecnologie è certamente quello costituito dai *social network*, ciascuno dei quali, tuttavia, si caratterizza per strutture e meccanismi di funzionamento che solo in via di prima approssimazione rendono convincente il riferimento a una generale etichetta definitoria.

La Corte di cassazione, con la sentenza n. 19363 del 2021, si è confrontata con un caso di atti persecutori "a mezzo *Facebook*", nel quale, più esattamente, venivano in considerazione delle minacce reiterate rivolte alle persone offese attraverso la bacheca del *social network*.

I giudici di legittimità, confermando che l'utilizzo di *social network* ben potrebbe integrare la condotta di atti persecutori, precisano che «non è tanto il mezzo attraverso il quale si diffonde la comunicazione che consente di ritenere il delitto di cui all'art. 612-*bis* c.p. ma è, piuttosto, il contenuto della stessa che deve costituire un comportamento concretamente vessatorio a danno della persona offesa»[10]. Quando a venire in considerazione è il *social-media Facebook*, poi, deve tenersi conto del fatto le comunicazioni possono essere inviate al "profilo" del destinatario oppure pubblicate sul proprio "profilo". Se il messaggio sia inviato al "profilo" della persona offesa, questa forma comunicazione risulta equivalente a quelle veicolate con altro mezzo di diffusione (sms, *Whatsapp*, *Telegram*, *Messenger*, per esempio). Qualora, invece, il messaggio, pur rivolto a una determinata persona, risulti pubblicato sul profilo imputato, se ne dovrà verificare la conoscenza, anche solo indiretta, da parte della persona offesa[11].

Queste considerazioni sembrano sufficientemente chiare e univoche quando a venire in considerazione sono condotte di minaccia, ma non altrettanto, forse, potrebbe ritenersi a fronte di molestie reiterate, specie se a venire in considerazione sia l'utilizzo di messaggistica interna al *social network*.

[10] Cass., Sez. V, 31 marzo 2021, n. 19363, punto 5 *del Considerato in diritto*.

[11] Cass., Sez. V, 31 marzo 2021, n. 19363, punti 7 e 8 del *Considerato in diritto*, in cui si richiama l'orientamento giurisprudenziale per cui «ai fini della configurabilità del delitto di minaccia, non è necessario che le espressioni intimidatorie siano pronunciate in presenza della persona offesa, potendo quest'ultima venirne a conoscenza anche attraverso altri, in un contesto dal quale possa desumersi la volontà dell'agente di produrre l'effetto intimidatorio».

A questo proposito pare opportuno precisare che, dopo alcune incertezze iniziali, la giurisprudenza inquadra la fattispecie di atti persecutori nello schema del reato abituale improprio[12], richiedendo, quindi, che le singole condotte costituiscano di per sé un fatto penalmente rilevante.

Se a venire in considerazione sono delle molestie, il riferimento obbligato è alla contravvenzione prevista dall'art. 660 c.p., che, con una norma anacronistica e inadeguata alle esigenze di tutela ricavabili (anche) dalle fonti internazionali[13], punisce chiunque, in un luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo. Il riferimento al "mezzo del telefono", sebbene interpretato estensivamente dalla giurisprudenza, potrebbe comportare irragionevoli limitazioni della tutela, proprio quando a venire in considerazione siano fatti commessi avvalendosi delle nuove tecnologie. Con particolare riguardo alla casistica offerta dalla messaggistica telematica a mezzo *social network* (*Facebook* o *Instagram*, per esempio), parte della giurisprudenza ha ritenuto configurabile il reato di molestie[14], ma non sono mancate pronunce che ne hanno escluso l'operatività, valorizzando la circostanza per cui il destinatario può disattivare le notifiche di ricezione[15].

Una riscrittura dell'art. 660 c.p., oltre ad essere necessaria per aggiornare una tutela in materia di molestie irragionevolmente imbrigliata nelle categorie e nel linguaggio del legislatore del 1930, sarebbe certamente auspicabile anche per chiarire alcuni dubbi interpretativi sul versante del cyberstalking, a conferma del fatto che l'esclusivo e generico riferimento all'uso di strumenti informatici o telematici, da solo, rischia di rivelarsi insufficiente.

c) stalking *e* cyberstalking*: un rapporto di genere a specie?*

Un ulteriore aspetto problematico attiene ai rapporti tra *stalking* offline e online, che, come più volte precisato, il legislatore italiano "risolve" affidandosi alla descrizione del secondo attraverso un elemento aggiuntivo, di natura circostanziale, che arricchisce la fattispecie base, per il resto inalterata.

Non è così scontato, per la verità, che il cyberstalking costituisca una mera variante dello *stalking* tradizionale. Questa premessa, da un punto di vista delle tecniche di incriminazione, potrebbe tradursi nel fatto che la componente digitale della condotta si

[12] Cass., Sez. V, 8 luglio 2019, n. 48055; Cass., Sez. V, 5 marzo 2018, n. 31996.

[13] Con particolare riguardo alle molestie sessuali, v. l'art. 40 della Convenzione del Consiglio d'Europa sulla prevenzione e la lotta dei fenomeni di violenza contro le donne e violenza domestica, firmata a Istanbul l'11 maggio 2011 (Convenzione di Istanbul), il quale stabilisce che «le Parti adottano le misure legislative o di altro tipo necessarie per garantire che qualsiasi forma di comportamento indesiderato, verbale, non verbale o fisico, di natura sessuale, con lo scopo o l'effetto di violare la dignità di una persona, segnatamente quando tale comportamento crea un clima intimidatorio, ostile, degradante, umiliante o offensivo, sia sottoposto a sanzioni penali o ad altre sanzioni legali».

[14] Cass. pen., Sez. I, 25 ottobre 2024, n. 44477; Cass., sez. I, 28 aprile 2023, n. 34171; Cass., sez. I, 6 aprile 2023, n. 43642.

[15] Cass. pen., Sez. I, 3 ottobre 2023, n. 40033.

sostituisca, anziché aggiungersi, agli altri elementi costitutivi della fattispecie, rappresentando una delle alternative modalità di realizzazione del delitto di atti persecutori.

In questa direzione sembrerebbero muoversi altri codici penali europei, a partire da quello tedesco e da quello spagnolo, nei quali il cyberstalking costituisce una modalità di realizzazione dello *stalking*, alternativa alle altre, ma espressiva di un equivalente disvalore sul piano sanzionatorio.

Il § 238 StGB (*Nachstellung*) punisce «chi perseguita un'altra persona in modo illecito, in una maniera idonea a compromettere in modo non trascurabile la sua condotta di vita, agendo ripetutamente come segue: 1. si avvicina fisicamente a questa persona; 2. cerca di mettersi in contatto con questa persona mediante strumenti di telecomunicazione, altri mezzi di comunicazione, oppure tramite terzi; 3. utilizza abusivamente i dati personali di questa persona per: a) effettuare ordini di beni o servizi a suo nome, oppure b) indurre terzi a prendere contatto con lei; 4. minaccia questa persona, un suo familiare o un'altra persona a lei vicina, con la lesione della vita, dell'integrità fisica, della salute o della libertà; 5. commette, ai danni di questa persona, di un suo familiare o di un'altra persona a lei vicina, un reato previsto dagli articoli § 202a, § 202b o § 202c (violazioni di segreti informatici); 6. diffonde o rende accessibile al pubblico un'immagine di questa persona, di un suo familiare o di una persona a lei vicina; 7. diffonde o rende accessibile al pubblico un contenuto (§ 11, comma 3) idoneo a ridicolizzare o screditare pubblicamente questa persona, simulando che ne sia lei stessa l'autrice; 8. pone in essere una condotta assimilabile a quelle previste ai punti da 1 a 7». Nel secondo comma, poi, si prevedono degli aggravamenti di pena in casi ritenuti particolarmente gravi, anche riferibili allo *stalking* digitale: un caso ritenuto di particolare gravità, per esempio, è quello dell'utilizzo di un programma informatico destinato all'intercettazione digitale di altre persone.

Anche nell'art. 172-*ter* del codice penale spagnolo lo *stalking* digitale è una modalità di realizzazione del reato, alternativa alle altre e alle altre equivalente sul versante sanzionatorio: si punisce, infatti, «chi perseguita un'altra persona, in modo insistente e reiterato, e senza essere legittimamente autorizzato, compiendo una delle seguenti condotte, e alterando in tal modo il normale svolgimento della sua vita quotidiana: 1.ª La sorveglia, la segue o cerca di avvicinarsi fisicamente a lei. 2.ª Stabilisce o tenta di stabilire contatto con lei attraverso qualsiasi mezzo di comunicazione, oppure tramite terze persone. 3.ª Utilizzando in modo indebito i suoi dati personali, acquista beni o prodotti, stipula contratti di servizi, oppure induce terze persone a mettersi in contatto con lei. 4.ª Lede la sua libertà o il suo patrimonio, oppure la libertà o il patrimonio di una persona a lei vicina».

A ciò si aggiunga che il concetto di cyberstalking "proposto" dalle fonti non nazionali risulta spesso particolarmente ampio o, comunque, non coincidente a quello ricavabile dall'art. 612-*bis* c.p. Il riferimento è, in particolare, all'art. 6 della Direttiva UE 1385/2024 sulla lotta alla violenza contro le donne e alla violenza domestica, il quale, con un obbligo di tutela penale rivolto agli Stati, prevede che gli stessi criminalizzino, come *stalking online*, le condotte dolose consistenti nel sottoporre ripetutamente o continuamente un'altra persona a sorveglianza tramite tecnologie dell'informazione

della comunicazione (TIC), senza consenso o autorizzazione, per seguirne o monitorarne i movimenti e le attività, qualora tali condotte possano arrecare un danno grave alla persona in questione. L'aspetto di maggiore criticità, sembrerebbe, consiste nella pretesa incriminazione anche di condotte realizzate all'insaputa della vittima. In assenza di una consapevolezza della persona offesa, in effetti, non potrebbero applicarsi le fattispecie di reato che, come gli atti persecutori o la violenza privata, sono costruite mediante il riferimento alla violenza, alla minaccia o alla costrizione. Anche il delitto di interferenza illecita nella vita privata (art. 615-*bis* c.p.) rischia di risultare insufficiente, posto che deve trattarsi di un'indebita acquisizione di immagini o video attinenti alla vita privata che si svolge nei luoghi di domicilio della vittima. Al fine di adempiere correttamente agli obblighi imposti dalla Direttiva, si renderebbe necessario un intervento del legislatore, che attribuisca specifico rilievo alla sorveglianza continua di una persona e alle finalità che sorreggono questa particolare condotta persecutoria. Potrebbe però porsi un problema di compatibilità con i principi generali in materia penale (a partire da quelli di necessaria offensività e determinatezza), rispetto ai quali potrebbe risultare insufficiente il solo riferimento, contenuto nella Direttiva, al pericolo di un danno grave alla persona[16].

4. *Cyberbullismo: la definizione extrapenale e le proposte di una fattispecie* ad hoc

La definizione di cyberbullismo, nell'ordinamento giuridico italiano, è attualmente affidata a norme extrapenali, mentre sul versante penalistico, in assenza di fattispecie *ad hoc*, troveranno applicazione le norme di volta in volta riferibili alla condotta posta in essere, comprese quelle contenute nell'art. 612-*bis* c.p.

Il riferimento è alla legge 29 maggio 2017, n. 71, che in origine conteneva la sola definizione di cyberbullismo, ma che, dopo le modifiche apportate dalla legge 17 maggio 2024, n. 70, si riferisce anche alle ipotesi di bullismo.

Seguendo una tendenza esattamente speculare a quella più ricorrente, quindi, l'ordinamento muove da una prioritaria considerazione del fenomeno "digitale", per poi estendere la disciplina anche alla sua versione "analogica".

Secondo le definizioni contenute nell'art. 1, l. n. 71 del 20178, «per "bullismo" si intendono l'aggressione o la molestia reiterate, da parte di una singola persona o di un gruppo di persone, in danno di un minore o di un gruppo di minori, idonee a provocare sentimenti di ansia, di timore, di isolamento o di emarginazione, attraverso atti o comportamenti vessatori, pressioni o violenze fisiche o psicologiche, istigazione al suicidio o all'autolesionismo, minacce o ricatti, furti o danneggiamenti, offese o derisioni».

[16] Per più ampie considerazioni sulla Direttiva UE 1385/2024 sia consentito il rinvio ad A. Massaro, *La Direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica: il possibile impatto sull'ordinamento italiano*, in «Sist. pen.», 26 marzo 2025.

Per "cyberbullismo", invece, «si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».

Di particolare interesse, poi, è l'art. 7 della l. n. 71 del 2017, il quale prevede che fino a quando non è proposta querela o non è presentata denuncia per taluno dei reati di cui agli articoli 594, 595, 612 e 612-*ter* del codice penale e all'articolo 167 d.lgs. n. 196 del 2003, anche mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento da parte del Questore, già prevista, in materia di atti persecutori, dall'art. 8, commi 1 e 2, del d.l. 23 febbraio 2009, n. 11.

Senza entrare nel dettaglio delle singole definizioni[17], può rilevarsi come in quella di cyberbullismo, accanto al *nomen iuris* di specifiche fattispecie incriminatrici (molestia, diffamazione…), facciano la loro comparsa concetti tratti dal linguaggio comune e, proprio per questo, di più difficile interpretazione (ricatto, denigrazione…). Il disvalore, poi, si concentra (anche) sulla finalità perseguita dall'agente, che deve consistere nello scopo intenzionale e predominante di isolare un minore o un gruppo di minori.

Sono state avanzate proposte di legge volte a introdurre una specifica fattispecie incriminatrice per il bullismo e il cyberbullismo, che, ovviamente, passano per una autonoma "ridefinizione" degli stessi, senza la possibilità di rinviare alle ampie e poco precise definizioni offerte dalla legge n. 71 del 2017. La proposta di legge AC 910 del 2023, in particolare, prevede l'introduzione di un art. 612-*bis*.1 c.p., che, rubricato «bullismo e cyberbullismo», così dispone: «salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a sette anni chiunque, con condotte reiterate, mediante violenza, atti ingiuriosi, denigratori o diffamatori o ogni altro atto idoneo, intimidisce, minaccia o molesta taluno, in modo da porlo in stato di grave soggezione psicologica ovvero da isolarlo dal proprio contesto sociale». Si prevede poi una pena più elevata «se i fatti di cui al primo comma sono commessi mediante la rete internet o la rete di telefonia mobile». Sebbene la proposta in questione non sia poi confluita nel testo unificato adottato come testo base, il suo esame conferma la difficoltà di definire, tramite una fattispecie autonoma, uno spettro di condotte indubbiamente ampio ed eterogeneo, con quel riferimento allo «stato di grave soggezione psicologica» che richiama alla mente il «totale stato di soggezione» che compariva nella fattispecie di plagio (603 c.p.), dichiarata incostituzionale dalla Corte costituzionale con sentenza n. 96 del 1981.

[17] V. sul punto M.C. Parmiggiani, *Il cyberbullismo*, in *Cybercrime*, cit., pp. 588 ss.; V. Sellaroli, *Cyberbullismo*, in «Ius», 2 settembre 2024; A. Bramante, V. Lamarra, *Bullismo e cyberbullismo. Dinamiche e interventi di prevenzione*, in «Ius», 15 giugno 2017.

5. *Determinatezza e offensività: antichi ingredienti per nuove ricette*

Da un rapido esame della rilevanza penale attribuita alle condotte di cyberstalking nell'ordinamento italiano e alle riflessioni attualmente in corso sulla possibile introduzione di un'apposita fattispecie per il cyberbullismo, emergono spunti per una riflessione più ampia sui rapporti tra diritto penale e nuove tecnologie.

È innegabile che, in concreto, le nuove tecnologie abbiano fatto irruzione (anche) nella realtà criminale, ridefinendo la fenomenologia di molte fattispecie incriminatrici. In astratto, tuttavia, la soluzione ottimale non sempre coincide con una esplicita rilevanza attribuita all'uso di strumenti informatici o telematici, magari collegando all'elemento in questione, di per sé solo, una risposta sanzionatoria più severa. Proprio la capillare diffusione delle tecnologie digitali e la distanza sempre meno definita tra la realtà tradizionale e la realtà cibernetica, in effetti, suggerisce che, almeno in certi casi, l'opzione più convincente resti quella di affidarsi alle fattispecie tradizionali. A meno che i singoli elementi costitutivi non risultino del tutto incompatibili con l'utilizzo delle nuove tecnologie o, ancora, le condotte che si intende criminalizzare siano compatibili solo con una realizzazione "tecnologica", il proliferare di fattispecie sovraccariche di elementi costitutivi incerti e ondivaghi è, come al solito, da guardare con sospetto.

Le parole d'ordine, sembrerà banale a dirsi, restano quelle di un diritto penale ispirato ai principi di necessaria determinatezza e di offensività in astratto, che, in fondo, sono due facce della stessa medaglia. Il diritto penale fondato sull'offesa tipica e su un bene giuridico chiaramente delineato, sebbene ritenuto spesso l'inutile ingombro di un sistema anacronistico e "analogico", offre già, se adeguatamente maneggiato, gli strumenti per arginare l'incontrollata proliferazione di fattispecie "tecnologicamente orientate", riservando l'esplicita valorizzazione delle nuove tecnologie ai soli casi in cui, dalla stessa, derivi un effettivo rafforzamento di tutela.

LE MOLESTIE SESSUALI NELL'UNIVERSO DIGITALE. RIFLESSIONI SULLA DIMENSIONE "NON FISICA" DELLA LIBERTÀ SESSUALE

Matilde Botto

1. *Le molestie sessuali "virtuali" come ipotesi di "*technology-facilitated sexual violence*" (TFSV)*

Allo scopo di offrire una panoramica concernente le molestie sessuali nell'universo digitale, si avverte la necessità di muovere da una premessa generale. Molteplici ambiti dell'agire umano sono oramai protagonisti di un "processo di digitalizzazione" e questo ha coinvolto anche la sfera più intima degli individui: la loro sessualità. Da ciò, inevitabilmente, sono derivati anche riflessi sul fronte della tutela penale della libertà sessuale, che arrivano a coinvolgere il piano dei suoi confini contenutistici[1]. Dinnanzi all'emergere di nuove problematiche, inoltre, si è assistito al mutare della portata applicativa di categorie già note nella "realtà offline". È questo il caso delle molestie sessuali, che, come confermato dalle indagini empiriche in materia, hanno oramai assunto anche una rilevante dimensione "virtuale"[2].

Più nel dettaglio, la nozione di "*digital sexual violence and harassment*" ricomprende al suo interno una molteplicità di ipotesi, che vanno da minacce a sfondo sessuale, molestie, aggressioni sino a forme di abuso basate sulle immagini e, non di rado, è oggetto di approfondimento nell'ambito di ricerche e studi in materia di violenza di genere[3].

[1] In argomento, anche per gli opportuni riferimenti bibliografici, si veda B. PANATTONI, *Violazioni "incorporee" della sfera sessuale. Possibili evoluzioni ed insidie nell'ambito dei reati sessualmente connotati*, in «Archivio penale (web)», 3 (2022), pp. 1-33.

[2] Invero, se i primi studi sulle molestie online si concentravano in via sostanzialmente prioritaria su quelle aventi come protagonisti gli adolescenti – collocandosi tendenzialmente nell'ambito di analisi relative al cosiddetto "cyberbullismo" –, progressivamente, si è avuto modo di constatare che il fenomeno ha un impatto significativo anche sulla popolazione adulta. Sul punto, M. FERESIN, *Molestie 2.0*, in *Le molestie sessuali. Riconoscerle, combatterle, prevenirle*, a cura di P. Romito e M. Feresin, Carocci, Roma, 2019, pp. 61-68.

[3] A ben vedere, infatti, a mutare è non solo il livello di incidenza (maggiore sulla popolazione femminile) ma anche il "tipo di comportamento offensivo": le donne, infatti, risultano avere una probabilità più elevata di

Stante a monte un simile "termine ombrello", la molteplicità dei comportamenti che vi rientrano possono altresì considerarsi come forme di "*technology-facilitated sexual violence*" (TFSV) – lett. violenza sessuale "facilitata" dalla tecnologia – posto che tale espressione è riferibile ad una varietà di azioni, "violente"[4] o, appunto, moleste, accomunate dall'essere realizzate con l'ausilio (o mediante l'impiego) delle tecnologie di informazione e comunicazione (TIC)[5]. Invero, pur evidenziando l'assenza di uniformità definitoria[6], per quanto attiene al presente discorso, si sottolinea che, allorquando

essere vittime degli episodi più gravi (quali, ad esempio, lo *stalking online*, e, appunto, le molestie a sfondo sessuale). In argomento, con riferimento alle indagini empiriche condotte a livello europeo, si richiama innanzitutto lo studio a cura della EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Violence against women: an EU-wide survey – Main results*, Publications Office of the European Union, Lussemburgo, 2014, p. 112, dal quale è emerso che, già al tempo, il 73% delle donne dichiarava di aver subito una qualche forma di *online abuse*. Negli anni successivi, tale *trend* non solo ha trovato conferma ma si è caratterizzato anche per un andamento crescente. Oltre a ricordare l'*escalation* che si è registrata nel corso della pandemia da COVID-19 (EUROPEAN INSTITUTE FOR GENDER EQUALITY (EIGE), *Combating Cyber Violence against Women and Girls*, Publications Office of the European Union, Lussemburgo, 2022, pp. 7-9 (d'ora in avanti: EIGE (2022)), anche le ricerche empiriche più recenti continuano ad evidenziarne un impatto sempre più significativo (sul punto, EUROPEAN WOMEN'S LOBBY (EWL), *Report on Cyber Violence Against Women*, 2024, liberamente consultabile alla pagina https://womenlobby.org/new-publication-report-on-cyber-violence-against-women/, ed EUROPEAN INSTITUTE FOR GENDER EQUALITY (EIGE), *Combating Cyber Violence against Women and Girls: Developing an EU Measurement Framework*, Publications Office of the European Union, Lussemburgo, 2025).

[4] Deve precisarsi che, nel contesto in parola, la nozione di "violenza" ha un'accezione estesa. Nella letteratura anglofona, si segnala che alternativamente al termine "*violence*" può comparire quello di "*abuse*": entrambi sono impiegati al fine di descrivere le diverse tipologie di comportamenti a sfondo abusivo e di matrice sessuale che hanno luogo nell'ambiente digitale (cfr., sul punto, le considerazioni di O. JURASZ, K. BARKER, *Sexual Violence in the Digital Age: A Criminal Law Conundrum?*, in «German Law Journal», 22/5 (2021), pp. 784-785).

[5] Nel senso anzidetto, A.R. CHAMPION, F. OSWALD, D. KHERA, C.L. PEDERSEN, *Examining the Gendered Impacts of Technology-Facilitated Sexual Violence: A Mixed Methods Approach*, in «Archives of Sexual Behavior», 51/3 (2022), p. 1607. Cfr. N. HENRY, A. POWELL, *Technology-facilitated sexual violence: A literature review of empirical research*, in «Trauma, Violence, and Abuse», 19/2 (2018), pp. 195 s., dove gli Autori riferiscono il concetto *de quo* «*to a range of criminal, civil, or otherwise harmful sexually aggressive and harassing behaviours that are perpetrated with the aid or use of communication technologies*» (lett.: «ad un insieme di comportamenti sessualmente aggressivi o molesti, penalmente o civilmente rilevanti, o comunque offensivi, perpetrati con l'aiuto o mediante l'uso delle tecnologie di comunicazione»). Per un approfondimento sulle due espressioni, v. N. HENRY, A. POWELL, *Beyond the 'sext': Technology-facilitated Sexual Violence and Harassment against Adult Women*, in «Australian and New Zealand Journal of Criminology», 48(1), (2015), pp. 104-118 (spec. p. 108). Nella dottrina italiana, di recente, cfr. G.M. CALETTI, Habeas corpus *digitale. Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Giappichelli, Torino, 2024, p. 16.

[6] In argomento si segnala la "*review* concettuale" proposta da M. MITCHELL ET AL., *Technology-facilitated Violence: A Conceptual Review*, in «Criminology & Criminal Justice», 25/2 (2025), pp. 649-669, la quale ha ad oggetto una vera e propria rassegna terminologica delle diverse definizioni del fenomeno presenti negli studi in lingua anglofona. Nell'analisi, si rileva, ad esempio, che il *focus* della nozione di "*technology-facilitated violence*" (TFV) può variare anche a seconda dell'accento che viene posto sul ruolo delle tecnologie di informazione e comunicazione. Possono, infatti, distinguersi almeno tre diversi approcci, nei quali si enfatizza rispettivamente: (a) l'uso – esclusivamente come strumento – delle TIC (c.d. «*use-based conceptions*»); (b) non solo la natura "di mezzo", ma anche il fatto che le TIC contribuiscono ad agevolare il verificarsi dei comportamenti offensivi e ad amplificarne gli effetti (c.d. «*extension conceptions*», nelle quali, dunque, è valorizzata la funzione di "facilitazione"); e, infine, (c) le definizioni in cui viene sottolineato l'impatto "promozionale" delle nuove tecnologie sulla realizza-

si procede a fornirne esemplificazioni, vengono annoverate tanto condotte verbali e scritte dal diverso potenziale offensivo (le quali possono sfociare anche in vere e proprie minacce o forme di istigazione all'odio), quanto l'invio o la condivisione non consensuale di immagini, messaggi o video dai contenuti sessuali ovvero la divulgazione pubblica di informazioni personali della vittima, al fine di istigare terzi ad arrecarle un danno fisico o un grave danno psicologico (c.d. «*doxing*» o «*doxxing*»), fino ad altre tipologie di "intrusione" idonee a ledere *privacy* e riservatezza sessuale dell'individuo[7].

Come si accennava, la materia, sia nella reportistica che in letteratura[8], viene trattata di frequente nell'ambito di studi e approfondimenti sulla *Cyber-Violence Against Women and Girls* (CVAWG) ovvero sulla *Online Gender-Based Violence* (OGBV).

La prospettiva appena descritta, d'altra parte, è anche quella attraverso la quale i fenomeni appena richiamati sono permeati all'interno della Direttiva UE 1385/2024 (d'ora in avanti: la Direttiva)[9], che costituisce il primo atto dell'Unione dedicato in via specifica alla prevenzione e al contrasto della violenza contro le donne e della violenza domestica[10]. Invero, è lo stesso legislatore europeo che, sin dall'avvio del documento,

zione delle condotte offensive (c.d «*mediation-based approach*»). Per completezza, ulteriori difformità riguardano altresì la circostanza per cui, allo scopo di descrivere lo stesso fenomeno, non sempre si ricorre all'espressione in parola, ma ad una varietà di nozioni (come, ad esempio, quella a portata più generale di "*digital sexual violence*"; cfr. in senso critico rispetto ad una simile frammentazione, K. BARKER, O. JURASZ, *Online Violence Against Women as an Obstacle to Gender Equality: a Critical View from Europe*, in «European Equality Law Review», 1 (2020), pp. 47-60). In generale, dall'assenza di univocità derivano una serie di problematiche, prima tra tutte la difficoltà di comparare gli studi e le indagini empiriche, seguita da quella di classificare i comportamenti che vi rientrano e rilevarne l'impatto che hanno sulle vittime (v. N. HENRY, A. FLYNN, A. POWELL, *Technology-facilitated Domestic and Sexual Violence: A Review*, in «Violence against Women», 26/15-16 (2020), pp. 1828-1854).

[7] Cfr., per tutti, J. BAILEY, S. DUNN, *Recurring Themes in Tech-Facilitated Sexual Violence Over Time. The More Things Change, the More They Stay the Same*, in *Criminalizing Intimate Image Abuse*, a cura di G.M. Caletti e K. Summerer, Oxford University Press, Oxford, 2024, pp. 40-59.

[8] Per un richiamo alle indagini empiriche rilevanti si veda la precedente nota (3). Quanto alla letteratura, senza alcuna presunzione di completezza, quanto evidenziato nel testo emerge nei contributi di: A. POWELL, N. HENRY, *Sexual Violence: A Feminist Criminological Analysis*, in *Sexual Violence in a Digital Age*, a cura di ID., Palgrave Macmillan UK, Londra, 2017, pp. 23-47 e O. JURASZ, K. BARKER, *Sexual Violence in the Digital Age*, cit., pp. 784-799.

[9] Occorre precisare che, nella Dir. UE 1385/2024, tra gli obblighi di incriminazione, non è presente una disposizione rubricata "molestie *sessuali* (*online*)", ancorché queste vengono espressamente menzionate tra le forme "virtuali" di violenza contro le donne al punto 9 del *Considerando.* Difatti, l'articolo dedicato in via specifica alle molestie è quello rivolto, più in generale, alle «*Molestie online*» (art. 7). Tuttavia, come si approfondirà analizzando tale norma, alcune ipotesi contenute al suo interno possono essere lette come rientranti nella categoria delle molestie *sessuali* (è questo, ad esempio, il caso del "*cyberflashing*", lett. c)) ovvero ricondotte ad essa qualora il comportamento rilevante si caratterizzi per avere una connotazione sessuale (*infra*, § 4). A completamento, seppur non sarà oggetto dell'analisi della presente trattazione, si evidenzia che tra gli obblighi di incriminazione afferenti alle forme di "violenza online" compaiono altresì quelli rivolti a: la condivisione non consensuale di materiale intimo o manipolato (art. 5, comprensivo quindi sia della cosiddetta pornografia non consensuale che dei c.d. "*deepfake*" pornografici), lo *stalking online* (art. 6) e, infine, l'istigazione alla violenza o all'odio online basata sul genere (art. 8).

[10] In argomento, A. MASSARO, *La Direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica: il possibile impatto sull'ordinamento italiano*, in «Sistema penale», 3 (2025), pp. 107-143 e S. BRASCHI, *La nuova direttiva sulla lotta alla violenza contro le donne e alla violenza domestica e le sue ricadute*

evidenzia la portata dell'impatto della dimensione online della violenza di genere[11], muovendosi, dunque, nel solco delle indagini empiriche che ne certificano un tasso di diffusione in crescita[12] e finendo col riservarle una precipua attenzione, nel contesto degli obblighi di incriminazione che gli Stati parte sono chiamati ad ottemperare entro il 14 giugno 2027 (art. 49). Ed è da una simile angolatura che, quindi, possono considerarsi le "*cyber-sexual harassment*" (*id est* le molestie sessuali "virtuali"), da intendersi, pertanto, altresì come peculiari forme di manifestazione di una problematica più vasta. D'altro canto, anche le nuove forme di "intrusione" nella sfera sessuale della persona, realizzate mediante le TIC, sono descrivibili come parte integrante di un *continuum*, non essendo svincolate dalle dinamiche e dai fattori culturali che si trovano alla base della violenza domestica e di genere nella "realtà fisica", ma ponendosi, piuttosto, in continuità rispetto ad essi[13].

2. *Le sfide connesse alla delimitazione dei contenuti di una categoria eterogenea*

L'affermarsi a livello fenomenologico di una dimensione online delle molestie sessuali risulta essere comprovato, oltre che dal quadro brevemente delineato in sede introduttiva, dalla tendenza a inserire tra i comportamenti ascrivibili alla categoria in parola anche quelli che avvengono tramite messaggi, *chat* o *e-mail* ovvero aventi ad oggetto la condivisione o pubblicazione di contenuti sessualmente espliciti[14]. Più nel dettaglio, a condotte verbali o scritte, si affiancano casi in cui la condotta abusiva

nell'ordinamento nazionale, in «Diritto penale e processo», 10 (2024), pp. 1367-1379, nonché C. Rigotti, C. McGlynn, F. Benning, *Image-Based Sexual Abuse and EU Law: A Critical Analysis*, in «German Law Journal», 25(9), (2024), pp. 1472-1493.

[11] In tal senso, i punti 17-27 del *Considerando* della Dir. UE 1385/2024.

[12] Nello studio condotto da J. Hicks, *Global Evidence on the Prevalence and Impact of Online Gender-based Violence (OGBV)*, K4D Helpdesk Report, No. 1049, Institute of Development Studies, Brighton, 2021, p. 2, viene registrato un significativo incremento (dal 16 al 58%) della percentuale di donne vittime di "*technology facilitated violence against women*" (il dato è riportato anche nel recente rapporto dell'8 ottobre 2024 del Segretario Generale delle Nazioni Unite, United Nations-General Assembly, *Intensification of efforts to eliminate all forms of violence against women and girls: Technology-facilitated violence against women and girls: Report of the Secretary-General*, A/79/500, p. 5).

[13] L'espressione «*continuum*» si deve alla costruzione teorica, elaborata sul finire del secolo scorso, da L. Kelly, *Surviving sexual violence*, Polity Press, Cambridge, 1988. Tale impostazione, a ben vedere, ricorre ampiamente nell'ambito degli studi dedicati alla CVAWG ovvero alla OGBV. Si veda, ad esempio, un passaggio del già menzionato report EIGE (2022), cit., p. 7, dove viene ribadito che: «*However, as digital (online) and face-to-face (offline) spaces become more and more integrated, CVAWG often amplifies (or is a precursor for) violence and victimisation in the physical world*». Si ricorda altresì che nella *General Recommendation No 1 on the Digital Dimension of Violence against Women* adottata il 20 ottobre 2021 dal Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), la CVAWG è stata espressamente qualificata come una forma di violenza rilevante ai sensi della cosiddetta Convenzione di Istanbul.

[14] Cfr. l'elenco delle condotte ascrivibili alla nozione di «*Sexual Harassment*» fornito dal Rape, Abuse & Incest National Network (RAINN) (https://rainn.org/articles/sexual-harassment).

dell'autore si realizza "attraverso" le immagini[15]. Un esempio può essere il cosiddetto "*cyberflashing*"[16]: espressione con cui si indica l'invio indesiderato di immagini sessualmente esplicite generalmente raffiguranti l'organo sessuale maschile, il quale in letteratura, talvolta, è qualificato anche come una forma di «*image-based sexual abuse*»[17]. Proseguendo, inoltre, vengono attratte nell'orbita delle "*cyber-sexual harassment*" anche quelle che, di frequente, sono considerate nuove frontiere del voyeurismo. Si tratta, nello specifico, dei fenomeni che, in lingua inglese, sono indicati con il termine "*creepshots*" – con cui si fa riferimento all'azione di immortalare (mediante fotografie o video) le parti intime delle vittime, operando di nascosto e in assenza del consenso della persona ritratta – ovverosia con le espressioni "*upskirting*" o "*downblousing*"; laddove la prima è evocativa di una condotta, speculare a quella poc'anzi descritta, finalizzata a "carpire" ciò che "si intravede sotto la gonna" della persona offesa e la seconda si riferisce all'eventualità in cui "si operi attraverso la scollatura" del soggetto immortalato[18].

Nel trasporre quanto tratteggiato in un discorso che dalla *species* (molestie sessuali online) guardi al *genus* (molestie sessuali), occorre rilevare che, dal canto suo, ad essere caratterizzata da un contenuto eterogeneo è la stessa categoria di appartenenza. Invero, per definizione e al di là della presenza di un riferimento a uno specifico contesto, il termine "molestie sessuali" si rivolge a comportamenti profondamente diversificati tra di loro, i quali possono estrinsecarsi in gesti ed espressioni verbali, oltre che in azioni in cui è presente una componente fisica[19]. Come ben si coglie dal testo dell'articolo 40 («*Molestie sessuali*») della Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica (c.d. Convenzione di Istanbul), infatti, queste ricomprendono «qualsiasi forma di comportamento

[15] *Ibidem*, atteso che, nel novero degli esempi delle forme di manifestazione delle molestie sessuali, si richiama espressamente anche la seguente ipotesi: «*Unwanted sexually explicit photos, emails, or text messages*».

[16] In argomento, M. Botto, *Le molestie sessuali "dentro" e "fuori" dal confine dell'art. 609* bis *c.p. Un'indagine sulla distinzione tra molestia e aggressione sessuale a partire dalla "doppia narrazione" degli «atti repentini»*, in «Archivio penale (web)», 2 (2023), pp. 42-48 e G.M. Caletti, Habeas corpus *digitale*, cit., pp. 203-212. Nella dottrina internazionale, per tutti, diffusamente, C. McGlynn, K. Johnson, *Cyberflashing: Recognising Harms, Reforming Laws*, Bristol University Press, Bristol, 2021.

[17] In tal senso, C. McGlynn, K. Johnson, *Criminalising Cyberflashing: Options for Law Reform*, in «The Journal of Criminal Law» (2021), p. 172. L'espressione «*image-based sexual abuse*» si rivolge ad un articolato ventaglio di ipotesi, che ricomprende anche casi che fuoriescono dall'ambito circoscritto della riflessione in oggetto. Nello specifico, questa include la creazione e/o la diffusione di immagini di nudo o sessualmente esplicite senza consenso, comprese le minacce di porre in essere tale comportamento. Pertanto, al suo interno ricadono sia il cosiddetto "*revenge porn*" (ovverosia la pornografia non consensuale), quanto il "voyeurismo digitale" (che si analizzeranno a breve), sia i "*deepfake*" pornografici e le ipotesi di estorsione "sessuale" (c.d. *sextrortion*), nonché la videoripresa di episodi di violenza sessuale (cfr. C McGlynn et al., *Shattering Lives and Myths: A Report on Image-Based Sexual Abuse*, Durham University - University of Kent, 2019, il report è liberamente accessibile al link: https://durham-repository.worktribe.com/output/1605209).

[18] Si segnala che le anzidette ipotesi di "voyeurismo digitale" sono state rese oggetto di incriminazioni specifiche tanto in Inghilterra (*section* 67A del *Sexual Offences Act*), quanto in Germania (§ 184k dello *Strafgestzbuch*). Sul punto, G.M. Caletti, Habeas corpus *digitale*, cit., p. 103.

[19] Cfr. M. Botto, *Le molestie sessuali "dentro" e "fuori" dal confine dell'art. 609* bis *c.p.*, cit., pp. 1-55.

indesiderato, verbale, non verbale o fisico, di natura sessuale, con lo scopo o l'effetto di violare la dignità di una persona, segnatamente quando tale comportamento crea un clima intimidatorio, ostile, degradante, umiliante o offensivo».

Accingendosi a proporre una disamina che consideri la rilevanza penale dei fenomeni all'attenzione nell'ambito dell'ordinamento giuridico nazionale per poi assumere, a partire dal confronto con prescrizioni rilevanti della recente Direttiva europea, una prospettiva *de iure condendo*, risulta funzionale evidenziare i tratti distintivi di un concetto contraddistinto da un raggio applicativo così esteso, il quale, pertanto, presenta *in re ipsa* criticità sul piano della tassatività. In particolare, tali elementi possono sintetizzarsi come segue: (a) la presenza di comportamenti sessualmente connotati e non voluti/indesiderati (*id est: unwelcome*) da parte di colui che ne è destinatario, i quali (b), sul piano degli effetti, risultano essere idonei a dispiegare un impatto significativo sulla sfera psico-emotiva di quest'ultimo. A ben vedere, i detti requisiti si ripresentano anche quando ad essere considerata è quella che si è avuto modo di definire come una specie del genere "molestie sessuali"; rilevato che le "*cyber-sexual harassment*", nel loro nucleo essenziale, altro non sono se non comportamenti sessualmente connotati che hanno luogo online e comportano effetti speculari a quelli appena richiamati.

3. *Molestie sessuali e diritto vivente: i disorientamenti derivanti da una "doppia narrazione"*

Il confronto con la dimensione "digitale" delle molestie sessuali, dal canto suo, conduce a rilevare che un tratto comune alle condotte che vi rientrano è, inevitabilmente, l'assenza del coinvolgimento della sfera corporea della persona. Ai fini di un'indagine sulla rilevanza penale degli anzidetti comportamenti nell'ordinamento giuridico italiano, un simile rilievo finisce, in particolare, non solo con l'assumere la funzione di apripista, ma, parallelamente, consente anche di muovere da un punto di partenza: l'assenza di una fattispecie *ad hoc* per le molestie sessuali. Come noto, infatti, la disciplina dei reati sessuali è la risultante dell'impianto normativo definito con la legge 15 febbraio 1996, n. 66 («*Norme contro la violenza sessuale*»). E, nello specifico, se, in tale occasione, il legislatore ha inciso in modo determinante sulla portata applicativa del delitto di violenza sessuale (art. 609-*bis* c.p.), conferendogli la formulazione "unificata"[20] che ancora oggi lo caratterizza, al contempo non ha disposto l'introduzione di un'ipotesi "minore" e specifica per le molestie, nonostante quest'ultima comparisse in taluni progetti anteriforma e si potessero ravvisare, già al tempo, sollecitazioni della dottrina in tal senso.

[20] Con la riforma del 1996, infatti, nel reato di violenza sessuale è stato disposto l'accorpamento dei previgenti delitti di violenza carnale e atti di libidine violenti (artt. 519 e 521 c.p.) e il concetto di «atti sessuali», non definito dal legislatore, è divenuto il baricentro dell'incriminazione.

Passando dalla *law in the books* alla *law in action*, i comportamenti riconducibili alla categoria in parola si sono quindi trovati (e si trovano tuttora) ad essere oggetto di una sorta di "doppia narrazione", potendo, di fatto, ricadere sia "dentro" che "fuori" dall'ambito applicativo dell'art. 609-*bis* c.p. E, in particolare, a risultare determinante per l'integrarsi dell'una piuttosto che dell'altra soluzione qualificatoria è la presenza o meno di un coinvolgimento della dimensione fisico-corporea del soggetto passivo.

Nella prima eventualità, anche episodi percepiti nel sentire comune come "molesti" possono infatti essere attratti nell'orbita del reato di violenza sessuale. Questi, dunque, convivono, sotto lo spettro di un comune *nomen iuris*, con gravi forme di aggressione alla sfera sessuale della persona[21]; all'opposto, invece, qualora manchi una "dimensione corporea" le soluzioni offerte in giurisprudenza sono estremamente diversificate, data l'assenza di un'incriminazione specifica in grado di ricomprenderle. Quello a cui si assiste, quindi, è un quadro di diritto vivente composito e "frammentato", dove, rispetto alla "onnicomprensività" del reato di violenza sessuale, si avvertono tensioni non solo in materia di tassatività-determinatezza, ma anche in punto di proporzionalità; a cui si affiancano, nei riguardi delle molestie "non fisiche" (o "extracorporee"), i disorientamenti che si correlano alla eterogeneità delle loro possibili qualificazioni giuridiche.

A ben vedere, la prima delle due "conseguenze" annoverate è riconnessa al fatto che la portata applicativa del reato di violenza sessuale – già estesa per definizione, considerata la sua "veste unificata" – è oggetto di una progressiva espansione verso il basso, stratificatasi negli orientamenti giurisprudenziali, la quale si manifesta in particolar modo nell'ambito della casistica relativa ai cosiddetti atti repentini o a sorpresa, da sempre oggetto di attenzione da parte della dottrina[22].

Per contro, relativamente al secondo ordine di effetti, come si anticipava, quando si fuoriesce dai casi di molestie sessuali di natura fisica, comportamenti comunque ascrivibili al *genus* molestie sessuali si trovano ad essere privi di uno "specifico contenitore di riferimento" in grado di coglierne il disvalore (nei termini di offesa alla libertà di autodeterminazione sessuale).

[21] Sulle tensioni che derivano, in punto di proporzionalità, dall'attribuzione di un medesimo *nomen iuris* a fatti dotati di un disvalore offensivo estremamente differenziato, si vedano i rilievi di A. CADOPPI, *Il "reato penale". Teorie e strategie di riduzione della criminalizzazione*, Edizioni Scientifiche Italiane, Napoli, 2022, pp. 300 ss.; G.M. CALETTI, *Dalla violenza al consenso nei delitti sessuali. Profili storici, comparati e di diritto vivente*, Bologna University Press, Bologna, 2023, pp. 254 ss. e M. BOTTO, *Le molestie sessuali alla prova del diritto vivente. Dall'ipertrofia applicativa dell'art. 609-bis c.p. a un insieme (fin troppo vario) di "soluzioni di completamento"*, in «Diritto penale contemporaneo – Rivista trimestrale», 4 (2024), pp. 115-120.

[22] A tal proposito, ci si limita a ricordare che si tratta di un processo derivante, da un lato, dalla definizione di atti sessuali mediante l'impiego di un concetto di zone erogene che in via ermeneutica assume una valenza molto più estesa di quella che gli era stata attribuita nella sua elaborazione dottrinale; e, dall'altro, dall'impiego di approcci che affiancano al criterio anatomico-culturale quello contestuale-relazionale. Per una prospettiva critica, rispetto all'ampia estensione verso il basso della fattispecie, per tutti, A. CADOPPI, *La violenza sessuale alla ricerca della tassatività perduta*, in «Diritto penale e processo», 11 (2016), pp. 1469-1479.

D'altronde, a partire dalla riforma del 1996, la tutela penale dell'anzidetto bene giuridico è stata sostanzialmente affidata in via esclusiva alla fattispecie violenza sessuale. Le ipotesi delittuose che seguono il reato *de quo* – con la sola eccezione della violenza sessuale di gruppo (art. 609-*octies* c.p.), la cui tipicità è comunque definita mediante un rinvio al delitto di violenza sessuale – infatti non sono poste tanto a garanzia della libertà sessuale (negativa), ma piuttosto dell'integrità psicofisica del minore (artt. 609-*quater* ss. c.p.), proteggendone lo sviluppo della personalità nella sfera affettiva e sessuale. Al contempo, inoltre, nel codice penale italiano, si riscontra anche l'assenza di incriminazioni specifiche per gli atti di esibizionismo (nei confronti di vittime non minorenni[23]) o di voyeurismo, le quali, in altri ordinamenti, si pongono a "completamento" rispetto alle fattispecie rientranti tra i reati *stricto sensu* sessuali.

Un simile quadro implica che le soluzioni offerte dalla casistica, dinnanzi ad episodi privi di una componente fisica (e, dunque, qualificabili come di "mera molestia") ovvero ascrivibili alle ultime due categorie menzionate, constano nel richiamo ad una rosa di fattispecie poste a garanzia degli interessi più disparati.

Invero, tanto che ci si muova nel *cyberspazio*, quanto che si tratti di qualificare episodi di molestie "non corporee" nella realtà offline, vengono in gioco incriminazioni che non sono poste a tutela della sfera sessuale della persona, ma rivolte a garanzia di altri beni giuridici. Questi, infatti, vanno dal comune senso del pudore, a cui si riferiscono gli atti osceni in luogo pubblico (art. 527 c.p.)[24], alla libertà morale, allorquando i fatti vengono qualificati come di violenza privata (art. 610 c.p.) o sono sussumibili nel reato di atti persecutori (art. 612-*bis* c.p.), sino all'ordine e alla tranquillità pubblica ovvero, in termini più contemporanei, alla «tranquillità personale»[25], nel caso in cui si faccia ricorso alla contravvenzione di «molestia o disturbo alle persone» (art. 660 c.p.). Inoltre, al cospetto di azioni che integrano gli estremi della diffamazione o della minaccia potrebbero ricorrere altresì le relative incriminazioni. Se, infine, l'attenzione si circoscrive al contesto online e ai comportamenti che si sono esemplificati come rientranti tra le

[23] Posto che, in caso di vittime minorenni, potrebbe integrarsi il reato di cui all'art. 609 *quinquies* c.p. («corruzione di minorenne»).

[24] Si ritiene necessario precisare che, a seguito della parziale depenalizzazione dell'art. 527 c.p. (d.lgs. 15 gennaio 2016, n. 8), il primo comma della fattispecie originaria è divenuto mero illecito amministrativo. Di conseguenza, l'ipotesi di cui al comma 2 (che prima costituiva una variante aggravata del delitto in parola) finisce oggi con l'essere un reato autonomo. Nello specifico, si rivolge al caso in cui gli atti osceni in luogo pubblico o esposto al pubblico siano commessi «all'interno o nelle immediate vicinanze di luoghi abitualmente frequentati da minori» e vi sia il pericolo concreto che i minori vi assistano. Preso atto di questo, il bene giuridico tutelato dalla disposizione, come evidenziato dalla Suprema Corte, attualmente coincide in realtà con la «"privacy sessuale" dei minori, da intendere come tutto ciò che afferisce al riserbo della loro sfera sessuale», Cass. pen., Sez. III, sent. n. 49550, 22 giugno 2017 (dep. 27 ottobre 2017), in *www.penalecontemporaneo.it*, 22 novembre 2017.

[25] Sia in giurisprudenza che in dottrina è diffusa la tendenza a ridefinire il bene giuridico della fattispecie contravvenzionale in parola nei termini di «tranquillità personale» (v., anche per gli opportuni riferimenti bibliografici e giurisprudenziali, F. Basile, *Commento all'art. 660 – Molestia o disturbo alle persone*, in *Codice penale commentato*, diretto da E. Dolcini e G.L. Gatta, coordinato da A. Galluccio e M.C. Ubiali, IV, Wolters Kluwer, Milano, 2021[5], p. 82).

molestie (sessuali) digitali – fermo restando che, purché siano soddisfatti i requisiti di tipicità della fattispecie, nell'ambito dell'art. 612-*bis* c.p., è presente un'aggravante *ad hoc* per il cosiddetto cyberstalking (comma 2) – qualora ne ricorrano i presupposti, si potrebbe assistere al richiamo dei delitti di interferenze illecite nella vita privata e accesso abusivo ad un sistema informatico o telematico (artt. 615-*bis* e *ter* c.p.)[26].

Di fronte a condotte qualificabili come di "mera molestia" – che siano gestuali, verbali, esibizionistiche o altrimenti invasive della sfera sessuale – la giurisprudenza, quindi, laddove ravvisi la rilevanza penale del caso concreto, si trova "costretta a dover operare una scelta", che è inevitabilmente condizionata dal soddisfacimento dei connotati tipici delle singole fattispecie, i quali, in ogni caso, trattandosi di reati che non sono posti a garanzia dell'autodeterminazione sessuale, non considerano il profilo dell'interessamento della sfera sessuale dell'individuo.

In un contesto che, quindi, assume i caratteri dell'"inevitabile incertezza", accade altresì che, in talune decisioni di legittimità, operando di fatto una "ri-denominazione" della fattispecie, si arrivi ad impiegare l'espressione "molestie sessuali" con riferimento alla contravvenzione di cui all'art. 660 c.p. Tale "impropria assimilazione" ha luogo in pronunce che affrontano il tema della determinazione del confine verso il basso del reato di violenza sessuale, e, tendenzialmente, si pone a margine del rilievo secondo cui quest'ultimo non è atto a ricomprendere «espressioni volgari a sfondo sessuale ovvero di atti di corteggiamento invasivo ed insistito diversi dall'abuso sessuale […] ove lo "sfondo sessuale" costituisce soltanto un motivo e non un elemento della condotta»[27] (*id est*: ciò che, in via residuale, è considerato dalla giurisprudenza "molestia sessuale")[28].

La reviviscenza dell'art. 660 c.p., da contravvenzione introdotta a tutela della "pubblica quiete" a fattispecie di riferimento per le molestie sessuali (non fisiche), si riverbera anche tra le maglie della casistica afferente ad episodi avvenuti nel contesto digitale. Per il tramite di un'interpretazione estensiva del «mezzo telefono»[29], infatti, il reato in parola, sembra aver trovato uno spazio applicativo in casi di comporta-

[26] Il delitto di «interferenze illecite nella vita privata» (art. 615-*bis* c.p.) si rivolge alla condotta di chiunque mediante «l'uso di strumenti di ripresa visiva o sonora si procura indebitamente notizie o immagini» attinenti, appunto, alla vita privata di un terzo, che hanno luogo nell'ambito dell'altrui spazio domiciliare (per cui si rimanda alla nozione di domicilio rilevante ai sensi dell'art. 614 c.p.); il successivo all'art. 615 *ter*, invece, modellandosi sul delitto di cui all'art. 614 («violazione di domicilio»), incrimina l'accesso abusivo ad un sistema informatico.

[27] Cfr., di recente, Cass. pen., Sez. III, sent. n. 32770, 11 luglio 2024 (dep. 21 agosto 2024) e Cass. pen., Sez. III, sent. n. 22 giugno 2023 (dep. 27 dicembre 2023), entrambe in *DeJure*; in precedenza, già Cass. pen., Sez. III, sent. n. 38719, 26 settembre 2012 (dep. 4 ottobre 2012), in *DeJure*, in cui si è rilevato che: «La molestia sessuale si differenzia dall'abuso, anche nella forma tentata, in quanto prescinde da contatti fisici a sfondo sessuale e normalmente si estrinseca o con petulanti corteggiamenti non graditi o con petulanti telefonate o con espressioni volgari, nelle quali lo sfondo sessuale costituisce un motivo e non un momento della condotta» (richiamando, in senso conforme, Cass. pen., Sez. III, sent. n. 45957 del 26 ottobre 2005, Rv. 233319).

[28] Per un'analisi approfondita del diritto vivente, sia consentito il rinvio a M. Botto, *Le molestie sessuali alla prova del diritto vivente*, cit., pp. 95-126.

[29] Per agevolare il lettore, si ricorda che ai sensi dell'art. 660 c.p. è richiesto, alternativamente, che la condotta sia stata posta in essere «a mezzo telefono» oppure «in un luogo pubblico o aperto al pubblico».

menti intrusivi e sessualmente connotati, posti in essere dall'autore anche mediante le (nuove) tecnologie di comunicazione, che hanno luogo nell'ambito di conversazioni private[30] (*infra*, § 4).

L'anzidetta soluzione ermeneutica "a rime forzate", in ogni caso, desta perplessità. A tacer d'altro, la contravvenzione in parola è *in re ipsa* una fattispecie inidonea a cogliere la presenza di un'offesa che coinvolge la dimensione più intima della persona; e, questo, a partire dai suoi connotati tipici, rimasti immutati rispetto alla sua formulazione originaria, allorquando, lungi dall'essere posto a garanzia diretta di una prerogativa del singolo, il reato era piuttosto orientato a tutelare la dimensione individuale «in via mediata, ed in vista pur sempre dell'ordine pubblico»[31].

4. *La Direttiva UE 1385/2024 e gli obblighi di incriminazione in materia di "*mob attack*" e "*cyberflashing*"*

Muovendo dalla controversa narrazione delle molestie sessuali nel diritto vivente, non resta che aggiungere un tassello alla riflessione che consideri gli obblighi di incriminazione derivanti dalla Direttiva UE 1385/2024. La tematica delle molestie sessuali "virtuali", infatti, si riverbera tra le pagine del documento. Nello specifico, il legislatore sovranazionale ha dedicato una disposizione *ad hoc* alla più generale tematica delle «*molestie online*» (art. 7) e, nel farlo, ha individuato quattro gruppi di comportamenti "molesti", accomunati dall'essere perpetrati mediante l'uso delle tecnologie di informazione e comunicazione.

A ben vedere, la prima ipotesi annoverata (lett. a)), ponendosi di fatto a completamento del precedente art. 6 («*Stalking online*»), sembra rivolgersi a una casistica che, nel contesto italiano, potrebbe essere colta non solo dal reato di minaccia (art. 612 c.p.), ma anche dal cosiddetto cyberstalking (art. 612-*bis*, comma 2, c.p.), posto che concerne la reiterazione di comportamenti minacciosi, che siano tali da indurre la persona offesa a «temere seriamente per la propria incolumità o per l'incolumità di persone a carico». *Mutatis mutandis*, considerazioni specifiche riguardano l'ultimo caso individuato (lett. d)), il quale ha ad oggetto la pratica del «*doxing*» e, in particolare, afferisce al «rendere accessibile al pubblico […] materiale contenente i dati personali di una persona, senza il consenso di quest'ultima, al fine di istigare altre persone ad arrecare un danno fisico o psicologico grave alla persona in questione». Siffatta condotta, infatti, sembra fuoriuscire dal campo delle molestie sessuali e integrare, piuttosto, *de lege ferenda*, la materia dei possibili interventi sul fronte dei "*gender-based hate crimes*". Atteso che, anche alla luce delle prescrizioni sovranazionali contenute nel successivo art. 8 («*Istigazione alla*

[30] Cfr. M. Botto, *Le molestie sessuali "dentro" e "fuori" dal confine dell'art. 609* bis *c.p.*, cit., p. 48.

[31] G.M. Flick, *Molestia o disturbo alle persone*, in *Enciclopedia del diritto*, XXVI, Giuffrè, Milano, 1976, p. 699.

violenza o all'odio online»)[32], il legislatore italiano dovrà confrontarsi con le esigenze di riforma dei cosiddetti crimini d'odio – e, nello specifico, del delitto di cui all'art. 604-*bis* c.p. –, pare questo il contesto in cui potrebbe confluire anche il caso *de quo.*

Di maggiore interesse per il discorso in oggetto risultano quindi essere le due ipotesi centrali.

In particolare, l'art. 7, lett. b) si rivolge al caso di chi assume «pubblicamente, insieme ad altre persone […] comportamenti minacciosi o ingiuriosi», così da arrecare un «grave danno psicologico» al soggetto passivo. A seguire, la lettera c) attiene all'invio «a una persona senza che questa lo richieda» di «un video o altro materiale analogo raffigurante i genitali qualora tale condotta possa arrecare un grave danno psicologico alla persona in questione».

Seppur la rosa dei comportamenti oggetto di specifici obblighi di incriminazione non esaurisce la complessità delle condotte che, come si è visto, possono rientrare nell'ampia categoria delle molestie sessuali "virtuali", si ritiene comunque funzionale, per le ragioni che si illustreranno, un approfondimento delle due fattispecie appena richiamate.

La lettera b) è rappresentativa degli episodi di "*mob attack*" (o "*shit-storm*"), ovverosia del "linciaggio online" che ha luogo quando, sulle piattaforme digitali, un utente diviene il bersaglio di "attacchi" da parte di terzi, dai contenuti denigratori, offensivi o minacciosi, i quali si susseguono tra di loro trasformandosi in un vero e proprio "flusso". Nell'ordinamento italiano, la casistica *de qua* potrebbe rilevare – a seconda della condotta contestata nel caso concreto – come minaccia (art. 612 c.p.) ovvero come diffamazione (art. 595 c.p.) eventualmente aggravata dalla pubblicità del mezzo (comma 3)[33]. Entrambe le soluzioni, tuttavia, si ancorano a fattispecie, che – come si ricordava descrivendo la disomogeneità del quadro normativo di riferimento per le molestie sessuali "non fisiche" – non riescono a cogliere lo specifico disvalore che si rinviene quando le azioni descritte coinvolgono anche la sfera intimo-sessuale della persona.

Assumendo una prospettiva comparata, sembra che tale elemento non sia sfuggito al legislatore francese; laddove, nel 2018[34] – nella stessa occasione in cui si è disposta la criminalizzazione delle c.d. molestie di strada – ha modificato la (già presente) fattispecie di molestie sessuali (art. 222-33 c.p. francese), introducendo, al primo paragrafo della norma, due sotto-ipotesi, la cui *ratio*, come evidenziato in dottrina, è stata ricondotta

[32] In tal senso, S. BRASCHI, *La nuova direttiva sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., pp. 1375-1376.

[33] Atteso il consolidato orientamento giurisprudenziale che equipara i *social-network* ai mezzi di pubblicità ai fini del riconoscimento circostanza aggravante di cui al comma 3. *Ex plurimis*, Cass. pen., Sez. V, sent. n. 34057, 7 maggio 2024 (dep. 9 settembre 2024), in *DeJure*, in cui si è ribadito che: «La diffusione di un messaggio diffamatorio attraverso l'uso di un social network (come Instagram o Facebook) integra un'ipotesi di diffamazione aggravata ai sensi dell'art. 595, comma 3, c.p., sotto il profilo dell'offesa arrecata "con qualsiasi altro mezzo di pubblicità" diverso dalla stampa, poiché la condotta in tal modo realizzata è potenzialmente capace di raggiungere un numero indeterminato, o comunque quantitativamente apprezzabile, di persone».

[34] Si tratta, nello specifico, dell'intervento normativo operato con la *LOI n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes.*

proprio all'esigenza di fornire una risposta *ad hoc* ai fenomeni di "*harcèlement par raid numérique*" (espressione francese evocativa delle stesse condotte oggetto di quelle anglofone che si sono richiamate)[35].

Nello specifico, l'ipotesi base di «*harcèlement sexuel*» si rivolge alla condotta di colui che impone ad un altro, ripetutamente, osservazioni o comportamenti a connotazione sessuale oppure sessista, i quali a causa del loro carattere umiliante o degradante, ledono la dignità di chi ne è vittima oppure creano nei suoi confronti una situazione intimidatoria, ostile o offensiva[36].

A seguire, si collocano le due nuove sotto-ipotesi, dove di fatto si creano delle eccezioni alla reiterazione della condotta (lett.: *répétition*)[37]. Nel dettaglio, la prima riguarda l'eventualità in cui più persone, "in maniera concertata" oppure su istigazione di una di esse, impongano alla vittima i comportamenti descritti nella prima parte della disposizione; mentre la seconda è rivolta alla circostanza in cui si verifichi un "susseguirsi di condotte", anche in assenza di una previa *concertation* tra gli autori, e ciascuna di esse venga posta in essere individualmente. In quest'ultimo caso, il legislatore, afferma, in sostanza, che la consapevolezza, in capo ai vari attori, della sequenzialità delle azioni – le quali quindi possono essere verbali o di altro genere – è un elemento sufficiente a ritenere integrato il requisito della ripetizione degli atti[38].

Soffermandosi invece sulla lettera c) dell'art. 7 della Direttiva, la disposizione è sostanzialmente rivolta al fenomeno del "*cyberflashing*", il quale, nel Regno Unito, è divenuto oggetto di un'incriminazione *ad hoc* alla *section* 66A («*Sending etc photograph or film of genitals*») del *Sexual Offences Act* (SOA), a seguito dell'entrata in vigore, il 26

[35] Cfr. C. Claverie-Rousset, *Commentaire des principales dispositions de la loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles ou sexistes*, in «Droit Pénal», 10 (2018), pp. 9-16. Per completezza, si rileva che le dette "sotto-ipotesi", nella stessa occasione, sono state introdotte anche nell'ambito della più generale fattispecie di «*harcèlement moral*» (art. 222-33-2-2 c.p. francese).

[36] A seguire il testo in lingua originaria dell'art. 222-33, par. 1: «*Le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante*».

[37] A onor del vero, si deve altresì ricordare che ai sensi del par. 2 è prevista un'ulteriore ipotesi derogatoria del requisito della reiterazione. Precisamente si dispone, infatti, che è assimilata alle molestie sessuali qualsiasi forma di pressione grave, anche non reiterata, esercitata allo scopo (reale o apparente) di ottenere un atto di natura sessuale, sia esso ricercato a vantaggio dell'autore degli atti o a beneficio di un terzo (lett.: «*Est assimilé au harcèlement sexuel le fait, même non répété, d'user de toute forme de pression grave dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers*»). Sul punto, L.C. Hébert, *Dignity and Discrimination in Sexual Harassment Law: A French Case Study*, in «Washington and Lee Journal of Civil Rights and Social Justice», 25(1), (2018-2019), pp. 3-50 (spec. p. 11).

[38] Per completezza, si riporta il testo in lingua originaria della seconda parte del par. 1 dell'art. 222-33: «[1] *Lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée* […] [2] *Lorsque ces propos ou comportements sont imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une repetition*».

ottobre 2023, dell'*Online Safety Act*[39]. Si tratta, a ben vedere, di una "nuova frontiera" dell'esibizionismo (sessuale), che, tenendo ferma la comparazione con la realtà inglese, risulta essere a sua volta oggetto di una fattispecie specifica (*section* 66, SOA).

Quanto all'ordinamento italiano, atteso che, da un lato, come noto, si registra l'assenza di una "generica" fattispecie di molestie sessuali e, dall'altro, non si rinvengono ipotesi atte ad incriminare in modo specifico gesti di esibizionismo imposti ad un terzo (eccezion fatta, come si ricordava, per il caso in cui la vittima sia un minore), simili comportamenti, quando sono perpetrati nella realtà "non virtuale", tendono a seconda dei casi ad essere qualificati nell'ambito del reato di violenza privata (art. 610 c.p.), ovvero, a seguito della parziale depenalizzazione della norma, della "residuale" fattispecie di atti osceni in luogo pubblico (art. 527, comma 2, c.p.), sino a porter ricadere, di nuovo, nella già più volte richiamata contravvenzione di molestia o disturbo alle persone (art. 660 c.p.).

Concentrandosi sul contesto online – e, di conseguenza, anche a fronte dei comportamenti descritti all'art. 7, lett. c) – la detta contravvenzione pare delinearsi come una delle principali *sedes* di riferimento. Va infatti precisato altresì che, nei casi di specie, difficilmente, potrebbe ricorrere il reato di cui all'art. 612-*bis*, comma 2, c.p. Invero, ai sensi di quest'ultima fattispecie sono necessarie tanto la reiterazione della condotta, quanto l'integrazione di almeno uno degli eventi tipizzati dalla norma; all'opposto, il "*cyberflashing*" di regola si manifesta a partire da un singolo episodio di invio di un contenuto indesiderato, che può avvenire con mezzi e modalità diverse: per il tramite di applicazioni di messaggistica istantanea, via *chat* o *e-mail*, mediante *sharing bluetooth* o *AirDrop* e così via dicendo.

Attesi, quindi, i già menzionati orientamenti di legittimità in conformità dei quali si registra un'interpretazione estensiva del richiamo al «mezzo telefono» focalizzata sulla «invasività del mezzo»[40], pare piuttosto prospettabile che l'ipotesi di riferimento per la fattispecie in oggetto sia proprio il reato *ex* art. 660 c.p. Tuttavia, nonostante sulla scorta di simili argomentazioni la contravvenzione sia stata ritenuta integrata anche in episodi afferenti a conversazioni avvenute via *WhatsApp*[41], si deve evidenziare che la presenza di un richiamo testuale ad un mezzo specifico – il telefono, appunto –, e non, più in generale, agli «strumenti informatici o telematici» (come avviene, invece, nell'ambito dell'art. 612-*bis*, comma 2, c.p.), comporta che la giurisprudenza dovrà

[39] Sul punto, nella dottrina italiana, sia consentito di richiamare nuovamente M. Botto, *Le molestie sessuali "dentro" e "fuori" dal confine dell'art. 609* bis *c.p.*, cit., p. 46 (nota 155), in cui, prima dell'approvazione, si faceva riferimento al testo dell'*Online Safety Bill*, HL Bill 87(Rev). Più di recente, Id., *Le molestie sessuali alla prova del diritto*, cit., p. 115 (nota 102) nonché G.M. Caletti, Habeas corpus *digitale*, cit., p. 205.

[40] Si veda, ad esempio, Cass. pen., Sez. I, sent. n. 37974, 18 marzo 2021 (dep. 22 ottobre 2021), in *DeJure*, dove l'assimilazione della messaggistica tramite *WhatsApp* al telefono, è stata motivata come segue: «ciò che rileva è l'invasività in sé del mezzo impiegato per raggiungere il destinatario, non la possibilità per quest'ultimo di interrompere l'azione perturbatrice, già subita e avvertita come tale, ovvero di prevenirne la reiterazione, escludendo il contatto o l'utenza sgradita senza nocumento della propria libertà di comunicazione».

[41] *Ibidem.* Sia consentito inoltre, il rinvio a M. Botto, *Le molestie sessuali "dentro" e "fuori" dal confine dell'art. 609* bis *c.p.*, cit., p. 48 e Id., *Le molestie sessuali alla prova del diritto vivente*, cit., pp. 113-115.

valutare, caso per caso, se la nuova tecnologia di comunicazione impiegata possa essere equiparata ad esso. Inoltre, anche ammesso che questo avvenga, continuano a riemergere, ancora una volta, i profili critici correlati alla non idoneità della fattispecie *de qua* a cogliere la specificità di un'offesa alla dimensione intimo-sessuale della persona, che spingono a rilevare quanto quest'ultima sia, di fatto, impropriamente tratteggiata dalla prassi come un reato di molestie sessuali.

5. *Brevi note di sintesi*

Alla presenza di un contesto così controverso, che affonda le sue radici nell'assenza di una specifica norma incriminatrice per le molestie sessuali e si manifesta anche di fronte alle "nuove frontiere virtuali" della problematica, si registrano quindi le criticità derivanti dalle "asimmetrie" connesse alla duplice narrazione di fenomeni che sono ascrivibili ad una stessa categoria di appartenenza. E, di conseguenza, si avverte l'opportunità di considerare un intervento normativo finalizzato ad introdurre una fattispecie *ad hoc*, nella quale considerare tutte le dimensioni della tematica in oggetto.

Da ciò deriva che anche le riflessioni effettuate in sede di verifica della capacità del quadro normativo interno di soddisfare le esigenze di tutela penale richieste dalla recente Direttiva europea (e, nello specifico, quelle relative alle forme di TFSV rilevanti), sembrano in realtà destinate a non essere trattate in modo svincolato da una riflessione complessiva sulle prospettive di riforma dei delitti sessuali, ma piuttosto ad integrarsi con essa. In altri termini, l'esigenza di chiarire maggiormente la qualificazione giuridica delle "*cyber-sexual harassment*" finisce con l'incardinarsi nell'ambito di un ripensamento organico dei reati a tutela dell'autodeterminazione sessuale, in cui, preso atto del contesto attuale, la riflessione *de iure condendo* dovrebbe articolarsi su più livelli.

Invero, questa dovrebbe muovere dalla sempre più tangibile necessità di riformulare l'art. 609-*bis* c.p. superando l'approccio ispirato da un modello "vincolato"[42], rimasto immutato dagli anni Novanta, allo scopo di addivenire ad una ridefinizione della fattispecie incentrata sull'assenza del consenso. Posto che non è questa la sede per approfondire nel dettaglio la questione, ci si limita a rilevare che tale esigenza risulta essere non solo motivata dalle sollecitazioni sovranazionali[43] e orientata ad allineare il quadro

[42] Si ricorda, infatti, che guardando al dettato normativo, ai sensi del comma 1 dell'art. 609-*bis* c.p., anziché fissare la soglia della rilevanza penale della condotta sulla base dell'elemento del dissenso del soggetto passivo (o, ancor di più, della mancanza di consenso), si è continuata a richiedere la presenza dell'impiego di mezzi di costrizione qualificati che sorreggono l'azione dell'agente (*id est:* la violenza, la minaccia e l'abuso di autorità).

[43] Cfr. il rapporto del Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), *Baseline Evaluation Report Italy (Adopted on 15 November 2019)*, GREVIO/Inf(2019)18, pubblicato il 13 gennaio 2020, p. 8, relativo al monitoraggio del livello di implementazione della Convenzione di Istanbul nello Stato italiano, dove si è evidenziata l'opportunità che il legislatore intervenisse allo scopo di rendere la definizione del delitto di «violenza sessuale» conforme a quella dell'art. 36 del menzionato testo convenzionale (ai sensi del quale questa è definita sulla base dell'elemento del consenso della persona coinvolta). A margine, si

normativo italiano alle tendenze di riforma della materia che stanno interessando gli altri Paesi europei[44], ma anche indirizzata a ripristinare il rispetto del principio di legalità che oggi sfuma a causa di una riscrittura giurisprudenziale della tipicità del reato. In particolar modo nelle più recenti pronunce di legittimità, infatti, si assiste al consolidarsi di un "superamento (giurisprudenziale) della costrizione violenta nella violenza sessuale per costrizione" (art. 609-*bis*, comma 1, c.p.), da cui derivano tensioni manifeste con il principio di legalità[45]. In tali orientamenti, di fatto, il consenso della persona coinvolta diviene il baricentro della tipicità del reato in parola, mentre resta immutata la lettera della legge in cui è ancora presente un richiamo a specifiche modalità della condotta, e in particolare, alla costrizione mediante violenza. Nella trama di un percorso di progressivo allontanamento tra disposizione e norma[46], si assiste, in altri termini, ad una ridefinizione ermeneutica dei connotati tipici della fattispecie, che disvela criticità anche con riguardo ai profili di prevedibilità, atteso che, oltretutto, non sempre gli orientamenti della Suprema Corte sono fatti propri dalla giurisprudenza di merito[47].

Al contempo, come è emerso dalla presente analisi, in una prospettiva di riforma, si è chiamati a considerare altresì il complesso delle ipotesi "minori" di lesione al bene giuridico *de quo*, ovverosia le varie forme di molestia sessuale (fisiche, gestuali, verbali; offline ed online), e, *de lege ferenda*, a valutare l'opportunità di introdurre una disposizione rivolta specificatamente a contenere simili ipotesi.

sottolinea, inoltre, che, anche se – per ragioni legate alla competenza in campo penale dell'Unione (art. 83, par. 1, TUFE) – è scomparsa dalla versione finale Direttiva UE 1385/2024 la norma che, nella bozza originaria, introduceva, nel novero degli obblighi di incriminazione, una prescrizione afferente all'armonizzazione della definizione della fattispecie di violenza sessuale sulla base dell'elemento del consenso, nel documento il ruolo del consenso nell'ambito delle relazioni sessuali viene comunque rimarcato. Si rileva, in particolare, che il legislatore europeo dedica un'intera disposizione (art. 35) alle «*Misure specifiche per prevenire lo stupro e promuovere il ruolo centrale del consenso nelle relazioni sessuali*».

[44] Per una prospettiva comparata, sia consentito il rinvio ai contributi raccolti nel volume a cura di T. Hörnle, *Sexual Assault. Law Reform in a Comparative Perspective*, Oxford University Press, Oxford, 2023. Relativamente a panoramica sull'ondata di riforme c.d. "*consent-based*" dei reati sessuali che sta riguardando l'Europa, v. S. Uhnoo, S. Erixon, M. Bladini, *The Wave of Consent-based Rape Laws in Europe*, in «International Journal of Law, Crime and Justice» (2024), pp. 1-16.

[45] Cfr., ad esempio, Cass. pen., Sez. III, sent. n. 19599, 19 aprile 2023 (dep. 10 maggio 2023), in *DeJure*. In dottrina, si vedano i contributi di: G. Balbi, Legem et iustitiam facere. *La giurisprudenza e il delitto di violenza sessuale*, in «Legislazione penale», 23 novembre 2023, pp. 1-29; M. Bertolino, *Spigolature a margine del seminario "La riforma dei reati contro la libertà e l'autodeterminazione sessuale"* e A.M. Maugeri, *Osservazioni sulle proposte in materia di reati sessualmente connotati del gruppo di lavoro dell'AIPDP*, entrambi in *La riforma dei delitti contro la persona. Proposte dei gruppi di lavoro dell'AIPDP. Atti dei seminari di discussione in collaborazione con il DiPLaP*, a cura di Associazione Italiana dei Professori di Diritto Penale e Laboratorio Permanente di Diritto e Procedura Penale, Edizioni DiPLaP, Milano, 2023, rispettivamente alle pp. 359-362 e 363-389; M. Botto, *Le molestie sessuali alla prova del diritto vivente*, cit., pp. 96-102, nonché l'opera monografica di G.M. Caletti, *Dalla violenza al consenso*, cit., *passim* (in particolare, v. il secondo Capitolo del volume, pp. 141-280, dedicato ad una puntuale ricostruzione dell'evoluzione giurisprudenziale in materia di art. 609-*bis* c.p.).

[46] In argomento, M. Donini, *Europeismo giudiziario e scienza penale. Dalla dogmatica classica alla giurisprudenza-fonte*, Giuffrè, Milano, 2011, pp. 87-92.

[47] Cfr. Trib. Busto Arsizio, 26 gennaio 2022, in *www.sistemapenale.it*.

A tale reato, in particolare, spetterebbe una doppia funzione.

Da una parte, quella di affermare un recupero del principio di proporzionalità "scorporando" i casi di molestia "fisica" che attualmente sono "assorbiti" dall'ampia portata dall'art. 609-*bis* c.p. incidendo, peraltro, anche sul fronte di una maggior determinatezza della sfera applicativa della più grave ipotesi di violenza/aggressione sessuale.

Dall'altra, considerata la presenza di forme di molestia sessuale "non fisiche", in cui ricadono anche (ma non solo) le ipotesi di "*cyber-sexual harassment*", si impone altresì l'esigenza di definire in che modo farle confluire nella nuova fattispecie. Come si è illustrato, infatti, nel complesso, le molestie sessuali constano in comportamenti intrusivi, non desiderati (*unwanted*) e connotati sessualmente, che possono avere una diversa natura: verbali o gestuali, appunto, oltre che fisici. In tutti questi casi, il diritto vivente offre soluzioni disomogenee e non idonee a fissare una distinzione tra le ipotesi di molestia caratterizzate da uno specifico disvalore offensivo, in quanto afferenti alla sfera intimo-sessuale dalla persona, e altre condotte che, seppur invasive, sono prive di una connotazione sessuale.

In conclusione, quindi, rilevata la necessità di superare le criticità derivanti dall'attuale assetto normativo, la sfida principale che si correla all'introduzione di un reato *ad hoc* sembra senz'altro essere quella che attiene alla definizione dei connotati tipici di una fattispecie che sia atta a contenere un così vario insieme di comportamenti. A prendere avvio, quindi, è un percorso che richiede un rigoroso confronto, anche comparato, con le tecniche di incriminazione adottate *in subiecta materia*, per il tramite del quale addivenire ad una definizione del perimetro del penalmente rilevante in conformità con i princìpi costituzionali.

SEZIONE 2

OFFESE ALLA PERSONA E CONTESTI DIGITALI: NUOVE PROSPETTIVE

PARTE 2

DISCORSI OFFENSIVI NELLO SPAZIO DIGITALE: REPUTAZIONE, *HATE SPEECH* E DISINFORMAZIONE

LA REPRESSIONE DELLE OFFESE ONLINE ALLA REPUTAZIONE: TRA ANOMIA DI CONTESTO E ANOMIA NORMATIVA*

Arianna Visconti

SOMMARIO: 1. Dal 'regime disciplinare' alla 'quarta rivoluzione' digitale: la persistenza delle (inossidabili?) fattispecie di ingiuria e diffamazione. – 2. (*Segue*) Nuove ICT e repressione penale delle offese all'onore e alla reputazione. Sintesi del quadro giurisprudenziale. – 3. Una duttilità solo apparente: problematiche applicative e vuoti di tutela. – 4. Un *caveat* conclusivo: la necessità di un «design pro-etico» dell'ecosistema digitale.

1. *Dal 'regime disciplinare' alla 'quarta rivoluzione' digitale: la persistenza delle (inossidabili?) fattispecie di ingiuria e diffamazione*

Guardando alla sua vitalità giurisprudenziale – cui sarà dedicata la parte centrale di questo contributo – sembra quasi incredibile come una fattispecie concepita negli anni Trenta del Novecento, nel pieno splendore del modello 'disciplinare' di focaultiana memoria[1], qual è ancora oggi la diffamazione[2], possa essersi adattata senza apparente soluzio-

* Si segnala che, nelle more della pubblicazione, è stata approvata la l. 23 settembre 2025, n. 132, recante *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, in vigore dal 10 ottobre 2025, il cui art. 26 ha introdotto alcune modifiche al Codice penale (oltre che ad altre disposizioni penali) rilevanti ai fini dell'analisi qui sviluppata. Se ne farà sintetico cenno ove pertinente, pur non essendone ovviamente possibile in questa sede un'analisi approfondita.

[1] Cfr. M. FOUCAULT, *Surveiller et punir. Naissance de la prison*, Gallimard, Paris, 1975 (trad. it., Einaudi, Torino, 1993), in part. pp. 147 ss.

[2] Per ovvi motivi, non sarà possibile, in questa sede, soffermarsi su molti degli aspetti tecnici della disciplina delle fattispecie sanzionatorie – penali (diffamazione) e civili (ingiuria) – a tutela dell'onore e della reputazione. In tema si rinvia dunque fin d'ora ampiamente, *ex plurimis*, ai recenti contributi di F. BELLAGAMBA, R. GUERRINI, *Delitti contro l'onore*, Giappichelli, Torino, 2010; L. BISORI, *I delitti contro l'onore*, in *I delitti contro l'onore e la libertà individuale*, vol. VIII del *Trattato di diritto penale. Parte speciale*, diretto da A. Cadoppi, S. Canestrari, A. Manna e M. Papa, UTET, Torino, 2010, pp. 3-209; S. BOLOGNINI, A. D'AVIRRO, M. D'AVIRRO, *La diffamazione. A mezzo stampa, radio, televisione e internet*, Giuffrè, Milano, 2022; A. GULLO, *Delitti contro l'onore*, in *Reati contro la persona*, a cura di F. Viganò, vol. XVII del *Trattato teorico-pratico di diritto penale*, diretto da F. Palazzo, C.E. Paliero e M. Pelissero, Giappichelli, Torino, 2022, pp. 213-312; F. MANTOVANI, *Diritto penale. Parte speciale*, I, *Delitti contro la persona*, CEDAM, Padova, 2013[5], pp. 200-258; N. MAZZACUVA, *Delitti contro la persona: le altre ipotesi di tutela*, in S. Canestrari, L. Cornacchia, A. Gamberini, G. Insolera, V. Manes, M. Mantovani, N. Mazzacuva, F. Sgubbi, L. Stortoni, F. Tagliarini, *Diritto penale. Lineamenti di parte speciale*, 7ª ed., Monduzzi, Milano, 2016, pp. 601-624; V. PEZZELLA, *La diffamazione*, UTET, Torino, 2020[2]; D. PROVOLO, *Dei delitti contro l'onore*, in *Commentario breve al Codice penale*, a cura di G. Forti, S. Riondato e S. Seminara, CEDAM, Padova, 2024[7], pp. 2260-2306; nonché, per aspetti e approfondimenti più specifici, agli ulteriori testi (anche più risalenti) e Autori citati *infra*.

ne di continuità all'era delle attuali 'infocrazie'[3], tanto da riuscire ancora (almeno all'apparenza) a svolgere il suo ruolo di tutela della reputazione anche in un ecosistema – quello delle comunicazioni digitali – che il legislatore dell'epoca non avrebbe potuto concepire neppure lontanamente. In meno di cento anni, infatti, si è assistito a una vera 'rivoluzione', cui pare necessario far cenno in esordio onde comprendere meglio, nel prosieguo, a quali fattori tale vitalità sia riconducibile e se, come e quanto essa sia effettiva, o non costituisca piuttosto un sottile velo sovrapposto a una realtà di sostanziale, e strutturale, ineffettività dell'attuale quadro normativo, come tale bisognoso di radicale ripensamento.

Come osserva Luciano Floridi, infatti, la «quarta rivoluzione» scientifica oggi in corso completa un processo di 'scardinamento' dell'autopercepita centralità umana nell'universo (materiale e simbolico) iniziato con Copernico (e la collocazione *fisica* dell'uomo nel mondo sensibile), proseguito con Darwin (frantumando l'idea di una radicale differenza e superiorità *biologica* umana nel regno animale) e approfondito da Freud (con la perdita dell'illusione di essere padroni almeno dei nostri *contenuti mentali*), con implicazioni e con una rapidità che, tuttavia, risultano ancor più destabilizzanti, per «la nostra comprensione di sé», delle 'rivoluzioni' precedenti: la costruzione di macchine in grado di superarci nella capacità di *processare informazioni*, infatti, ha fatto sì che «non siamo più gli indiscussi padroni» neppure «dell'infosfera»[4].

Con questo neologismo, coniato negli anni Settanta del secolo scorso[5], Floridi intende, in particolare, «*a un livello minimo* […], l'intero ambiente informazionale costituito

[3] Cfr. B.-C. Han, *Infokratie*, Matthes & Seitz, Berlin, 2021 (trad. it., Einaudi, Torino, 2023). Con questo termine il filosofo coreano indica un «regime dell'informazione», ossia una «forma di dominio nella quale l'informazione e la sua diffusione determinano in maniera decisiva, attraverso algoritmi e intelligenza artificiale, i processi sociali, economici e politici. Diversamente dal regime disciplinare», tipico della modernità, oggi «a essere sfruttati non sono *corpi ed energie*, ma *informazioni e dati*. Decisivo per la conquista del potere non è il possesso dei mezzi di produzione, bensì l'accesso a informazioni che vengono utilizzate ai fini della sorveglianza psicopolitica, del controllo e della previsione dei comportamenti. Il regime dell'informazione si accompagna al capitalismo dell'informazione, che evolve in capitalismo della sorveglianza e declassa gli esseri umani a *bestie da dati e consumo*. […] Il capitalismo dell'informazione, fondato sulla connessione e sulla comunicazione, rende obsolete [le] tecniche disciplinari […]. La docilità (*docilité*), che significa anche arrendevolezza e remissività, non è l'ideale del regime dell'informazione. Il soggetto sottomesso nel regime dell'informazione non è docile né ubbidiente. Piuttosto si crede *libero, autentico e creativo*: *produce* e *performa* sé stesso» (ivi, pp. 3-4).

[4] Cfr. L. Floridi, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, Oxford University Press, Oxford-New York, 2014 (trad. it., Cortina, Milano, 2017), pp. 99-105.

[5] Il primo ad averne fatto uso sembra essere stato l'economista e filosofo Kenneth E. Boulding, il quale riteneva che l'essere umano – come individuo e nei gruppi in cui è inserito, e dunque come essere sociale – potesse esistere ed essere concepito solo come 'nodo' in una 'rete' di *input* e *output* informativi, simbolici e linguistici, individuando sei 'sfere' in cui questi è strutturalmente inserito, ossia litosfera, atmosfera, idrosfera, biosfera, idrosfera, sociosfera e, appunto, infosfera, quest'ultima costituita da «*input* e *output* di conversazione, libri, televisione, radio, discorsi, servizi religiosi, lezioni, relazioni, nonché ogni informazione ricevuta dal mondo fisico tramite la nostra osservazione». Pur riconoscendone la natura di «segmento della sociosfera», riteneva tale 'segmento' dotato di autonomia e di una particolare rilevanza, e financo prevalenza sulle altre componenti di quest'ultima, dal momento che «qualsiasi forma di sviluppo [umano] è essenzialmente un processo di apprendimento e come tale è essenzialmente dipendente da una rete di flussi informativi» (cfr. K.E. Boulding, *Economics as a Science*, McGraw-Hill, New York, 1970, pp. 15-16; traduzione nostra). In tema cfr. anche B. Van der Veer Martens, *An Illustrated Introduction to the Infosphere*, in «Library Trends», 63/2 (2015), pp. 317-361.

da tutti gli enti informazionali, le loro proprietà, interazioni, processi e reciproche interazioni», dunque

> un ambiente paragonabile al, ma al tempo stesso differente dal, cyberspazio, che è soltanto una sua regione, dal momento che l'infosfera include anche gli spazi d'informazione offline e analogici. *A un livello massimo*, l'infosfera è un concetto che può essere utilizzato anche come sinonimo di realtà, laddove interpretiamo quest'ultima in termini informazionali. In tal caso, l'idea è che ciò che è reale è anche informazionale e ciò che è informazionale è reale. È in questa equivalenza che hanno origine alcune delle più profonde trasformazioni e delle sfide più rilevanti di cui faremo esperienza nel prossimo futuro riguardo alla tecnologia[6].

Ed è proprio quest'ultimo concetto 'espansivo' di infosfera a risultare particolarmente rilevante per la presente riflessione, dal momento che, al di là delle diverse concezioni giuspenalistiche dei beni 'onore' e 'reputazione' (che non è possibile qui ripercorrere in dettaglio)[7], da un punto di vista empirico-sociale – una dimensione con cui l'ordinamento non può a fare a meno di confrontarsi, a pena di un radicale 'scollamento' rispetto ai fenomeni che pretenderebbe di regolare e quindi, in definitiva, di una radicale ineffettività[8] – questi concetti risultano legati a filo doppio alla natura (anche) 'informazionale' del 'reale' (per come ne facciamo esperienza in quanto esseri umani).

La *reputazione*, in particolare, da un punto di vista squisitamente sociologico e *funzionale*, può essere compresa dinamicamente solo alla luce del concetto di «capitale sociale»[9], costituendo anzi una precondizione fondamentale per il mantenimento e/o

[6] Floridi, *The Fourth Revolution*, cit., pp. 45-45. Per un approfondimento cfr. altresì Id., *The Logic of Information. A Theory of Philosophy as Conceptual Design*, Oxford University Press, Oxford-New York, 2019 (trad. it., Cortina, Milano, 2020), in part. pp. 129 ss.

[7] Sul punto si rinvia pertanto, oltre che ai testi citati *supra* (nota 2), nelle parti pertinenti, anche, *ex multis*, a A. Gullo, *Diffamazione e legittimazione dell'intervento penale: contributo a una riforma dei delitti contro l'onore*, Aracne, Roma, 2013, in part. pp. 11-31; A. Manna, *Beni della personalità e limiti della protezione penale. Le alternative di tutela*. CEDAM, Padova, 1989, in part. pp. 3-91 e 177-231; E. Musco, *Bene giuridico e tutela dell'onore*, Giuffrè, Milano, 1974; A. Nappi, *Ingiuria e diffamazione*, in «Enciclopedia giuridica Treccani», XVIII, Treccani, Roma, 1989, in part. pp. 1-3; P. Siracusano, *Ingiuria e diffamazione*, in «Digesto delle discipline penalistiche», VII, UTET, Torino, 1993, pp. 32-36; M. Spasari, *Sintesi di uno studio sui delitti contro l'onore*, Giuffrè, Milano, 1961; Id., *Diffamazione e ingiuria (dir. pen.)*, in «Enciclopedia del diritto», XII, Giuffrè, Milano, 1964, pp. 483-487; A. Tesauro, *La diffamazione come reato debole e incerto*, Giappichelli, Torino, 2005, in part. pp. 1-24; nonché, per tutti gli opportuni ulteriori riferimenti, a A. Visconti, *Reputazione, dignità, onore. Confini penalistici e prospettive politico-criminali*, Giappichelli, Torino, 2018, in part. pp. 317-395.

[8] Cfr. per tutti G. Forti, *L'immane concretezza. Metamorfosi del crimine e controllo penale*, Cortina, Milano, 2000, *passim*, e in part. pp. 1-188 e 223 ss.

[9] Fondamentale, in tema, resta il contributo di James S. Coleman, il quale definisce il «capitale sociale» come la meno tangibile delle forme di 'capitale' a disposizione degli individui, in quanto «incorporato nelle *relazioni* tra le persone. Il capitale fisico e il capitale umano agevolano l'attività produttiva, e il capitale sociale fa la stessa cosa. Ad esempio, un gruppo i cui membri si dimostrano affidabili e hanno grande fiducia reciproca sarà in grado di fare molto di più di un gruppo per il resto simile ma privo di tali affidabilità e fiducia reciproca. […] Il capitale umano sta nei nodi» delle reti di cui è composto un gruppo, ossia nei singoli individui, mentre «il capitale sociale nelle linee che li congiungono». Nella prospettiva dell'individuo, «la funzione identificata dal concetto di "capitale sociale" è il valore che questi aspetti della struttura sociale hanno per gli attori, in

incremento di questo o, al contrario, ove 'danneggiata', per la sua erosione e/o perdita. La reputazione, infatti, quale elemento primario del *sé sociale* delle persone, costituisce essenzialmente – e ha valore per il suo titolare in quanto – 'patrimonio relazionale' della persona (fisica o giuridica, anche in senso lato), ossia un tipo di 'ricchezza immateriale' che si sostanzia in

> una forma di investimento in relazioni sociali in vista di un ricavo per l'investitore; e ciò sia che il ricavo abbia luogo in termini di reciprocità semplice (*do ut des*); sia che il ricavo abbia luogo in forma di comportamenti cooperativi, o in altri modi di collaborazione[10].

Come ogni 'capitale' di questo tipo, la reputazione è, dunque, un bene infungibile, non trasferibile[11] (pur se comunicabile, in particolare 'in verticale')[12], che connota il singolo soggetto che ne è titolare nella sua specificità e individualità, costituendo un suo esclusivo patrimonio; al tempo stesso, tuttavia, malgrado sia interesse e facoltà del titolare preservarla, o possibilmente incrementarla con azioni appropriate – e malgrado rientri nella sua sfera d'azione, ovviamente, anche danneggiarla e diminuirla con comportamenti soggetti a valutazioni sociali negative – la 'custodia' di questo capitale è largamente affidata ad *altri*, sia perché esso è, in pratica, 'depositato' nelle menti dei

quanto risorse che essi possono utilizzare per realizzare i propri interessi». Cfr. J.S. COLEMAN, *Foundations of Social Theory*, Belknap Press, Cambridge (MA)-London, 1990 (trad. it., il Mulino, Bologna, 2005), pp. 390-391, nonché ID., *Social Capital in the Creation of Human Capital*, in «American Journal of Sociology», 94/1 (1988), Supplement, pp. 95-120. Per ulteriori dettagli e riferimenti bibliografici si rinvia, *ex multis*, a A. ANDREOTTI, *Che cos'è il capitale sociale*, Carocci, Roma, 2009, e a J. FIELD, *Social Capital*, Routledge, London, 2003 (trad. it., Erickson, Trento, 2004). V. anche *infra*, nota seguente.

[10] Cfr. A. PIZZORNO, *Il velo della diversità. Studi su razionalità e riconoscimento*, Feltrinelli, Milano, 2007, p. 221. Si noti, per altro, come questo capitale individuale possa comportare vantaggi per l'intera comunità, dal momento che l'interesse dei singoli a mantenere una reputazione positiva può rafforzare la 'densità' e 'tenuta' di relazioni fiduciarie nei gruppi e nella società (cfr. ancora COLEMAN, *Foundations*, cit., pp. 385-412, nonché il fondamentale saggio di R. PUTNAM, *Bowling Alone. The Collapse and Revival of American Community*, Touchstone, New York, 2000, trad. it., il Mulino, Bologna, 2004) attraverso la spinta implicita al rispetto delle norme indispensabili alla sopravvivenza e funzionalità del gruppo/comunità di appartenenza, quanto e più della presenza di strumenti coercitivi esterni, vista la riconosciuta maggiore forza relativa delle sanzioni sociali informali (attuate o attese), e dei *payoff* immateriali a queste collegati (cfr. altresì V. PELLIGRA, *I paradossi della fiducia. Scelte razionali e dinamiche interpersonali*, il Mulino, Bologna, 2007), rispetto all'effettiva efficacia di orientamento dei comportamenti dei c.d. controlli esterni, specie formali (cfr. già W.C. RECKLESS, *The Etiology of Delinquent and Criminal Behavior: A Planning Report for Research*, Social Science Research Council, New York, 1943; ID., *The Crime Problem*, Goodyear, Pacific Palisades, 1973[5]).

[11] Cfr. COLEMAN, *Foundations*, cit., p. 405; J.A. LACHMAN, *Reputation and Risktaking*, in *The Cost of Libel. Economic and Policy Implications*, ed. by E.E. Dennis, E.M. Noam, Columbia University Press, New York, 1989, pp. 229-256.

[12] Esistono, infatti, «effetti di rete» tra reputazioni collettive e reputazioni individuali, per cui l'appartenere o l'entrare a far parte di gruppi (più o meno strutturati) che godano di 'buona' reputazione può migliorare la reputazione individuale, così come, per un gruppo, accogliere o includere membri con una reputazione 'danneggiata' può incidere negativamente su quella del gruppo stesso (cfr. per tutti G. ORIGGI, *La réputation*, PUF, Paris, 2015, trad. it., EGEA, Milano, 2016, p. 71).

partner (attuali e potenziali) dell'interazione[13], sia perché il titolare non ha affatto il monopolio sulla costruzione e sul mantenimento della propria reputazione, influenzati in modo decisivo, al contrario, dalla diffusione di informazioni operata da altri[14].

Così «tutte le nostre interazioni sociali lasciano negli altri una traccia informativa […] al tempo stesso indelebile e fragile […] che non può più essere cancellata» e le «mediazioni differenti di ciò che chiamiamo informazione sociale creano distorsioni ed effetti di amplificazione»[15] sulla reputazione oltremodo complessi. Una complessità legata, in particolare, all'estrema varietà dei contesti in cui tali 'tracce informative' si generano, che «vanno dall'interazione faccia a faccia ai pettegolezzi diffusi in assenza dell'interessato, alla stampa e a Internet»[16]. Resta fermo, però, che è proprio la circolazione di informazioni e giudizi sul soggetto (individuo o entità collettiva) ciò che rende possibile considerarlo portatore di una «identità intertemporale», la quale a sua volta è ciò che consente agli altri partner dell'interazione sociale di valutare e decidere se e come entrare con questi in relazione[17], così appunto determinando una serie di benefici (o di svantaggi, in caso di 'cattiva fama') per il singolo titolare di reputazione[18].

A complicare il quadro, la circolazione di informazioni rilevanti risulta, costitutivamente, *imperfetta*: informazioni 'screditanti' possono non arrivare mai alla conoscenza dei partner, attuali o potenziali, interessati (anche per gli sforzi attivi, in tal senso, del titolare del 'capitale reputazionale')[19], così come, per altro verso, queste possono essere messe in circolazione, anche ove completamente infondate, da terzi (consapevoli o meno della loro falsità, intenzionalmente oppure per disattenzione o superficialità),

[13] In questo senso cfr. anche C. PEDRAZZI, *L'exceptio veritatis. Dogmatica ed esegesi*, in «Rivista italiana di diritto penale» (1947), p. 433.

[14] Cfr. LACHMAN, *Reputation and Risktaking*, cit., pp. 230-233.

[15] Cfr. ORIGGI, *La réputation*, cit., p. 9.

[16] *Ibidem*.

[17] Cfr. PIZZORNO, *Il velo della diversità*, cit., p. 224.

[18] In realtà, si può constatare come tutti godano di una sorta di 'credito minimo di base', in termini reputazionali, in assenza di segnali informativi di segno opposto (nello stesso senso cfr. anche K. AMELUNG, *Die Ehre als Kommunikationsvoraussetzung. Studien zum Wirklichkeitsbezug des Ehrbegriffs und seiner Bedeutung im Strafrecht*, BWV, Baden Baden, 2002), tanto maggiore quanto più alto è il livello di fiducia sociale e reciprocità generalizzata nel rispetto delle regole (cfr. PUTNAM, *Bowling Alone*, cit., pp. 168-169). Tuttavia, questa 'dote reputazionale' di partenza (che tende comunque a essere influenzata da fattori esogeni 'etichettanti', come classe sociale, qualifica professionale, genere, gruppo etnico o colore della pelle, ecc., il cui influsso sarà più o meno importante a seconda del contesto socioculturale di riferimento) è soggetta a mantenersi, incrementarsi o diminuire in base alle condotte del soggetto o, meglio, alla circolazione di informazioni (corrette o scorrette) a queste relative, data la già richiamata natura *dinamica* del 'bene' reputazione.

[19] «Le persone 'vendono' sé stesse come vendono merci. Professano alti standard di comportamento per indurre altri a impegnarsi in interazioni sociali o economiche con loro, dalle quali ricavano vantaggi, ma allo stesso tempo nascondono alcuni fatti che questi partner nell'interazione troverebbero utili per formarsi un ritratto compiuto della loro personalità. […] Le persone desiderano manipolare il mondo intorno a loro attraverso la rivelazione selettiva di fatti che le riguardano». Cfr. R.A. POSNER, *The Right of Privacy*, in «Georgia Law Review», 12/3 (1978), pp. 399-401 (trad. nostra). In tema, nell'ambito della psicologia sociale resta fondamentale il riferimento a E. GOFFMAN, *The Presentation of Self in Everyday Life*, Doubleday, Garden City NY, 1959 (trad. it., il Mulino, Bologna, 1969), in part. pp. 239-272.

senza che il soggetto 'danneggiato' possa impedirlo (discorso che vale, per altro, anche per informazioni 'accreditanti' false). Anche il livello di diffusività della circolazione delle informazioni di rilievo reputazionale è assai spesso sottratto, in misura rilevante o del tutto, al controllo del soggetto affetto (e però spesso anche al controllo degli altri 'comunicanti')[20].

Si comprende allora come la 'quarta rivoluzione' digitale non possa che avere, sulle problematiche relative a costituzione e gestione della reputazione, un impatto dirompente, legato non solo all'enorme accelerazione delle comunicazioni, alla drammatica espansione della platea di comunicanti e riceventi coinvolti in ogni singola interazione, e alla tendenziale permanenza del dato informativo rilasciato, che sono propri delle nuove ICT (*Information & Communication Technologies*), ma, più radicalmente, al mutamento *antropologico* che esse stanno determinando. Come osserva sempre Floridi, infatti, ormai «il mondo digitale online trabocca nel mondo analogico offline, con il quale si sta mescolando», tanto da poter affermare che già oggi (e sempre più in futuro) «in misura crescente conduciamo le nostre vite *onlife*»[21]. In questo contesto, quella di chi scrive è

> probabilmente l'ultima generazione a fare esperienza della chiara distinzione tra ambienti online e offline. […] Deleghiamo o esternalizziamo in misura crescente ad agenti digitali ricordi, decisioni, compiti di routine e altre attività con modalità che sono sempre più integrate con le nostre vite. […] La quarta rivoluzione concerne, in negativo, la nostra "unicità" appena perduta (non siamo più al centro dell'infosfera) e, in positivo, il nostro nuovo modo di comprendere noi stessi in quanto inforg. […] Le nostre ICT sono, di regola, più in gamba di noi e più capaci di svolgere funzioni in modo efficiente. […] E, proprio in conseguenza di questo, stanno modificando o creando l'ambiente in cui viviamo. Abbiamo iniziato a concepire noi stessi come inforg, non attraverso qualche trasformazione biotecnologica del nostro corpo, ma, più seriamente e realisticamente, attraverso la radicale trasformazione del nostro ambiente e degli agenti che vi operano. […] La quarta rivoluzione ha portato alla luce la natura intrinsecamente informazionale dell'identità umana. […] Nel lungo periodo, inforg *disindividualizzati* (siamo "un genere di") e *reidentificati* (siamo concepiti come lo specifico punto d'incontro di molti "generi di") possono essere trattati come beni da vendere e acquistare sul mercato della pubblicità. Possiamo diventare come le *anime morte* di Gogol', ma dotati di portafoglio. […] Non c'è una borsa valori per tali anime morte online, ma tanti Čičikov (il personaggio principale del racconto di Gogol') che vogliono acquistarle. […] Possiamo costruire, personalizzare e riappropriarci di noi stessi nell'infosfera per mezzo di blog, post su Facebook, pagine di Google, video su YouTube, album su Flickr, condividendo le nostre preferenze […] Usiamo e pubblichiamo informazioni che ci riguardano per diventare meno anonimi e irriconoscibili dal punto di vista informazionale [e al tempo stesso] vogliamo conservare un alto livello di privacy

[20] Cfr. ancora Origgi, *La réputation*, cit., in part. pp. 44-112.

[21] Cfr. Floridi, *The Fourth Revolution*, cit., p. 47. Cfr. altresì Id. (ed.), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, Cham-London, 2015.

> informazionale come se fosse l'unico modo di salvaguardare un prezioso capitale da investire in seguito pubblicamente (i pessimisti direbbero, da sperperare), per costruire la nostra immagine di individui facilmente riconoscibili e re-identificabili nella loro unicità. Mai nel passato la privacy informazionale ha avuto un ruolo così cruciale nella vita di milioni di persone[22].

Per questo l'attuale «società dell'informazione» è stata definita anche una «società della trasparenza», in cui gli individui, attraverso le onnipresenti ICT, «si espongono a partire da un bisogno interiore, senza alcuna costrizione esterna. *Producono sé stessi*, vale a dire: inscenano sé stessi», «bramano» la «luce dei riflettori» ormai a portata di un clic sull'onnipresente smartphone[23]. Questo contribuisce a dar vita a una «società della prestazione (*Leistungsgesellschaft*)» i cui cittadini non sono «"soggetti d'obbedienza" ma "soggetti di prestazione" (*Leistungssubjekte*)», ossia «imprenditori di se stessi. […] Il verbo modale positivo, proprio della società della prestazione, è il "poter-fare" (*Können*) illimitato». Il 'prezzo' di tale trasformazione antropologica è, per altro, anche la genesi di «soggetti depressi e frustrati»[24] dalla costante pressione a 'produrre sé stessi' e 'inscenare sé stessi' esercitata dal nuovo ecosistema digitale, in cui, tuttavia (e proprio a causa della sua struttura), «autenticamente liberi non sono gli esseri umani, ma le informazioni»[25]. Il nuovo «dispositivo indisciplinare», che «genera euforia» e «sigilla gli individui in una dimensione aporetica»[26], è funzionale a una massiva 'messa a reddito' della sempre più imponente (sul piano quantitativo, per quanto in genere sempre più scadente, sul piano qualitativo) 'produzione' informativo-comunicativa di ciascun individuo. Sempre più spesso

> un numero sempre più elevato di persone trascorre una quantità crescente di tempo a diffondere notizie sul proprio conto, interagendo digitalmente con altre persone […], entro un'infosfera che non è né interamente virtuale né soltanto fisica. […] Le ICT sono diventate […] [le] più potenti *tecnologie del sé* alle quali siamo mai stati esposti. […] Dovremmo gestirle con attenzione, poiché stanno modificando in maniera significativa i contesti e le pratiche attraverso le quali diamo forma a noi stessi. […] Il sé sociale è il principale canale attraverso cui le ICT, e in particolar modo i social media interattivi, esercitano il loro profondo impatto sulle nostre identità personali. Se cambiamo le condizioni sociali in cui viviamo, mutiamo la rete di relazioni e il flusso di informazioni di cui godiamo e ridisegnamo natura e novero dei limiti e delle possibilità che regolano come ci presentiamo al mondo e indirettamente a noi stessi, allora il nostro sé sociale può essere radicalmente aggiornato, avendo una ricaduta sulla concezione che abbiamo di noi, che

[22] Cfr. Floridi, *The Fourth Revolution*, cit., pp. 107-114.

[23] Cfr. B.-C. Han, *Infokratie*, cit., p. 8.

[24] Cfr. B.-C. Han, *Müdigkeitsgesellschaft - Burnoutgesellschaft - Hoch-Zeit*, Matthes & Seitz, Berlin, 2010; 2016 (trad. it., Nottetempo, Milano, 2020), pp. 23-24.

[25] Cfr. Han, *Infokratie*, cit., p. 8.

[26] Cfr. G. Bottiroli, *Non sorvegliati e impuniti. Sulla funzione sociale dell'indisciplina*, in *Forme contemporanee del totalitarismo*, a cura di M. Recalcati, Bollati Boringhieri, Torino, 2007, pp. 137-140.

> finisce per conformare la nostra identità personale. […] L'intero fenomeno della costruzione dell'identità personale online […] è una questione concreta e urgente per un numero crescente di persone che trascorre ormai tutta la propria vita adulta su Facebook, Gloogle+, LinkedIn, Twitter, blog, YouTube, Flickr e così via[27].

Si è così creato un contesto comunicativo molto diverso dal passato, in cui erano più agevoli forme di 'segregazione' delle diverse espressioni del sé sociale e, quindi, delle differenti sfere reputazionali (professionale, familiare-amicale, politica, ecc.)[28]: oggi «viviamo in una singola infosfera, che non possiede alcun "fuori", e dove diventa più difficile distinguere le relazioni intra-comunitarie da quelle inter-comunitarie»[29], come pure contenere e circoscrivere gli effetti dannosi di comunicazioni (*lato sensu* diffamatorie) relative a una sfera della propria personalità sociale. E se è vero che le nuove ICT hanno aperto anche nuovi spazi di controllo sui propri dati e sulla propria reputazione – «per esempio, società di gestione della reputazione che monitorano e arricchiscono le informazioni concernenti un individuo o un marchio online stanno crescendo come funghi»[30] – è anche vero che questo tipo di 'management reputazionale'[31] richiede risorse e investimenti (in termini non solo economici, ma anche di competenze digitali e di psicologia sociale) ben lontane da quelle dell'utente medio di Internet.

A fronte di questo sconvolgimento epocale, prevenzione e repressione *penali* delle offese alla reputazione restano affidate a un microsistema di fattispecie sanzionatorie[32] – costituito, oggi, in tema di diffamazione, dagli artt. 595-599 c.p. e, fino alla

[27] Cfr. FLORIDI, *The Fourth Revolution*, cit., pp. 67-69. «È la generazione iperconsapevole di sé, che condivide attraverso social network e instant-messaging visioni e gusti personali, dettagli privati e persino esperienze intime, in una sorta di flusso continuo».

[28] È infatti un dato di realtà empirico-sociologica che per ciascuno possano coesistere – e di fatto generalmente coesistano – varie reputazioni 'settoriali', differenziate in ragione delle diverse «cerchie di riconoscimento» (PIZZORNO, *Il velo della diversità*, cit., p. 234) nelle quali ci si trova a interagire, sia perché le diverse cerchie possono presentare aspettative normative differenziate (cfr. anche G. SIMMEL, *Soziologie. Untersuchungen über die Formen der Vergesellschaftung*, Dunker & Humblot, Leipzig, 1908, trad. it., Edizioni di Comunità, Torino, 1989, pp. 460 ss.), sia perché la stessa persona può presentare una diversa attitudine a corrispondere alle aspettative di cerchie differenti (PIZZORNO, *Il velo*, cit., p. 235), di modo che la sua inadeguatezza rispetto agli standard dell'una può essere controbilanciata, in tutto o in parte, dalla sua abilità nel soddisfare le aspettative di cerchie diverse. Da questo punto di vista, la più risalente concezione 'fattuale' dell'onore continua indubbiamente a cogliere nel segno: cfr. in part. E. FLORIAN, *Ingiuria e diffamazione. Sistema dei delitti contro l'onore secondo il Codice penale italiano*, SEL, Milano, 1939, in part. pp. 99 ss.; v. anche *supra*, nota 7.

[29] Cfr. FLORIDI, *The Fourth Revolution*, cit., p. 126.

[30] Cfr. FLORIDI, *The Fourth Revolution*, cit., pp. 129-130.

[31] Ormai da tempo 'scienza' a sé: cfr. ad es. D.L. DEEPHOUSE, *Media Reputation as a Strategic Resource: An Integration of Mass Communication and Resource-Based Theories*, in «Journal of Management», 26/6 (2000), pp. 1091-1112; J. RAYNER, *Managing Reputational Risk: Curbing Threats, Leveraging Opportunities*, Wiley, Chichester, 2003; V.P. RINDOVA, I.O. WILLIAMSON, A.P. PETKOVA, J.M. SEVER, *Being Good or Being Known: An Empirical Examination of the Dimensions, Antecedents and Consequences of Organizational Reputation*, in «Academy of Management Journal», 48/6 (2005), pp. 1033-1049; S.V. SCOTT, G. WALSHAM, *Reconceptualizing and Managing Reputation Risk in the Knowledge Economy: Toward Reputable Action*, in «Organization Science», 16/3 (2005), pp. 308-322.

[32] In merito al quale si rinvia, per maggiori dettagli e ulteriori riferimenti bibliografici, ai testi citati *supra*, nota 2.

dichiarazione di illegittimità costituzionale pronunciata nel 2021, dall'art. 13 l. 8 febbraio 1948, n. 47 e dall'art. 30, co. 4 della l. 6 agosto 1990, n. 223[33] (cui si affiancano, in tema di responsabilità del direttore di testata giornalistica, gli artt. 57-58 c.p.), e in tema di ingiuria dall'art. 4 co. 1 e 4 del d.lgs. 15 gennaio 2016, n. 7 (il quale, come è noto, ha abrogato gli artt. 594 e 599 co. 1 e 3 c.p.) – che affonda le sue radici in un modello sociale e comunicativo lontanissimo dall'attuale.

Il legislatore del 1930 si dimostra, infatti, pesantemente condizionato da una concezione ancora 'cetuale' o 'castuale' dei beni tutelati[34] (debitrice a modelli profondamente premoderni di 'società d'onore')[35], nell'orizzonte di una prevalente comunicazione-intra-comunitaria, al più potenziata dai tradizionali media analogici. Un aspetto, questo, segnalato anche dalla scelta legislativa del criterio discretivo tra le due fattispecie, ossia presenza (ingiuria, fattispecie meno grave) o assenza (diffamazione, fattispecie più severamente punita) della persona offesa al momento dell'esternazione: un criterio improntato alla presunzione di una minore lesività della condotta ove l'individuo colpito

[33] Con la sentenza n. 150 del 12 luglio 2021 la Corte Costituzionale ha infatti dichiarato l'illegittimità, per violazione dell'art. 21 Cost., nonché dell'art. 117, co. 1 Cost. in relazione all'art. 10 Convenzione EDU, dell'art. 13 l. n. 47/1948, in quanto la previsione, non già alternativa (come nell'art. 595, co. 3 c.p.), bensì cumulativa, di pena pecuniaria e pena detentiva per l'aggravante integrata dalla condotta di diffamazione a mezzo stampa consistente nell'attribuzione di un fatto determinato, comportando (in assenza di attenuanti ritenute equivalenti o prevalenti) «l'indefettibilità dell'applicazione della pena detentiva», rendeva tale disposizione «incompatibile con il diritto a manifestare il proprio pensiero». Infatti, «la necessaria irrogazione della sanzione detentiva (indipendentemente poi dalla possibilità di una sua sospensione condizionale, o di una sua sostituzione con misure alternative alla detenzione rispetto al singolo condannato)», replicata ed estesa alla diffamazione radiotelevisiva dal citato art. 30, co. 4 l. n. 223/1990, è divenuta «ormai incompatibile con l'esigenza di non dissuadere, per effetto del timore della sanzione privativa della libertà personale, la generalità dei giornalisti dall'esercitare la propria cruciale funzione di controllo sull'operato dei pubblici poteri». Come è noto, la pronuncia della Consulta si inserisce nel solco delle precedenti decisioni della Corte EDU nei casi *Belpietro c. Italia* (sez. II, 24 settembre 2013, ric.n. 43612/10) e *Sallusti c. Italia* (sez. I, 7 marzo 2019, ric.n. 22350/13). A commento cfr. rispettivamente, *ex plurimis*, F. Viganò, *Belpietro c. Italia: una pronuncia della Corte di Strasburgo in tema di (s)proporzione della sanzione detentiva inflitta a un giornalista*, in «Quaderni costituzionali», 1 (2014), pp. 177-181; U. Zingales, *Il "caso Belpietro" e la ricerca del giusto bilanciamento tra la libertà di espressione e il diritto alla reputazione*, in «Critica del diritto», 2 (2013), pp. 231-245; S. Lonati, *Diffamazione a mezzo stampa e applicazione della pena detentiva: ancora qualche riflessione a margine del c.d. caso Sallusti in (perenne) attesa di un intervento del legislatore*, in «MediaLaws», 1 (2020), pp. 69-83; A. Salerno, *Diffamazione aggravata a mezzo stampa: profili di incostituzionalità dell'aggravante ex art. 13 della l. 8 febbraio 1948 n. 47 per violazione della Convenzione Europea dei Diritti dell'Uomo*, in «Critica del diritto», 2 (2019), pp. 50-73; G. Corrias Lucente, *Il difficile percorso della Corte Costituzionale nella limitazione delle sanzioni penali per la diffamazione tra prescrizioni della Corte di Strasburgo e bilanciamento di valori costituzionali*, in «Il diritto dell'informazione e dell'informatica», 3 (2021), pp. 480-485; A. Napolitano, *Il difficile bilanciamento tra libertà di informazione professionale e tutela della reputazione della persona. Riflessioni sulla dichiarazione di incostituzionalità della pena detentiva nei confronti dei giornalisti*, in «MediaLaws», 1 (2022), pp. 272-290.

[34] Sull'inestricabile compenetrazione del concetto stesso di 'onore' (diversamente da quanto possibile, invece, per quello di reputazione) con codici valoriali legati a un modello sociale rigidamente diviso in gruppi tra loro gerarchizzati occorre qui rinviare, per esigenze di sintesi, a Visconti, *Reputazione, dignità, onore*, cit., in part. pp. 155-354 e 505 ss.

[35] Cfr. per tutti K.A. Appiah, *The Honor Code: How Moral Revolutions Happen*, Norton & Company, New York, 2010 (trad. it., Cortina, Milano, 2011).

abbia la materiale possibilità di una reazione 'difensiva' immediata[36]. Per non parlare poi della colorazione autoritaria alla radice della scelta originaria di tutelare la reputazione esclusivamente nel suo aspetto formale[37], ossia a prescindere dal suo fondamento di verità o meno[38].

Scelta, quest'ultima, che, paradossalmente, deve la sua salvezza, nel successivo contesto democratico, all'evoluzione personalistica e costituzionalmente orientata dell'interpretazione dei beni dell'onore e della reputazione, oggi sostanzialmente ancorati, come è noto[39], al valore della dignità umana (art. 3 Cost.), da proteggere – in linea di massima e salvo ovvie esigenze di bilanciamento con diritti fondamentali quali, *in*

[36] Cfr. *Lavori preparatori del codice penale e del codice di procedura penale*. *Relazione del Guardasigilli*, vol. V, Tipografia delle Mantellate, Roma, 1929, p. 403: «Manifesta è la maggiore gravità obbiettiva del delitto di diffamazione, il quale produce alla persona offesa un più sensibile danno capace dei più ampi riverberi. Sotto altro riflesso è ancora evidente che la divulgazione delle offese rappresenta, solitamente, una manifestazione criminosa assai più malvagia, poiché esclude la possibilità di immediata reazione o di difesa del leso, il quale, se presente, potrebbe invece ritorcere le offese e contestarne la consistenza. Quest'ultima considerazione giustifica la disposizione [che] conserva il carattere di ingiuria, sebbene aggravata, all'offesa commessa in presenza del danneggiato e, insieme, di altre persone. Infatti, anche in tal caso la presenza dell'offeso, consentendo a costui di difendersi, attenua la influenza nociva, che le offese possono spiegare sull'opinione che le persone presenti abbiano del suo valore morale».

[37] Cfr. *Relazione del Guardasigilli*, cit., pp. 404-405: «Il problema [consisteva] nell'insanabile contrasto tra la mentalità liberale e democratica, che propugnava un illimitato diritto di censura, ed i principi, rigidi e semplici, dell'etica fascista, la quale, imponendo una revisione di tutti i valori, ha tenuto ad affermare la sicura e netta prevalenza di quelli sociali, primo fra tutti il rispetto e l'ossequio per l'Autorità, in rapporto con la disciplinata subordinazione dei diritti o interessi individuali. Partendo da tali principi politici ed etici […], la prova della verità per volontà consensuale delle parti è un assurdo logico e morale […]. Non può, invero, esser consentito a singoli individui distrarre l'Autorità giudiziaria dai suoi compiti essenziali, per farne il comodo arbitro delle proprie questioni morali. […] Consent[ire] un diritto privato di censura sull'attività dei pubblici ufficiali, è in manifesto contrasto con il sistema sociale e politico del Fascismo. Il prestigio dell'Autorità deve essere tutelato con il più inflessibile ed oculato rigore. […] Il Progetto, quindi, non riconosce agli individui un diritto di censura, né tanto meno di divulgazione di fatti attinenti all'altrui vita morale».

[38] Tra gli Autori che individuano due beni distinti (o, se si vuole, due estensioni distinte dello stesso bene), rispettivamente, nelle ipotesi di ammissibilità dell'*exceptio veritatis* (tutela riservata all'onore reale, o sostanziale che dir si voglia) e al di fuori del raggio applicativo della stessa (tutela estesa all'onore formale, o apparente) si vedano E. GAITO, *La verità dell'addebito nei delitti contro l'onore*, Giuffrè, Milano, 1966, in part. pp. 129-136; R. PANNAIN, *La natura giuridica dell'"exceptio veritatis" in un recente studio di Aldo Moro*, in «Archivio penale» (1955), in part. pp. 21-22; SPASARI, *Sintesi*, cit., in part. pp. 15-32; condividono la distinzione tra onore reale – tutelato nelle ipotesi di *exceptio veritatis* – e onore formale, pur non inquadrando le previsioni dell'art. 596 co. 3 c.p. come autonome fattispecie di reato, A. MORO, *Osservazioni sulla natura giuridica della "exceptio veritatis"*, in «Rivista italiana di diritto penale» (1954), in part. pp. 13 ss., e G. VASSALLI, *Cause di non punibilità*, in «Enciclopedia del diritto», VI, Giuffrè, Milano, 1960, p. 634; utilizza tale distinzione lo stesso FLORIAN, *Ingiuria e diffamazione*, cit., pp. 33 ss. e 423 ss., secondo il quale, anzi, l'onore 'propriamente inteso' coinciderebbe col solo onore reale, ossia corrispondente ai fatti. In giurisprudenza, fondamentale il riferimento a C. Cost. 5 luglio 1973, n. 103 (v. anche *infra*). Per una discussione più analitica del punto, e ulteriori riferimenti, ci si permette di rinviare, per esigenze di sintesi, a VISCONTI, *Reputazione, dignità, onore*, cit., pp. 580-597.

[39] Per approfondimenti e ulteriori riferimenti si vedano, ancora, i testi e gli Autori citati *supra*, note 2 e 7, nonché, da ultimo, la già richiamata (v. nota 33) sentenza C. Cost. n. 150/2021: «se è vero che la libertà di espressione – in particolare sub specie di diritto di cronaca e di critica esercitato dai giornalisti – costituisce pietra angolare di ogni ordinamento democratico, non è men vero che la reputazione individuale è del pari un diritto inviolabile, strettamente legato alla stessa dignità della persona».

primis, quello alla libera manifestazione del pensiero (art. 21 Cost.)[40] – contro ogni forma di mancanza di rispetto[41].

Proprio questo 'sfilacciamento' dei confini della reputazione, a tutto vantaggio di una sua sostanziale sovrapposizione al concetto, assai più vago e inafferrabile, di dignità[42], è ciò che ha, per altro, consentito di applicare la fattispecie di diffamazione anche alla divulgazione di fatti perfettamente veri, ma attinenti alla vita privata della persona (con una chiara sovrapposizione con la diversa sfera della riservatezza)[43] e addirittura

[40] Cfr. ancora, per tutti, C. Cost. n. 150/2021: «Aggressioni illegittime [al diritto alla reputazione] compiute attraverso la stampa, o attraverso gli altri mezzi di pubblicità cui si riferisce l'art. 595, terzo comma, cod. pen. – la radio, la televisione, le testate giornalistiche online e gli altri siti internet, i social media, e così via –, possono incidere grandemente sulla vita privata, familiare, sociale, professionale, politica delle vittime. E tali danni sono suscettibili, oggi, di essere enormemente amplificati proprio dai moderni mezzi di comunicazione, che rendono agevolmente reperibili per chiunque, anche a distanza di molti anni, tutti gli addebiti diffamatori associati al nome della vittima. Questi pregiudizi debbono essere prevenuti dall'ordinamento con strumenti idonei, necessari e proporzionati, nel quadro di un indispensabile bilanciamento con le contrapposte esigenze di tutela della libertà di manifestazione del pensiero, e del diritto di cronaca e di critica in particolare».

[41] Emblematica resta, in tal senso, la posizione di C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, Milano, 1958, secondo il quale la proclamazione della 'pari dignità sociale' di tutti i cittadini all'art. 3 Cost. «pretende […], precisamente, che la società e ciascun membro di essa *non si elevi mai, in buona o mala fede, a giudice della altrui indegnità* e che non esprima con gli atti o con le parole, direttamente o attraverso il riferimento di determinati fatti ritenuti spregevoli, valutazioni negative sulle persone; e che al giudizio qualificato delle autorità non si aggiungano quindi espressioni del giudizio non qualificato della società, ed alle espressioni di condanna di quelle, nuove espressioni di condanna di questa. In base a questi principi accolti dalla nostra Costituzione, e non alla generica affermazione della democraticità dello Stato od a preconcette seppure diffuse teorie», tra cui l'Autore annovera «quella […] che sia decisivo il criterio della "utilità sociale delle critiche"», «dovrebbe perciò esaminarsi oggi il problema della estensione e dei limiti del diritto di cronaca e di critica degli innocenti, dei presuntivamente innocenti e dei legalmente condannati, e degli uomini privati e degli uomini pubblici (che in verità non costituiscono, come oggi si ritiene, due diverse categorie di uomini diversamente tutelati nella dignità e nell'onore). *Si dovrebbero rettificare perciò alla luce delle norme costituzionali le ricostruzioni delle norme vigenti ed a volta le stesse disposizioni di legge ordinaria come quelle relative alla eccezione della verità* ed alla falsità dei fatti», in relazione alla quale l'Autore osserva come la disciplina introdotta dal legislatore del 1930 risultasse «più rispondente al principio sancito dall'art. 3 della Cost.» rispetto a quella determinatasi a seguito della reintroduzione dell'*exceptio veritatis* nel 1944: «[l]a verità dei fatti, invero, non dovrebbe avere rilievo ai fini della condanna di *manifestazioni contrarie alla dignità sociale delle persone, sempre vietate, vere o false che siano*». In base a questo approccio, dunque, l'art. 3 Cost. «viet[erebbe] categoricamente ai singoli come semplici membri della società (e cioè in quanto non siano rivestiti di alcuna autorità, pubblica o privata, generale o particolare, istituzionale o accidentale) di esprimere giudizi di indegnità sugli altri uomini. Né è divietato al singolo di esprimere giudizi lesivi dell'altrui onore per le conseguenze che essi possano avere per l'estimazione dei colpiti presso gli altri membri della società (ché se così fosse dovrebbero essere interdette anche le condanne legali dell'autorità), ma […] è vietato in modo immediato e diretto, indipendentemente dalle conseguenze eventuali e riflesse (sugli altri membri della società e sul colpito), alla società e ad ogni membro come socio, di esprimere tali giudizi di indegnità (presente o meno l'offeso, presenti o meno terzi oltre l'offeso). Appunto perché *la Costituzione divieta in maniera diretta e specifica all'art. 3 giudizi sociali di indegnità* (e la pari dignità non è solo un ideale o un fine da raggiungere) quell'articolo esprime un limite alla libertà di manifestazione di giudizio e pensiero garantita generalmente dall'art. 21» (ivi, pp. 44-50, corsivi nostri), limite qui evidentemente inteso come assoluto, coerentemente, del resto, con una completa sovrapposizione tra onore/reputazione e dignità.

[42] Per una critica meglio argomentata a tale confusione e sovrapposizione concettuale è qui necessario rinviare, per motivi di sintesi, a Visconti, *Reputazione, dignità, onore*, cit., pp. 505 ss.

[43] Per la distinzione logico-concettuale tra reputazione e riservatezza (entrambe riconducibili alla sfera dei diritti della personalità, ma chiaramente distinguibili tra loro) si rinvia ai contributi dedicati alla tutela di quest'ultima

a quella di fatti veri e già noti al pubblico, ma ormai lontani nel tempo[44], a tutela di quell'ibrido di reputazione, riservatezza e identità personale (attuale) che viene definito come 'diritto all'oblio'[45].

2. (Segue) *Nuove ICT e repressione penale delle offese all'onore e alla reputazione. Sintesi del quadro giurisprudenziale*

Proprio questa tutt'altro che chiara e razionale costruzione delle fattispecie di ingiuria e diffamazione[46], sul piano sia delle oggettività giuridiche tutelate, sia della stessa strutturazione degli illeciti in parola, sono, d'altro canto, ciò che ha consentito alla giurisprudenza di 'incorporare' fluidamente nel loro raggio applicativo condotte lesive inedite, inimmaginabili negli anni Trenta del secolo scorso, man mano che nuove tecnologie della comunicazione si presentavano sulla scena[47].

nel presente volume, nonché a molti degli Autori citati *supra* (in part. nota 7). Qui basti rilevare che la riservatezza, accomunata alla reputazione e distinta dal nome o dall'immagine per essere non già un *quid* oggettivo (i.e. un segno distintivo della persona immediatamente individuabile), bensì una relazione, una situazione del soggetto davanti alla sua comunità, dall'onore/reputazione tuttavia si distingue per la mancanza di qualsiasi carattere (anche solo potenzialmente) valutativo attinente a tale rapporto. La riservatezza, di per sé, riguarda, infatti, semplicemente un complesso di situazioni personali non destinate alla conoscenza altrui, quale che sia la loro eventuale potenzialità lesiva – ove divulgate – nei confronti dell'onorabilità del soggetto. Efficacemente, in questo senso, essa è stata sinteticamente definita uno «*ius excludendi alios* dalla intrusione nella propria sfera privata» (Pret. Roma, 11 gennaio 1989, in «Diritto dell'informazione e dell'informatica», 2 (1989), p. 498, con nota di G. Leo, *Diritto di cronaca e riservatezza nelle trasmissioni televisive di "informazione-spettacolo"*, pp. 503-512). Nella giurisprudenza in tema di diffamazione e diritto di cronaca è evidente come lo stesso sviluppo del parametro di legittimità della 'pertinenza' (su cui v. anche *infra*) sia strettamente legato all'aver accomunato, nell'oggetto della tutela della fattispecie di cui all'art. 595 c.p., reputazione e riservatezza (cfr. ad es., *ex multis*, Cass. pen., VI, 26 giugno 1979, n. 5636; Cass. pen., V, 6 febbraio 1998, n. 1473; Cass. pen., V, 12 marzo 2002, n. 10135; Cass. pen., V, 20 giugno 2019, n. 27616).

[44] Cfr. ad es. Cass. pen., V, 24 novembre 2009, n. 45051, con note di A. Cerri, *Diritto di cronaca, diritto di revocare fatti passati versus diritto di riservatezza e diritto all'oblio*, in «Critica del diritto», 3-4 (2009), pp. 236-238; P. Palermo, *Diffamazione e diritto all'oblio: equilibrio "elastico" tra tutela penale dell'onore e diritto di cronaca giudiziaria*, in «Rivista penale», 3 (2010), pp. 277-286, e 5 (2010), pp. 526-535; S. Peron, *La verità della notizia tra attualità e oblio*, in «Responsabilità civile e previdenza», 5 (2010), pp. 1067-1073.

[45] Sul tema, alquanto complesso e articolato, non si può in questa sede che rinviare, *ex multis*, a T.A. Auletta, *Diritto alla riservatezza e "droit à l'oubli"*, in *L'informazione e i diritti della persona*, a cura di G. Alpa, M. Bessone, L. Boneschi, G. Cajazza, Jovene, Napoli, 1983, pp. 127-132; E. Gabrielli (a cura di), *Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997*, ESI, Napoli, 1999; M. Iaselli, *I fondamenti e l'evoluzione del diritto all'oblio*, in *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio*, a cura di G. Cassano, Wolters Kluwer, Assago, 2017, pp. 231-337; M. Mezzanotte, *Il diritto all'oblio. Contributo allo studio della privacy storica*, ESI, Napoli, 2009; G. Resta, V. Zeno Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma TrE-Press, Roma, 2015.

[46] Per un approfondimento rispetto alle critiche che sarà possibile sviluppare in questa sede ci si permette di rinviare a Visconti, *Reputazione, dignità, onore*, cit., pp. 317-395 e 505 ss., e ai riferimenti bibliografici ivi citati.

[47] Tra le pronunce 'fondative' cfr. in particolare Cass. pen., V, 27 dicembre 2000, n. 4741 (con nota di E. Perusia, *Giurisdizione italiana anche per le offese online su un sito straniero*, in «Cassazione penale», 6 (2001), pp. 1835-1840): «che i reati previsti dagli artt. 594 e 595 c.p. possano essere commessi anche per via telematica o informatica, è addirittura intuitivo; basterebbe pensare alla c.d. trasmissione via e-mail, per rendersi conto che è certamente possibile che un agente, inviando a più persone messaggi atti ad offendere un soggetto, realizzi la

Senza particolari problemi le offese recate tramite SMS[48] o e-mail[49] indirizzati alla persona offesa sono state, infatti, ricondotte alla fattispecie di ingiuria, mentre quelle recate tramite testate giornalistiche online, blog, forum, bacheche virtuali e simili – ivi inclusi i sempre più pervasivi *social network* – a quella di diffamazione, aggravata, rispettivamente, dal «mezzo della stampa», nel primo caso[50], o dall'uso di «qualsiasi altro mezzo di pubblicità», nei restanti[51].

condotta tipica del delitto di ingiuria (se il destinatario è lo stesso soggetto offeso) o di diffamazione (se i destinatari sono persone diverse). Se invece della comunicazione diretta, l'agente "immette" il messaggio "in rete", l'azione è, ovviamente, altrettanto idonea a ledere il bene giuridico dell'onore. Per quanto specificamente riguarda il reato di diffamazione, è infatti noto che esso si consuma anche se la comunicazione con più persone e/o la percezione da parte di costoro del messaggio non siano contemporanee (alla trasmissione) e contestuali (tra di loro), ben potendo i destinatari trovarsi persino a grande distanza gli uni dagli altri, ovvero dall'agente. Ma, mentre nel caso di diffamazione commessa, ad esempio, a mezzo posta, telegramma o, appunto, e-mail, è necessario che l'agente compili e spedisca una serie di messaggi a più destinatari, nel caso in cui egli crei o utilizzi uno spazio web, la comunicazione deve intendersi effettuata potenzialmente *erga omnes* (sia pure nel ristretto – ma non troppo – ambito di tutti coloro che abbiano gli strumenti, la capacità tecnica e, nel caso di siti a pagamento, la legittimazione, a connettersi). Partendo da tale – ovvia – premessa, si giunge agevolmente alla conclusione che, anzi, l'utilizzo di internet integra una delle ipotesi aggravate di cui dell'art. 595 c.p. (comma terzo: "offesa recata… con qualsiasi altro mezzo di pubblicità"). Anche in questo caso, infatti, con tutta evidenza, la particolare diffusività del mezzo usato per propagare il messaggio denigratorio rende l'agente meritevole di un più severo trattamento penale. Né la eventualità che tra i fruitori del messaggio vi sia anche la persona nei cui confronti vengono formulate le espressioni offensive può indurre a ritenere che, in realtà, venga, in tale maniera, integrato il delitto di ingiuria (magari aggravata ai sensi del quarto comma dell'art. 594 c.p.), piuttosto che quello di diffamazione. Infatti, il mezzo di trasmissione-comunicazione adoperato (appunto internet) certamente consente, in astratto, (anche) al soggetto vilipeso di percepire direttamente l'offesa, ma il messaggio è diretto ad una cerchia talmente vasta di fruitori, che l'addebito lesivo si colloca in una dimensione ben più ampia di quella interpersonale tra offensore ed offeso. D'altronde, anche per altri media si verifica la medesima situazione. Un'offesa propagata dai giornali o dalla radio-televisione è sicuramente percepibile anche dal diretto interessato, ma la fattispecie criminosa che, in tal modo, si realizza è, pacificamente, quella *ex* art. 595 c.p. e non quella *ex* art. 594. Peraltro, la diffusività e la pervasività di internet sono solo lontanamente paragonabili a quelle della stampa ovvero delle trasmissioni radio-televisive. Internet è, senza alcun dubbio, un mezzo di comunicazione più "democratico" (chiunque, con costi relativamente contenuti e con un apparato tecnologico modesto, può creare un proprio "sito", ovvero utilizzarne uno altrui). Le informazioni e le immagini immesse "in rete", relative a qualsiasi persona, sono fruibili (potenzialmente) in qualsiasi parte del mondo».

[48] Cfr. ad es. Cass. pen., I, 17 maggio 2005, n. 18449; Cass. pen., I, 29 maggio 2007, n. 21158; Cass. pen., V, 2 novembre 2015, n. 44145.

[49] Cfr. ad es. Cass. pen., V, 28 maggio 2009, n. 22421; si noti, tuttavia, che la diffusione a una *mailing list* di cui faccia parte *anche* la persona offesa è comunemente inquadrata nella fattispecie di diffamazione, essenzialmente in ragione della non contestualità del recepimento del messaggio nelle caselle di posta elettronica di destinazione (cfr. ad es. Cass. pen., V, 16 novembre 2012, n. 44980; Cass. pen., V, 8 aprile 2021, n. 13252). Per altro verso, la Suprema Corte ha anche precisato che l'invio di una e-mail dal contenuto diffamatorio a singole caselle di posta elettronica riservate non configura l'aggravante dell'uso di altro mezzo di pubblicità (su cui v. *infra*), in quanto tale condotta non comporta un'automatica diffusione a un numero indeterminato di soggetti, né sarebbe corretto confondere lo strumento informatico usato per trasmettere la comunicazione con la diffusività della stessa: cfr. Cass. pen., V, 18 luglio 2023, n. 31179.

[50] Cfr. ad es. Cass. pen., V, 17 aprile 2008, n. 16262; Cass. pen., V, 20 settembre 2019, n. 38896.

[51] Cfr. ad es. Cass. pen., I, 16 aprile 2014, n. 16712, con nota di S. Turchetti, *Diffamazione su Facebook: comunicazione con più persone e individuabilità della vittima*, in «Diritto penale contemporaneo», 8 maggio 2014 (online); Cass. pen., V, 1° febbraio 2017, n. 4873, annotata da E. Birritteri, *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*, in

Una distinzione, quest'ultima, che ha permesso alla prassi di estendere solo alle prime le specificità della disciplina della diffamazione a mezzo stampa. *In primis* – fino alla richiamata pronuncia della Consulta del 2021[52] – l'applicabilità, almeno in linea di principio, dell'aggravante di cui all'art. 13 l. n. 47/1948 (divulgazione a mezzo stampa di un fatto determinato)[53]. Del pari, solo alle testate giornalistiche online sono state dichiarate applicabili le disposizioni in materia di responsabilità del direttore per omesso impedimento del reato di diffamazione[54] e, per altro verso, solo a queste si applica la garanzia costituzionale di cui al co. 3 dell'art. 21 Cost. (divieto di sequestro fuori dai casi tassativamente previsti dalla legge)[55].

«Diritto penale contemporaneo», 4 (2017), pp. 286-289, e da F. Pisconti, *Diffamazione aggravata e "Facebook": la Cassazione si adegua alla (sua) svolta interpretativa*, in «Rivista penale», 2 (2018), pp. 173-175; Cass. pen., V, 14 aprile 2021, n. 13979. V. anche *supra*, nota 47.

[52] V. *supra*, nota 33.

[53] Cfr. Cass. V n. 4873/2017, cit., la quale evidenzia come l'offesa recata attraverso una bacheca Facebook, pur dotata di rilevante diffusività, non può essere equiparata all'offesa recata «a mezzo stampa», suscettibile di applicazione dell'aggravante prevista all'art. 13 l. n. 47/1948, dal momento che i *social network*, a differenza delle testate giornalistiche online, non svolgono un'attività di informazione professionale diretta al pubblico. La pronuncia richiama testualmente, sul punto, le precedenti Sezioni Unite Fazzo (v. *infra*, nota 55), le quali ritennero compatibile col principio di legalità lo scostamento da un'esegesi letterale del termine 'stampa' e l'attribuzione allo stesso di «un significato evolutivo […] coerente col progresso tecnologico e, nel contempo, non […] estraneo all'ordinamento positivo, considerato nel suo complesso e nell'assetto progressivamente raggiunto nel tempo», al tempo stesso precisando che «l'esito di tale operazione ermeneutica non può riguardare tutti in blocco i nuovi mezzi, informatici e telematici, di manifestazione del pensiero (*forum, blog, newsletter, newsgroup, mailing list, pagine Facebook*), a prescindere dalle caratteristiche specifiche di ciascuno di essi, ma deve rimanere circoscritto a quei soli casi che, per i profili strutturale e finalistico che li connotano, sono riconducibili […] nel concetto di "stampa" inteso in senso più ampio». Il che a sua volta si traduce appunto nella necessità di distingue nettamente tra «l'area dell'informazione di tipo professionale, veicolata per il tramite di una testata giornalistica *on line*, dal vasto ed eterogeneo ambito della diffusione di notizie ed informazioni da parte di singoli soggetti in modo spontaneo» tipico di blog, forum, social network e simili. In seguito, l'applicabilità dell'aggravante in parola è stata riconosciuta, in relazione a un caso di diffamazione a mezzo di testata giornalistica online, da Cass. pen., V, 11 gennaio 2019, n. 1275, commentata in modo sostanzialmente critico (in relazione al rischio di analogia *in malam partem*) da F. Cecchini, *La responsabilità del direttore di periodico telematico ex art. 57 c.p. tra divieto di analogia, "esigibilità" del controllo e prevedibilità dell'esito giudiziario*, in «Archivio penale web», 2 (2019), e R.E. Mauri, *Applicabile l'art. 57 c.p. al direttore del quotidiano online: un revirement giurisprudenziale della Cassazione, di problematica compatibilità con il divieto di analogia*, in «Diritto penale contemporaneo», 28 febbraio 2019 (online). Critico anche F.P. Lasalvia, *Diffamazione via web nell'epoca dei social network*, in *Cybercrime*, diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, UTET, Torino, 2023[2], in part. pp. 356 ss.

[54] Tra le pronunce che escludono la possibilità di chiamare a rispondere l'amministratore di un sito internet, blog, forum, e simili, *ex* art. 57 c.p. proprio in ragione della ritenuta applicabilità di tale disposizione alle sole testate giornalistiche telematiche (laddove la sussistenza di una responsabilità a titolo di concorso eventuale *ex* art. 110 c.p. richiede la prova della sussistenza, nel caso di specie, di tutti gli elementi, oggettivi e soggettivi, di tale partecipazione attiva, materiale o morale) cfr. ad es. Cass. pen., V, 16 aprile 2018, n. 16751, annotata da C. Pedullà, *L'amministratore di un sito Internet non è responsabile ai sensi dell'art. 57 c.p.*, in «Cassazione penale», 11 (2018), pp. 3744-3749, e Cass. pen., V, 24 febbraio 2021, n. 7220. La responsabilità *ex* art. 57 c.p., per omesso impedimento del reato di diffamazione a mezzo stampa, è stata invece riconosciuta in capo al direttore di una testata giornalistica online dalla citata Cass. V n. 1275/2019 (v. *supra*, nota 53).

[55] Cfr. Cass. pen., SU, 17 luglio 2015, n. 31022, la quale, pronunciandosi in tema di sequestro di giornali e altre pubblicazioni, ha ritenuto le testate giornalistiche telematiche funzionalmente assimilabili a quelle 'tradizio-

La costruzione legislativa delle fattispecie di ingiuria e diffamazione come reati a forma libera (si discute, poi, in dottrina, se connotati da un evento di danno o di pericolo, ma la questione è, come noto, sostanzialmente 'bypassata' dalla giurisprudenza, che, a scanso di difficoltà probatorie, si accontenta dell'accertamento di una generica idoneità offensiva delle condotte)[56] ha certamente contribuito alla facilità con cui le emergenti ICT – e più in generale tutte le condotte tenute utilizzando i nuovi strumenti digitali – sono state accolte e incorporate nella casistica giurisprudenziale. Così come, già in precedenza, tale assetto normativo aveva del resto permesso di includere modalità di aggressione non verbali (ingiurie commesse con gestacci o percosse dalla colorazione eminentemente umiliante, diffamazioni commesse tramite caricature e simili[57], ecc.), è oggi agevole 'coprire' i casi di diffusione di immagini o materiali audiovisivi digitali variamente 'diffamatori' attraverso i molteplici nuovi mezzi di comunicazione[58].

Non solo la giurisprudenza italiana non ha incontrato difficoltà a ricondurre tutte le esternazioni offensive attuate, in senso ampio, 'a mezzo Internet' (tramite siti web, blog, social media e simili) alla fattispecie di diffamazione, ma si è adeguata alle peculiarità di tale nuovo ecosistema digitale istituendo, contestualmente, una *presunzione* in base alla quale il mero inserimento del contenuto su piattaforme online, «per [loro] natura destinat[e] ad essere normalmente visitat[e] in tempi assai ravvicinati da un numero indeterminato di soggetti», fa scattare l'integrazione del requisito della comunicazione «con più persone» *ex* art. 595 c.p.[59].

Contestualmente, e specularmente, l'adattamento alle peculiarità delle nuove tecnologie ha generato anche l'*ulteriore presunzione* in base alla quale, in assenza di prova contraria fornita dalla persona offesa, l'istante della pubblicazione online del contenuto asseritamente lesivo segna anche il *dies a quo* per il decorrere del termine per la

nali' (in formato cartaceo) e, come tali, ricomprese nella nozione di «stampa» di cui all'art. 1 l. n. 47/1948, n. 47, dal che discende appunto l'impossibilità di sottoporre tali pubblicazioni online a sequestro preventivo, in caso di commissione del reato di diffamazione a mezzo stampa, in quanto prodotti editoriali sottoposti alla normativa, di rango costituzionale e di livello ordinario, che disciplina l'attività di informazione professionale diretta al pubblico. Viceversa (v. anche *supra*, nota 53), in tale ambito non rientrano altri mezzi di comunicazione digitali quali forum, blog, newsletter, newsgroup, mailing list, social media e simili, i quali dunque, malgrado la stretta relazione col diritto costituzionale di manifestazione del pensiero, non possono godere delle garanzie costituzionali relative al sequestro della stampa. L'interpretazione 'evolutiva' del concetto di 'stampa' adottata dalla Suprema Corte in questa occasione non è per altro andata esente da (ragionevoli) critiche in dottrina. Cfr., tra i numerosi commenti, G. Corrias Lucente, *Le testate telematiche registrate sono sottratte al sequestro preventivo. Qualche dubbio sulla "giurisprudenza legislativa"*, in «Il diritto dell'informazione e dell'informatica», 6 (2015), pp. 1041-1052; L. Diotallevi, *La Corte di cassazione sancisce l'"equiparazione" tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di "scivolamento" dalla "nomofilachia" alla "nomopoiesi"?*, in «Giurisprudenza costituzionale», 3 (2015), pp. 1062-1071; L. Paoloni, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa: ubi commoda, ibi et incommoda?*, in «Cassazione penale», 10 (2015), pp. 3454-3480.

[56] Sul punto si rinvia, per esigenze di sintesi, ai numerosi riferimenti dottrinali e giurisprudenziali riportati nei testi citati *supra*, note 2 e 7.

[57] Cfr. ad es. Cass. pen., VI, 20 aprile 1978, n. 4724; Cass. pen., V, 16 marzo 1992, n. 2885.

[58] Cfr. ad. es. Cass. pen., V, 27 luglio 2018, n. 36076, relativa alla diffusione online di fotomontaggi digitali.

[59] Cfr. Cass. V n. 16262/2008, cit., e in generale le pronunce richiamate *supra*, note 50 e 51.

proposizione della querela, coincidendo (asseritamente) con quello della conoscenza da parte della persona offesa dell'avvenuta diffusione del contenuto diffamatorio[60].

Un assunto indubbiamente legato (come pure la prima e speculare presunzione testé richiamata) a esigenze di semplificazione probatoria, che tuttavia offre un primo spunto di riflessione critica circa la reale effettività della tutela della reputazione da offese online garantita dal presente assetto normativo. Va notato, infatti, come tale presunzione di coincidenza tra pubblicazione e conoscenza da parte della persona offesa sembri non solo far proprio, ma addirittura *assolutizzare* – oltre ogni ragionevolezza – il ricordato mutamento antropologico da cittadino a 'inforg'[61] di ciascun consociato. L'individuo sembra, cioè, ricostruito concettualmente come una sorta di entità perpetuamente connessa e onnisciente, in grado di filtrare con fulminea tempestività ed esattezza la rete e le sue propaggini a caccia della minima menzione di sé. E mal gliene incolga, ove non sia sufficientemente abile a individuare tempestivamente le offese alla sua reputazione: la scure dell'improcedibilità calerà infatti su di lui, costringendolo a pagare il fio della propria 'inefficienza digitale'.

3. *Una duttilità solo apparente: problematiche applicative e vuoti di tutela*

Il gap tra presunzioni giurisprudenziali e realtà esperienziale degli utenti della rete appena richiamato è solo il primo tra gli esempi di come, a uno sguardo più attento, la confusa – e in ultimo fallace – attuale strutturazione delle fattispecie di ingiuria e diffamazione (ciascuna in sé, e nei loro reciproci rapporti) in sede di applicazione delle norme non sia solo fonte di duttilità (seppur a spese del principio di legalità[62], il che non può certo essere considerato poca cosa), ma si riveli, in realtà, anche radice di una serie di problemi e, in ultimo, significativi vuoti di tutela.

Per proseguire e approfondire l'analisi di tali deficit, occorre tornare alla distinzione – sopra solo rapidamente richiamata – tra le fattispecie di ingiuria e diffamazione. Come è noto, il legislatore del 1930 decise di modificare profondamente l'impianto dei delitti contro l'onore ereditato dal Codice Zanardelli[63], il quale imperniava la distinzione tra i due reati sulla determinatezza (diffamazione: art. 393) o meno (ingiuria: art. 395) del fatto attribuito alla persona offesa, riservando alla presenza dell'offeso, nell'ingiuria, un ruolo espansivo della punibilità (rendendo, cioè, la condotta penalmente rilevante anche in assenza di comunicazione con più persone, e istituendo dunque un'eccezione alla normale tutelabilità della sola reputazione) e di aggravamento

[60] Cfr. ad es. Cass. pen., V, 25 luglio 2006, n. 25875; Cass. pen., V, 14 giugno 2012, n. 23624; Cass. pen., V, 18 settembre 2015, n. 38099; Cass. pen., V, 9 giugno 2021, n. 22787.

[61] V. *supra*, nota 22.

[62] V. anche *supra*, note 53 e 55.

[63] In tema cfr. A. Marongiu, *Diffamazione e ingiuria (dir. intermedio)*, in «Enciclopedia del diritto», XII, Giuffrè, Milano, 1964, pp. 480-481; Spasari, *Diffamazione*, cit., p. 482.

sanzionatorio (sull'assunto che una 'provocazione' alla presenza dell'offeso potesse scatenarne *escalation* suscettibili di maggiore pericolosità complessiva). Viceversa, nel quadro normativo introdotto nel 1930, sul piano dell'oggettività giuridica il bene tutelato dall'ingiuria (dal 2016 illecito civile assistito da sanzione pecuniaria) è venuto identificandosi nel c.d. 'onore interno', ossia il sentimento della propria onorabilità o, se si vuole, della propria dignità personale, mentre oggetto di tutela nel delitto di diffamazione risulta prevalentemente il c.d. 'onore esterno', ossia l'immagine che gli altri hanno dell'onorabilità della persona, la sua reputazione[64]. Tale bipartizione troverebbe poi coerente rispecchiamento nella già richiamata differenza di costruzione delle fattispecie, con la presenza dell'offeso quale requisito di tipicità dell'ingiuria e, specularmente, la sua assenza, a fronte di una comunicazione del contenuto offensivo rivolta a più persone, quale necessario elemento strutturale della diffamazione.

A ben guardare, tuttavia, il legislatore non ha applicato tale partizione, concettuale e pratica, con rigore: all'ingiuria 'aggravata' (già *ex* art. 594 co. 4 c.p., e oggi più severamente sanzionata in sede civile) *ex* art. 4, co. 4, lett. f) d.lgs. n. 7/2026, infatti, e non già alla diffamazione, sono ricondotti i casi in cui la persona, presente, sia offesa «in presenza di più persone». Ma la *pubblicità* dell'offesa, sul piano logico, lega indubbiamente quest'ultima al profilo *esterno* dell'onore, ossia alla reputazione, la cui lesione dunque, in questo caso, si va a *sommare* all'offesa 'tipica' dell'ingiuria (i.e. quella al sentimento dell'offeso), a fronte, tuttavia, della paradossale scelta legislativa di *mitigare* – oggi in misura ancor più ingente, considerata l'irrilevanza penale delle ingiurie – il trattamento sanzionatorio della condotta pur in presenza di un cumulo di profili di lesività. Questo, sul (discutibile) presupposto concettuale che l'essere presente garantisca automaticamente alla persona offesa un ridimensionamento della lesione al proprio onore, *sia* interno *sia* esterno, in ragione dell'(asserita) possibilità di immediata autodifesa che le sarebbe garantita dalla natura 'faccia a faccia' dell'interazione insultante[65].

Quest'ultimo 'nodo' viene oggi con decisione 'al pettine' delle ICT. Nell'ecosistema digitale, infatti, può essere assai arduo determinare con certezza se l'offesa sia avvenuta in 'presenza' o in 'assenza' della persona aggredita nella sua onorabilità, e infatti uno sguardo alla giurisprudenza rivela un quadro oscillante, in relazione soprattutto al tema delle condotte tenute in chat, quanto ad opzioni per l'una o l'altra fattispecie, come pure un certo affanno nei tentativi di applicare a questi scenari la 'vecchia' *ratio* distintiva tra le due fattispecie.

A titolo di esempio, si segnalano casi in cui condotte di questo tipo (e.g. offese recate in una chat vocale di Google Handouts) vengono ricondotte alla fattispecie di ingiuria

[64] Questa distinzione affonda le sue radici nella c.d. concezione fattuale dell'onore, prevalente all'epoca della redazione del Codice Rocco, che considerava l'onore nella sua dimensione empirica, di realtà psicologica e sociale. Cfr. *supra*, note 2 e 28, nonché, specificamente, V. MANZINI, *Trattato di diritto penale italiano*, VIII, UTET, Torino, 1986[5], pp. 505 ss. e 622 ss.; F. ANTOLISEI, *Diritto penale. Parte speciale*, I, Giuffrè, Milano, 2002[14], p. 194; SPASARI, *Sintesi*, cit., p. 6; ID., *Ingiuria e diffamazione*, cit., p. 482.

[65] V. *supra*, nota 36.

sulla base della considerazione che, in tali contesti, l'offeso sia «in grado di interloquire con l'offensore»[66] – laddove lo stesso uso del concetto di 'interlocuzione' appare, per così dire, 'troppo generoso', o quanto meno 'poco aggiornato', in un contesto digitale che consente a chiunque di 'mettere in muto' l'audio altrui, scollegarsi dalla comunicazione nella frazione di secondo necessaria a un clic, e così via. In altri casi, condotte analoghe sono state invece inquadrate nel delitto di diffamazione 'semplice' – ossia non aggravata dall'uso di un mezzo di pubblicità – avendo i giudici ritenuto WhatsApp «uno strumento di comunicazione di certo 'agevolante' ma al contempo 'ristretto', nel senso che il messaggio (di testo o immagine che sia) raggiunge esclusivamente i soggetti iscritti (e reciprocamente accettatisi) alla medesima chat»[67]: un'altra valutazione che, al di là delle specificità del caso concreto, non può non suscitare qualche perplessità di fronte all'esperienza empirica dell'estensione assai vasta di molti gruppi su tale piattaforma (e altre simili), nonché dell'estrema rapidità e facilità con cui qualsiasi utente coinvolto nello scambio è in grado di ricondividere, direttamente (inoltro) o indirettamente (inoltro e/o ripubblicazione di *screenshot*), i contenuti offensivi ivi diffusi[68], anche ove vengano cancellati dal mittente originario. Né maggiori certezze danno, in realtà, quelle pronunce che riconducono, in casi affini, il fatto all'ingiuria o alla diffamazione a seconda che la persona offesa fosse online o meno al momento dell'esternazione lesiva[69]: non è infatti difficile prefigurarsi i problemi probatori legati a una tale

[66] Cfr. Cass. pen., V, 31 marzo 2020, n. 10905, commentata da E. La Rosa, *Offese in videochat. La Corte di Cassazione si pronuncia sui rapporti tra ingiuria e diffamazione*, in «Giurisprudenza italiana», 7 (2020), pp. 1750-1756.

[67] Cfr. Cass. pen., I, 14 settembre 2023, n. 37618, con commento di C. Rossi, *Non ricorre l'aggravante dell'uso di un mezzo di pubblicità nel caso di diffusione di un messaggio offensivo in una "chat" attraverso "WhatsApp"*, in «Cassazione penale», 3 (2024), pp. 1006-1009.

[68] Un aspetto, quest'ultimo, che, in punto di puro diritto, correttamente la pronuncia in discorso (v. nota precedente) considera non pertinente («Non rileva, infatti, che il messaggio – destinato ad un numero ristretto di persone – possa essere inoltrato ad altri, posto che simile azione sarebbe opera del destinatario e non del mittente»), ma che tuttavia, da un punto di vista pratico – e, idealmente, in una prospettiva *de iure condendo* (v. *infra*) – non può non essere preso in considerazione nella valutazione dell'offensività *reale* delle condotte in esame.

[69] Cfr. Cass. pen., V, 20 luglio 2022, n. 28675: «il Collegio osserva – reputandolo dato di comune esperienza, data la massiccia diffusione del sistema di messaggistica istantanea adoperato nel caso di specie – che la chat di gruppo di whatsapp consente l'invio contestuale di messaggi a più persone, che possono riceverli immediatamente o in tempi differiti a seconda dell'efficienza del collegamento ad internet del terminale su cui l'applicazione viene da loro utilizzata; i destinatari possono, poi, leggere i messaggi in tempo reale (perché stanno consultando, in quel momento, proprio quella specifica chat) e, quindi, rispondere con immediatezza ovvero, come accade molto più spesso, possono leggerli, anche a distanza di tempo, quando non sono *on line* ovvero, pur essendo collegati a whatsapp, si trovino impegnati in altra conversazione virtuale e non consultino immediatamente la conversazione nell'ambito della quale il messaggio è stato inviato. Se questo è, per quanto di specifico interesse in questa sede, il funzionamento del servizio di messaggistica istantanea che viene in rilievo in questo procedimento, se ne può inferire che la percezione da parte della vittima dell'offesa può essere contestuale ovvero differita, a seconda che ella stia consultando proprio quella specifica chat di whatsapp o meno; nel primo caso, vi sarà ingiuria aggravata dalla presenza di più persone quanti sono i membri della chat perché la persona offesa dovrà ritenersi virtualmente presente; nel secondo caso si avrà diffamazione, in quanto la vittima dovrà essere considerata assente». La citazione letterale illustra meglio di qualsiasi commento il carattere totalmente casuale, *e indipendente da qualsiasi scelta consapevole dell'autore della condotta*, della sussumibilità del singolo, specifico caso sotto l'una o l'altra fattispecie, malgrado la differenza in termini di conseguenze sanzionatorie.

opzione, specie ove l'evidenza della presenza dell'offeso non possa essere ricavata dalla sua immediata reazione. Reazione che, per altro, nel caso, avrà il paradossale effetto di 'ritorcerglisi contro' (in termini di conseguenze sanzionatorie per l'autore del fatto) nel momento in cui questi cercherà la tutela dell'ordinamento penale.

Il che ci riconduce al tema della 'cattiva costruzione' del microsistema normativo in esame: se, come sopra accennato, l'assunto che la 'presenza dell'offeso' riduca gli effetti lesivi della condotta è sempre parso poco fondato, e quindi la distinzione tra le due fattispecie sostanzialmente irrazionale, lo 'stress test' cui le nuove ICT lo sottopongono ne rende inevitabile l'implosione. L'impostazione prescelta dal nostro legislatore, infatti, finisce – da sempre – per creare un *onere* in capo alla persona aggredita nel suo onore, la quale, implicitamente, viene normativamente ritenuta *meritevole* di minor tutela laddove – per motivi soggettivi o oggettivi – *non sia in grado* di esercitare un'efficace autodifesa. L'assurdità di tale assunto è disvelata pienamente ove questo sia applicato – come attualmente *deve* essere applicato – agli ecosistemi digitali. In essi, infatti, sia per l'assenza di reale 'faccia a faccia' tra i 'contendenti'[70], sia, soprattutto, per il già richiamato, e impressionante, aumento della velocità degli scambi comunicativi, unito all'enorme maggior diffusività degli stessi, la posizione di svantaggio dell''aggredito' (è dato di comune esperienza che le accuse infamanti hanno una notevole capacità di 'restare attaccate' alle persone, a prescindere da ogni più valida 'difesa') viene esasperata oltre ogni misura.

A questo primo profilo di grave irrazionalità – e conseguente seria ineffettività – dell'attuale impianto della tutela sanzionatoria della reputazione se ne aggiunge un altro, legato alla già richiamata netta opzione del legislatore del 1930 per una tutela rigidamente *formale* della stessa. Vero è che anche il Codice Zanardelli poneva limiti all'operatività della c.d. *exceptio veritatis*, confinando la tutela della (sola) reputazione sostanziale (i.e., corrispondente alla realtà fattuale) a ipotesi circoscritte, selezionate in ragione del loro rilievo 'pubblicistico' (art. 394, co. 2, n. 1: persona offesa qualificata come pubblico ufficiale e fatto offensivo ad essa attribuito inerente all'esercizio delle sue funzioni), dell'esigenza di garantire la 'non contraddizione' dell'ordinamento (art. 394, co. 2, n. 2: pendenza o apertura di un procedimento penale per il fatto attribuito alla persona offesa) o del riconoscimento all'offeso della libertà di optare in questo senso, anche in vista di un più efficace ripristino della limpidezza della propria reputazione (art. 394, co. 2, n. 3). Tuttavia, il legislatore del 1930 eliminò, come è noto, anche queste ipotesi. Ne risultò un sistema impostato sulla tutela della reputazione 'a prescindere', puramente formale, coerente con un'idea autoritaria per cui compito dello Stato era prevenire ogni turbamento dello *status quo*[71]. A conferma di ciò, non è un caso che, alla caduta del regime, lo stesso d.lgs.lgt. 14 settembre 1944, n. 288 che introdusse la scriminante della reazione legittima ad atti arbitrari del p.u. (in relazione ai delitti di violenza o minaccia, resistenza e oltraggio a un pubblico ufficiale) reintroducesse

[70] Cfr. anche P. WALLACE, *The Psychology of the Internet*, Cambridge University Press, Cambridge (MA), 2016[2] (trad. it., Cortina, Milano, 2017), in part. pp. 134-148.

[71] V. *supra*, note 37 e 38.

anche le ipotesi di *exceptio veritatis* già contemplate nel Codice del 1889, con l'inserimento nell'art. 596 c.p. dei co. 3 e 4, tutt'ora vigenti, così nuovamente 'ritagliando' una protezione ristretta alla sola reputazione sostanziale almeno in tali casi[72].

Nel dopoguerra, tuttavia, al legislatore mancò il coraggio di una riforma più radicale dei delitti contro l'onore, e lo spazio 'esimente' per la verità dei fatti addebitati fu individuato e modellato, come è noto, dalla giurisprudenza in tema di legittimo esercizio del diritto di cronaca (e di critica, in relazione alla base argomentativa dell'opinione espressa)[73]. In questo quadro – che è quello in cui tutt'oggi ci muoviamo – tuttavia, la verità dell'addebito non svolge un ruolo di circoscrizione della tipicità dell'offesa, bensì quello, concettualmente e strutturalmente diverso, di parametro di legittimità – insieme a quelli, concorrenti, della pertinenza (i.e. interesse pubblico) dell'esternazione e della continenza della forma espressiva usata – dell'esercizio della libertà di espressione (*ex* art. 21 Cost.) in funzione scriminante (*ex* art. 51, co. 1 c.p.). L'ordinamento continua, dunque, a essere impostato – tolte le ipotesi circoscritte di cui all'art. 596, co. 3 c.p. – su una tutela della reputazione *formale* (salva la possibile *liceità* della condotta diffamatoria, *tipica* anche quando consistente in addebiti perfettamente fondati, in presenza di *tutti* i presupposti di tali scriminanti). Un'impostazione, come si è avuto modo di osservare, in definitiva rafforzata dal progressivo slittamento interpretativo, in materia di oggettività giuridica tutelata, dall'originario approccio 'fattuale' all'attuale orientamento personalistico-costituzionale, che tende a sovrapporre reputazione e dignità.

Una tale impostazione è tutt'altro che 'fisiologica' e scontata: non solo negli ordinamenti di *common law* la stessa sussistenza del *tort* di *defamation* (o *libel*) richiede, costitutivamente, la *falsità* dell'addebito diffamatorio[74], ma, restando ai sistemi che

[72] La ragionevolezza di tali eccezioni alla – normale – tutelabilità dell'onore formale fu affermata dalla Consulta con la già richiamata sentenza n. 103/1973: «le norme sull'*exceptio* non possono dirsi incostituzionali in quanto vulneranti il principio di garanzia dell'eguale dignità dei cittadini davanti alla legge: la tutela dell'onore sostanziale presenta una sua ragione di essere in quanto la si riguardi in sé o in relazione a quella di altri rilevanti interessi concorrenti, tutela quest'ultima che è attuata attraverso la garanzia del rispetto della verità». In quest'ottica, la Corte ritiene sicuramente 'rilevante' «l'esigenza di carattere generale a che il pubblico ufficiale non si trinceri dietro lo scudo della tutela esteriore, ed invece si faccia interamente luce sull'addebito ed i cittadini possano esercitare un controllo sia pure indiretto sull'andamento della pubblica Amministrazione e sul comportamento del relativo personale, e quindi condizioni obiettive che ragionevolmente consigliano la tutela più ampia» (evidentemente, nel senso di 'più efficace' nel 'ripulirlo' dalla 'macchia' altrimenti sostanzialmente indelebile creata dall'allegazione diffamatoria) «dell'onore e della reputazione del pubblico ufficiale».

[73] La giurisprudenza in tema è ormai sterminata, e sarebbe estraneo agli scopi del presente contributo tentare di richiamarla qui anche solo in parte. Si rinvia quindi agli ampi riferimenti presenti nei testi citati *supra*, alle note 2 e 7.

[74] Come è noto, in tali ordinamenti il ruolo del diritto penale nella tutela della (sola) reputazione (essendo tradizionalmente considerato non meritevole di tutela giuridica il mero sentimento del proprio onore) è sempre stato del tutto marginale (per lo più confinato a casi di parziale sovrapposizione a interessi collettivi, quale quello a evitare un c.d. *breach of the peace*), ed è andato ulteriormente riducendosi (o sparendo) negli ultimi decenni. Per una discussione dettagliata, in particolare, degli ordinamenti inglese e statunitense ci si permette di rinviare, per

contemplano ancora un forte ruolo della tutela penale dell'onore e della reputazione, è sufficiente guardare oltralpe, all'ordinamento francese[75], per imbattersi in un modello molto diverso e, almeno ad avviso di chi scrive, più razionale. Qui, infatti, il discrimine tra ingiuria (art. 29, co. 2 LLP e art. R.621-2 c.p.) e diffamazione (artt. 29, co. 1 e 35, co. 3 LLP, e art. R.621-1 c.p.) è legato al consistere dell'offesa, rispettivamente, in un'attribuzione indeterminata – come tale non propriamente predicabile di 'verità' o 'falsità' (ingiuria) – oppure di un fatto diffamatorio falso e determinato (diffamazione), mentre la pubblicità o meno dell'offesa recata segna il confine tra natura delittuosa (artt. 29 e 35 LLP) o, al contrario, contravvenzionale (artt. R.621-1 e R.621-2 c.p.) dell'illecito (di ingiuria o diffamazione).

Come sopra accennato, l'attuale impostazione dell'ordinamento italiano sembra, almeno all'apparenza, avere portato benefici in termini di espansione della tutela, vieppiù 'apprezzabili' alla luce delle nuove sfide poste dalla 'quarta rivoluzione', la quale ha reso ancora più comuni, e più pervasive, offese 'ibride' ai diritti della personalità, e in particolare offese che, seppur più propriamente riconducibili alla sfera della riservatezza, per la particolare diffusività legata all'ecosistema digitale in cui avvengono presentano un tale impatto (almeno potenziale) sulla vita sociale delle persone da non poter essere certo liquidate come marginali o irrilevanti. Così, ad esempio, la giurisprudenza ha pacificamente ritenuto inquadrabile nel delitto di diffamazione la pubblicazione online di una sentenza di condanna penale nella quale, tuttavia, l'autore della divulgazione aveva evidenziato, graficamente e con chiose, i passaggi di testo relativi alla vita sessuale della persona offesa[76]; analogamente, è stata ritenuta punibile *ex* art. 595, co. 3 c.p. la condivisione su Internet, mediante un programma di condivisione *peer-to-peer*, di filmati riproducenti atti sessuali riferiti alla persona offesa[77]; ancora, è stata ritenuta riconducibile al delitto in parola la pubblicazione su Facebook di immagini fotografiche ritraenti una persona in pose pornografiche, allorché tale diffusione avvenga in un contesto e per destinatari diversi da quelli rispetto ai quali la persona stessa aveva in precedenza prestato il suo consenso alla pubblicazione[78].

esigenze di sintesi, a VISCONTI, *Reputazione, dignità, onore*, cit., pp. 397-466. In tema di *defamation* e nuovi mezzi di comunicazione digitali cfr. anche, specificamente, H.M. DREIBELBIS, *Social Media Defamation: A New Legal Frontier amid the Internet Wild West*, in «Duke Journal of Constitutional Law & Public Policy», 16 (2021), pp. 245-278, nonché, per un approfondimento sulla diffusione di *deepfake video* di natura pornografica, A. GEORGE, *Defamation in the Time of Deepfakes*, in «Columbia Journal of Gender and Law», 45/1 (2024), pp. 122-172.

[75] In cui la disciplina degli illeciti in esame si divide tra la *Loi du 29 juillet 1881 sur la liberté de la presse* (artt. 29-35 quater) e il Codice penale (artt. R621-1 e R621-1). Cfr. P. CONTE, *Droit pénal spécial*, Lexis Nexis, Paris, 2016[5], pp. 275 ss. Si vedano anche GULLO, *Diffamazione*, cit., pp. 136 ss., e, più sinteticamente, BISORI, *I delitti*, cit., pp. 5-6.

[76] Cfr. Cass. pen., V, 1° giugno 2021, n. 28634, commentata da A. IEVOLELLA, *Pubblica una sentenza online e sottolinea le performances sessuali della persona coinvolta: condannato per diffamazione*, in «Diritto & Giustizia», 144 (2021), p. 4.

[77] Cfr. Cass. pen., V, 14 ottobre 2015, n. 41276.

[78] Cfr. Cass. pen., III, 8 maggio 2019, n. 19659.

Se, dunque, la divulgazione di contenuti di per sé fattualmente fondati, ma non coperti da interesse pubblico (attuale), è allo stato perfettamente 'coperta' dalle fattispecie esistenti nella loro costante interpretazione giurisprudenziale, men che meno si può dubitare che lo sia la diffusione di materiali audiovisivi (non già illecitamente carpiti o divulgati, bensì, alla radice) creati o manipolati con strumenti di editing digitale o di IA. E questo non solo nel caso in cui tali materiali abbiano a oggetto la sfera privata (per lo più, ma non necessariamente, sessuale) della persona offesa, ma anche in casi molto diversi, che possono andare dalla rappresentazione della persona mentre commette un'azione socialmente, moralmente o legalmente riprovevole che non ha mai commesso, alla manipolazione della sua voce per farle pronunciare frasi (razziste, oscene, ecc.) mai pronunciate, e così via.

Questo, tuttavia, non rende l'attuale impianto normativo veramente 'a prova di ICT', pur avendone indubbiamente favorito l'adattabilità ai nuovi scenari tecnologici. Oltre ai problemi di perimetrazione delle condotte tra ingiuria e diffamazione già evidenziati, infatti, il sistema mostra la sua arretratezza e inadeguatezza sotto altri profili, primo dei quali (duole osservare al penalista) quello sanzionatorio. Le vecchie categorie del «mezzo della stampa» e dell'«altro mezzo di pubblicità», infatti, sono totalmente inadeguate a dar veramente conto delle specificità, in termini di diffusività e potenziale illimitata accessibilità dei contenuti diffamatori (oggi esasperata dall'integrazione nei motori di ricerca di sistemi di AI generativa, in grado di annullare anche quel poco di effetto 'protettivo' garantito, in passato, dalla deindicizzazione)[79], delle moderne ICT. Inoltre, la bilanciabilità legata alla loro natura circostanziale le rende, al momento, pressoché del tutto neutralizzabili nel caso concreto, a seconda delle attenuanti eventualmente riconosciute come prevalenti o equivalenti – così rispecchiando, ancora una volta, un approccio che, se poteva ritenersi valido rispetto alle dinamiche dei mezzi di comunicazione analogici, lo appare molto meno ove rapportato all'ecosistema delle comunicazioni digitali.

Queste problematiche appaiono solo parzialmente attenuate a seguito della recentissima introduzione, a opera della L. 23 settembre 2025, n. 132, del nuovo delitto di «illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale» di cui all'art. 612 *quater* c.p. La fattispecie, collocata tra i reati contro la libertà morale con l'idea, nelle parole della Relazione illustrativa, di «offrire una tutela rafforzata della persona» dal «pregiudizio all'autodeterminazione ed al pieno svolgimento della personalità derivante dalla diffusione di immagini, video, voci falsificati mediante sistemi di intelligenza artificiale», si presta a concorrere con il delitto di diffamazione (e non solo nei casi di c.d. *deepfake porn*). L'evento richiesto per l'integrazione del nuovo reato, infatti, è assai più ampio e generico – l'art. 612 *quater* c.p. richiede che sia cagionato un qualsiasi «danno ingiusto» alla persona offesa – di quello proprio della diffamazione

[79] Cfr. per tutti A. Amidei, *Piattaforme e content moderation. Vecchi e nuovi problemi in tema di motori di ricerca, tra oblio e informazione*, in «Giurisprudenza italiana», 2 (2024), pp. 466-472.

(offesa alla reputazione, che per altro si è già visto essere per lo più declinata in termini di mero pericolo), mentre, per altro verso, la condotta – consistente nel cedere, pubblicare o «altrimenti» diffondere (senza il consenso della persona offesa) «immagini, video o voci falsificati o alterati», *specificamente* «mediante l'impiego di sistemi di intelligenza artificiale», i quali siano «idonei a indurre in inganno sulla loro genuinità» – è connotata da una nota di *falsità* (addirittura *duplice*: *genetica*, quanto alla creazione *ex novo*, o alterazione, di contenuti non rispondenti a realtà, e *attitudinale*, quanto a idoneità ingannatoria nei confronti del fruitore del contenuto) del tutto aliena, come si è visto, alla diffamazione. In questi casi, anzi, il complessivo trattamento sanzionatorio rischia in teoria la sproporzione per eccesso (rischio, per altro, evitabile in pratica con un'applicazione oculata del cumulo giuridico *ex* art. 81 c.p.). Ma l'intervento legislativo in parola, a ben guardare, non incide affatto sulla sopra evidenziata debolezza *strutturale* del microsistema ingiuria-diffamazione in rapporto a tutte le *altre* forme di 'attacco' online (o, meglio, onlife) alla reputazione che non involgano la creazione e diffusione di *deepfakes* con le caratteristiche specificate.

Conclusivamente, l'attuale sistema degli illeciti a tutela dell'onore e della reputazione appare bisognoso, ad avviso di chi scrive, di un complessivo ripensamento (reso, semmai, *ancora* più urgente dall'introduzione di nuove, e non coordinate, disposizioni penali indirizzate a colpire il fenomeno dei *deepfakes* prodotti con sistemi di AI)[80]. Ragionando in termini di tutela della reputazione, perno della repressione penale dovrebbe essere il concetto di 'pubblicazione' del contenuto offensivo, mentre nessuna rilevanza dovrebbe avere la 'presenza' (reale o virtuale) dell'offeso. Questo non solo perché, come altrove meglio argomentato[81], in un ordinamento maturo e democratico il 'sentimento dell'onore' – troppo soggettivo, inafferrabile, e spesso legato a 'codici'

[80] Va infatti ricordato che lo stesso art. 26 della l. n. 132/2025 ha anche introdotto una circostanza aggravante comune all'art. 61 c.p., nuovo numero 11 *decies* (ma il legislatore pare aver dimenticato di aver *già* introdotto, nelle more dell'adozione della normativa in materia di AI, un numero 11 *decies*, di dubbia compatibilità costituzionale, con il d.l. 11 aprile 2025, n. 48 – c.d. pacchetto sicurezza – convertito con L. 9 giugno 2025, n. 80), applicabile ove il fatto di reato sia commesso «mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato». Appare quindi ragionevole domandarsi se, in un caso di diffamazione realizzata mediante diffusione di *deepfakes*, debba effettivamente ritenersi un concorso tra art. 595 c.p. e (nuovo) art. 612 *quater* c.p., o non piuttosto un caso di diffamazione aggravata *ex* art. 61 n. 11 *decies*) c.p. A una prima lettura, tuttavia, sembra doversi accordare rilievo preminente alla considerazione che l'AI, nello scenario in questione, interviene nella fase della *creazione* del contenuto lesivo della reputazione, fase di per sé estranea e indifferente alla condotta propriamente 'diffamatoria', in cui la comunicazione con più persone, anche online (il che, come si è visto, integra l'aggravante di cui al co. 3 dell'art. 595 c.p.), non implica normalmente un (volontario) uso *strumentale* di sistemi di AI. L''insidiosità' del mezzo AI si colloca, dunque, *a monte* della condotta diffamatoria (così come a monte di questa stanno le potenzialità di approfondimento dell'offesa alla reputazione tipiche dei più riusciti *deepfakes*), di talché sembra doversi concludere per un concorso tra art. 595 (per solito aggravato *ex* co. 3) c.p. e art. 612 *quater* c.p. (ovviamente a condizione che di questo ricorrano tutti i presupposti).

[81] Cfr. VISCONTI, *Reputazione, dignità, onore*, cit., pp. 597 ss.

culturali retrivi – non dovrebbe avere cittadinanza, ma soprattutto perché è la diffusività dell'addebito diffamatorio, a prescindere dalla reazione che la persona possa o meno avervi prestato nell'immediatezza, a rendere non solo concretamente afferrabile, ma anche dimensionalmente parametrabile, l'offesa, tanto da suggerire una differenziazione, già sul piano della tipicità (oltre che su quello sanzionatorio) delle fattispecie, tra forme di pubblicazione 'analogiche' e forme di diffusione 'onlife'.

Ma anche per altri versi una migliore perimetrazione dell'oggetto – o degli oggetti – della tutela penale sarebbe probabilmente, sul medio-lungo periodo, fonte di maggiore effettività del sistema. La reazione penale dovrebbe essere limitata, sul fronte della difesa della reputazione strettamente intesa, alla diffusione di addebiti offensivi falsi[82], eventualmente con apposita valorizzazione dell'accentuato potenziale decettivo legato all'uso di strumenti di AI nella *creazione* del contenuto mendace e diffamatorio (realizzando, quindi, una maggiore integrazione e un miglior coordinamento del sistema, rispetto a quanto risultante oggi, a seguito della l. n. 132/2025). Il tutto, salva l'individuazione di un'apposita, parallela tutela contro quegli attacchi alla riservatezza che, per la natura stigmatizzante (a torto o a ragione, ma comunque in relazione alla realtà socioculturale di contesto) dell'informazione illecitamente divulgata, siano a loro volta suscettibili di esporre la persona offesa a una perdita di capitale sociale[83], in particolare ove connotati dalla particolare pervasività e diffusività legata all'utilizzo di ICT.

Una tale razionalizzazione del quadro normativo ridurrebbe l'incertezza applicativa e le difficoltà probatorie complessive, migliorando il tasso di precisione e determinatezza del sistema e la sua compatibilità con i principi di offensività ed *extrema ratio*, il che – tra l'altro – restituirebbe legittimità anche ad eventuali scelte (consapevoli e mirate) di ricorso alla pena detentiva per quegli scenari eccezionali (e del tutto residuali) evocati dalla giurisprudenza EDU e costituzionale, quali «discorsi d'odio» o connotati da contestuale «istigazione alla violenza», o anche «campagne di disinformazione condotte attraverso la stampa, internet o i social media, caratterizzate dalla diffusione di addebiti gravemente lesivi della reputazione della vittima, e compiute

[82] L'inserimento della falsità dell'addebito tra gli elementi della tipicità, necessariamente coperti dal dolo, potrebbe forse (salvo il sempre presente rischio di un abuso strumentale della categoria del dolo eventuale) anche porre un argine a quel 'diritto vivente', giustamente stigmatizzato dalla Consulta nella richiamata sentenza n. 150/2021, che ha di fatto introdotto una fattispecie di diffamazione a mezzo stampa colposa, «condiziona[ndo] l'operatività della causa di giustificazione del diritto di cronaca nella sua forma putativa (art. 59, quarto comma, cod. pen.) al requisito dell'assenza di colpa nel controllo delle fonti: ammettendo conseguentemente la responsabilità del giornalista per il delitto di diffamazione anche nell'ipotesi in cui egli abbia confidato, seppur per un errore evitabile, nella verità del fatto attribuito alla persona offesa». Per una rassegna di riferimenti giurisprudenziali di merito e legittimità in argomento si rinvia, ancora una volta, ai testi citati *supra*, note 2 e 7.

[83] Come è stato osservato in dottrina, del resto, nell'ambito che qui interessa «spostare la dimensione della tutela da quella della reputazione e/o dell'onore a quella della riservatezza può aiutare a disincentivare meccanismi, consapevoli o inconsapevoli, di *victim blaming*. La reputazione di una persona non dovrebbe considerarsi a priori lesa per la messa in circolazione delle sue immagini sessualmente esplicite, poiché non è la condotta a inficiare la reputazione, ma la reazione sociale a tale condotta» (cfr. G.M. Caletti, *Habeas corpus digitale. Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Giappichelli, Torino, 2024, p. 230, nota 63).

nella consapevolezza da parte dei loro autori della – oggettiva e dimostrabile – falsità degli addebiti stessi»[84].

4. *Un* caveat *conclusivo: la necessità di un «design pro-etico» dell'ecosistema digitale*

Questa apertura a un ventaglio sanzionatorio differenziato, suscettibile di includere anche – rispetto a scenari di offensività estrema – la pena detentiva, non va però confusa con un affidamento fideistico nelle capacità preventive dello strumento penale. Al contrario, mai come nel contesto della 'quarta rivoluzione' e della dimensione 'onlife', quest'ultimo appare del tutto inadeguato, se non come 'elemento di chiusura' di un modello preventivo che dovrebbe puntare prima e prevalentemente sulla rimozione, o per lo meno sulla massima riduzione possibile, di quelli che la psicologia sociale definisce fattori 'sistemici' e 'situazionali' di genesi della devianza[85].

Come altrove osservato[86], è l'attuale design dell'ecosistema digitale a presentare una serie di fattori strutturalmente criminogeni – non solo in rapporto al reato di diffamazione, ma rispetto a tutte le possibili condotte illecite e lesive online – che vanno dall'anonimato, quanto meno percepito, degli utenti, al distanziamento fisico e psichico dalle conseguenze delle proprie azioni, all'eccessiva compressione dei tempi di azione-reazione, a meccanismi algoritmici di 'segregazione' in camere dell'eco che confermano (o rafforzano) l'individuo nella convinzione della validità dei propri assunti e delle proprie linee di condotta, e così via. In breve, quello digitale è, oggi, un ecosistema strutturalmente anomico, che in quanto tale favorisce circoli viziosi di crescente violazione delle regole[87], non solo giuridiche, ma di elementare civile convivenza.

[84] Cfr. C. Cost. n. 150/2021, cit. Nella giurisprudenza della Corte EDU si vedano, *ex multis*, oltre alle pronunce citate supra (nota 33), anche Gr. Ch., 17 dicembre 2004, *Cumpănă e Mazăre c. Romania*, ric.n. 33348/96; sez. I, 6 dicembre 2007, *Katrami c. Grecia*, ric.n. 19331/05; sez. II, 5 novembre 2020, *Balaskas c. Grecia*, ric.n. 73087/17.

[85] Cfr. per tutti P.G. Zimbardo, *The Lucifer Effect. How Good People Turn Evil*, Random House, New York, 2007 (trad. it., Cortina, Milano, 2008), in part. pp. 293 ss., anche per tutti gli ulteriori riferimenti bibliografici, per i quali si rinvia altresì, *ex multis*, a M. Catino, *Miopia organizzativa. Problemi di razionalità e previsione nelle organizzazioni*, Bologna, il Mulino, 2009.

[86] Cfr. A. Visconti, *Alcune considerazioni criminologiche e politico-criminali sulle c.d. 'fake news'*, in «Jus», 1 (2020), pp. 43-71, cui si rinvia, per necessità di sintesi, anche per tutti gli ulteriori, puntuali riferimenti bibliografici. V. inoltre *supra*, nota 70.

[87] Per 'contesto anomico' si intende qui qualsiasi ambiente che trasmetta la percezione di una diffusa, generalizzata violazione delle regole e quindi, implicitamente, anche quella di una diffusa tolleranza (sostanziale, se non ufficiale) per tali infrazioni: studi empirici hanno infatti dimostrato come in tali ambienti aumenti in modo statisticamente rilevante il numero di episodi di devianza. Per descrivere tale meccanismo si parla anche di '*broken window effect*'. Cfr. per tutti W.G. Skogan, *Disorder and Decline: Crime and the Spiral of Decay in American Neighborhoods*, University of California Press, Berkeley, 1990; M. Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference*, Little Brown, Boston, 2000; K. Keizer, S. Lindenberg, L. Steg, *The Spreading of Disorder*, in «Science», 322/5908 (2008), pp. 1681-1685 (quest'ultimo studio, strutturato in modo da rendere

Le recenti richieste di archiviazione nei casi Seymandi[88] e Segre[89], per quanto certamente in parte dovute alla nuova, più elevata 'asticella' posta all'esercizio dell'azione penale dalla c.d. riforma Cartabia[90], e per quanto in ultimo 'rintuzzate' in sede di

possibile il confronto con un gruppo di controllo, è decisamente più significativo dei precedenti, basati su evidenze maggiormente aneddotiche, e comunque non in grado di escludere variabili indipendenti).

[88] Cfr. Trib. Torino, sez. GUP, ord. 20 gennaio 2025: la richiesta di archiviazione si fondava (oltre che sull'asserita impossibilità di individuare gli autori dei commenti offensivi postati sul profilo social della persona offesa) sulla ritenuta applicabilità della scriminante del diritto di critica, trattandosi di vicenda e figura pubblica e dovendosi considerare che «l'interpretazione del requisito della continenza non potrebbe non tenere conto dell'evoluzione della società e del suo linguaggio (soprattutto del linguaggio utilizzato sui social network), dovendosi adeguare a criteri più elastici, sino a ricomprendere anche l'utilizzo di espressioni "forti"»; posizione non accolta dal GUP, il quale, al contrario, considerato anche che le espressioni fatte oggetto di querela per diffamazione, nel caso di specie, «attengono tutt[e], in buona sostanza, alla morale sessuale femminile» (sostanziandosi in epiteti quali 'puttana', 'zoccola' e simili), e sono dunque «inquadrabili nell'ambito di comportamenti sessisti e discorsi d'odio realizzati con l'utilizzo delle tecnologie dell'informazione e della comunicazione (TIC), cui la normativa comunitaria dedica particolare attenzione, ritenendoli forme di manifestazione del più ampio concetto di violenza sulle donne», non ha ritenuto configurabile la scriminante in parola. I commenti in esame, infatti, «proprio perché volti a stigmatizzare la parte lesa in funzione del genere, appaiono marcatamente discriminatori: essi non sono espressione di un giudizio meramente critico, ma appaiono basati su stereotipi di genere animati, in via esclusiva, da finalità offensive», cosa che «rende arduo, già dal principio, ravvisare un legittimo esercizio del diritto di critica». Seppur, quindi, il GUP «concord[i], in linea generale, sulla necessità di adeguare la valutazione del requisito della continenza al mutato contesto sociale e al luogo ove il commento viene espresso (Facebook)», nel caso di spece ritiene che «le parole scelte dagli autori appaiono oggettivamente sopra le righe e inutilmente umilianti […] veri e propri insulti. I termini scelti non sono semplicemente inurbani o forti, ma volutamente e inequivocabilmente offensivi», anche per l'assenza, o comunque estrema distanza, del nucleo fattuale dal quale la 'critica' asseritamente prenderebbe le mosse, dal momento che «la critica presuppone pur sempre un ragionamento logico, ma se insulto immotivatamente, senza indicare il presupposto di fatto del mio giudizio, la frase resta diffamatoria».

[89] Cfr. Trib. Milano, sez. GUP, 28 aprile 2025: anche in questo caso, tolti i profili squisitamente probatori (inerenti alla difficoltà di ottenere la collaborazione dei provider nella raccolta delle informazioni necessarie all'identificazione degli autori dei commenti diffamatori postati su diverse piattaforme), il principale argomento avanzato nella richiesta di archiviazione riguarda le peculiari 'consuetudini comunicative' invalse sui social media, e la conseguente diversa declinazione che il parametro della continenza dovrebbe assumere ove si consideri che «è frequente nel dibattito politico l'utilizzo, per contrastare e stigmatizzare l'avversario politico, del termine "nazista", ovviamente in un senso differente rispetto a quello proprio e storico»; anche in questo caso, la posizione della pubblica accusa viene respinta dal GUP sul rilievo che, pur se «condivisibile nella sua valenza astratta, […] il ragionamento proposto non può invece essere calato nella peculiare vicenda in esame. A ben vedere, infatti, accusare di nazismo una reduce dai campi di sterminio integra di per sé il reato di diffamazione sia nei casi in cui tale epiteto viene esternato in modo apodittico e non argomentato, sia quando esso si accompagna a riferimenti che richiamano con spregevole ironia la vita nei lager». Inoltre, «la circostanza che espressioni offensive siano state formulate sul web non caratterizza la vicenda in termini di minor disvalore»: al contrario, proprio il caso portato all'attenzione del giudice «conferma che l'estrema diffusività dello strumento informatico genera spirali di odio e violenza che sono alimentate proprio dalla inescusabile leggerezza con cui gli utenti si lasciano andare a commenti diffamatori. Il numero impressionante di messaggi che si pongono ben oltre il limite più estremo della continenza non può determinare una sorta di assuefazione a un fenomeno che, invece, deve essere valutato secondo i consueti canoni di giudizio che regolano il confine fra diritto di critica e diritto all'onore. […] Il web non rappresenta un terreno franco dove ogni insulto è consentito e dove la reputazione degli individui può essere calpestata impunemente. Va ribadito che lo schermo di un computer non è una barriera che assicura l'anonimato e che la tastiera non è un'arma contro la quale non ci sono difese».

[90] Come è noto, a norma dell'art. 408, co. 1 c.p.p. come riformulato dal d.lgs. 10 ottobre 2022, n. 150, il pubblico ministero deve richiedere l'archiviazione «quando gli elementi acquisiti nel corso delle indagini pre-

udienza preliminare, sono comunque sintomatiche di una montante presa di consapevolezza di quanto sia difficile pretendere l'osservanza delle 'vecchie' regole di condotta – in materia di continenza espressiva[91], ma non solo – in un contesto di interazione sociale e comunicativa connotato da tanti e tali elementi di criminogenicità, e di un conseguente disagio, anche da parte della stessa magistratura requirente, nel (continuare ad) affidare allo strumento penale un compito per il quale si rivela, oggi più che mai, così profondamente inadeguato.

In un contesto di questo tipo, infatti, è innegabile che la capacità di orientamento dei comportamenti della norma penale sia, allo stato, pressoché inesistente. Ecco allora irrompere prepotentemente sulla scena l'esigenza di ricorrere, prima di tutto, a quello che ancora Luciano Floridi definisce un «*design pro-etico*» dell'infosfera, ossia una «configurazione degli ambienti» in cui le persone interagiscono che possa «rendere più agevoli le scelte, le azioni o i processi etici», senza paternalismo, ma attraverso una strutturazione di partenza che possa «agevolare la *riflessione* da parte degli agenti coinvolti sulle loro scelte, azioni o processi»[92].

Non è questa la sede – né chi scrive avrebbe le competenze – per avanzare proposte dettagliate sul *quomodo* di tale design pro-etico[93], tanto più che «nelle società iperstoriche» qual è ormai la nostra «ogni regolamento che incide sul modo in cui le persone interagiscono con l'informazione è destinato […] a influenzare l'intera infosfera e l'habitat onlife in cui tali persone vivono»[94]. Questo richiede al legislatore (idealmente, sovranazionale – al minimo comunitario – vista la natura globale dell'infosfera stessa) non solo un'estrema cautela nel progettare ogni regolamentazione del sistema, la quale deve considerarne l'estrema complessità e interconnessione, ma anche la disponibilità

> a rivedere la propria decisione e strategia rapidamente, appena gli effetti sbagliati iniziano a manifestarsi. […] Non esistono leggi perfette, ma soltanto leggi che possono essere perfezionate più o meno facilmente. Un buon accordo relativo al modo in cui configurare la nostra infraetica dovrebbe includere una clausola concernente il suo tempestivo aggiornamento. […] Infine, è sbagliato credere che siamo come stranieri che intendono regolare un ambiente distinto da quello che abitano. […] Stiamo riparando la zattera su cui navighiamo […]. Proprio perché

liminari non consentono di formulare una ragionevole previsione di condanna», laddove in precedenza doveva farlo in presenza di una notizia di reato «infondata». Parallelamente, mentre in precedenza l'art. 425, co. 3 c.p.p. prevedeva la pronuncia di sentenza di non luogo a procedere «quando gli elementi acquisiti risultano insufficienti, contraddittori o comunque non idonei a sostenere l'accusa in giudizio», la nuova formulazione della norma fa riferimento ad elementi acquisiti nel corso delle indagini preliminari che «non consentono di formulare una ragionevole previsione di condanna».

91 V. *supra*, note 88 e 89.

92 Cfr. FLORIDI, *The Fourth Revolution*, cit., p. 218.

93 Anche se almeno alcune misure volte, ad esempio, alla riduzione dell'anonimato percepito e della conseguente deresponsabilizzazione degli utenti, al rallentamento dei tempi di azione-reazione online, ecc., parrebbero abbastanza agevoli da immaginare e da implementare tecnicamente: cfr. ancora VISCONTI, *Alcune considerazioni criminologiche e politico-criminali*, cit.

94 Cfr. FLORIDI, *The Fourth Revolution*, cit., pp. 223-224.

> l'intero problema del rispetto, della violazione o applicazione dei diritti […] è una questione infraetica e ambientale per avanzate società dell'informazione, la cosa migliore da fare, per individuare la soluzione corretta, è di applicare al processo stesso il quadro infraetico e i valori etici che vorremmo vedere promossi da tale processo. Ciò vuol dire che l'infosfera dovrebbe regolare se stessa dall'interno e non da un impossibile esterno[95].

Questa esigenza, innegabile, di rapido e flessibile adattamento del quadro normativo alla continua emersione di nuovi scenari e alla stretta connessione di soggetto e oggetto della regolamentazione mette di per sé in luce come un adeguato tasso di efficacia della stessa non possa prescindere da una significativa componente di cooperazione da parte delle piattaforme oggetto della regolamentazione stessa.

Un approccio non facile, vista la sostanziale extraterritorialità di queste ultime, il potere economico e di orientamento dell'opinione pubblica da esse detenuto (di molto superiore a quello della maggior parte degli Stati) e la troppo frequente mancanza di adeguata comprensione tecnologica e sociologica dei fenomeni da regolare da parte del legislatore stesso, al quale spetta pur sempre definire la cornice valoriale di riferimento e un quadro minimo di doveri di *risk assessment* e *risk management* da parte dei soggetti regolati, nonché le strategie di risposta a eventuali violazioni. Strategie che, tuttavia, una volta abbandonata una prospettiva esclusivamente incentrata sull'individuo e sulla deterrenza – più arcaica e inadeguata che mai, nel quadro appena tratteggiato – e recuperati un più ragionevole orizzonte organizzativo e il riferimento a un più flessibile ed efficace modello di *responsive regulation* (in cui la componente punitiva non scompare, ma gioca un ruolo più ridotto e, al tempo stesso, più incisivo)[96], permetterebbero almeno di 'giocare una partita' che vede oggi, al contrario, l'ordinamento sostanzialmente confinato ai margini del terreno di gioco, quando non spettatore impotente sugli spalti all'esterno di questo.

[95] Cfr. FLORIDI, *The Fourth Revolution*, cit., p. 224.

[96] In tema non si può in questa sede che rinviare ai fondamentali scritti di J. BRAITHWAITE, *Enforced Self-Regulation: A New Strategy for Corporate Crime Control*, in «Michigan Law Review», 80/7 (1982), pp. 1466-1507; ID., *Convergence in Models of Regulatory Strategy*, in «Current Issues in Criminal Justice», 2/1 (1990), pp. 59-65; I. AYRES, J. BRAITHWAITE, *Responsive Regulation. Transcending the Deregulation Debate*, Oxford University Press, New York-Oxford, 1992, in part. pp. 38 ss.; B. FISSE, J. BRAITHWAITE, *Corporations, Crime and Accountability*, Cambridge University Press, Cambridge-New York, 1993, in part. pp. 31 ss. e 138 ss. Nella dottrina italiana, e per ulteriori riferimenti, cfr. inoltre, per tutti, G. FORTI, *Il crimine dei colletti bianchi come dislocazione dei confini normativi. "Doppio standard" e "doppio vincolo" nella decisione di delinquere o di blow the whistle*, in AA.VV., *Impresa e giustizia penale: tra passato e futuro*, Giuffrè, Milano, 2009, in part. pp. 212 ss., e G. ROTOLO, *'Riconoscibilità' del precetto penale e modelli innovativi di tutela. Analisi critica del diritto penale dell'ambiente*, Giappichelli, Torino, 2018, in part. pp. 215 ss.

IL CONTRASTO ALL'*ONLINE HATE SPEECH* NEL CONTESTO DEL *DIGITAL SERVICES ACT*: FRA *PRIVATE ENFORCEMENT*, MECCANISMI DI COMPLIANCE E TUTELA DEI DIRITTI FONDAMENTALI

Alessandra Galluccio

1. *Premessa*

Lo scopo dell'incontro odierno – nel più ampio contesto del progetto di ricerca "*Leveling the field. Clarifying the notion of illegal content under the EU's Digital Services Act*", finanziato da Alphabet/Google e in corso presso la Libera Università di Bolzano e l'Università di Bologna – è quello di intavolare una prima discussione sulla nozione di "contenuto illecito" ai sensi del nuovo Regolamento sui servizi digitali dell'Unione europea (c.d. *Digital Services Act*). Com'è noto, tale provvedimento normativo – che pure rappresenta una significativa evoluzione della regolamentazione della rete – si limita a rinviare alla normativa dell'Unione europea e alle diverse legislazioni degli Stati membri per la definizione del cruciale concetto di "contenuto illecito" la cui diffusione dà luogo alla responsabilità delle grandi piattaforme digitali.

L'ovvia indeterminatezza di una tale individuazione fa sorgere rilevanti questioni interpretative, anche alla luce della vastità dei fenomeni lesivi che si intendono regolare. Di qui la necessità, come evidenzia il titolo del progetto stesso, di individuare un nucleo comune di contenuti illeciti la cui diffusione sia vietata e in relazione alla quale possano configurarsi responsabilità penali a carico (non solo del singolo utente che abbia provveduto a caricare il contributo, ma anche) delle grandi piattaforme digitali.

Il compito che mi è stato affidato è quello di ricostruire sulla base della normativa italiana pertinente la fisionomia del contenuto illecito con riferimento al fenomeno dell'*hate speech*.

Il mio intervento si strutturerà a partire da una ricognizione della fattispecie deputata a intercettare tale fenomeno nel codice penale italiano – l'art. 604-*bis* cod. pen. – rammentandone le ben note criticità (§ 2); mi soffermerò, poi, sulle peculiarità del sistema disegnato dal DSA (§ 3); evidenzierò, infine, le difficoltà che si generano adoperando tale fattispecie quale matrice del "contenuto illecito" in materia di *online hate speech* (§ 4).

2. *Il fenomeno dell'*online hate speech*, la legislazione italiana e le sue criticità*

Il fenomeno dell'*hate speech* e – per quel che qui maggiormente ci riguarda – dell'*online hate speech* costituisce una delle sfide più complesse da fronteggiare tramite l'ausilio del diritto penale. Ciò, per una pluralità di motivi.

In primo luogo e più in generale: perché da sempre i reati di opinione costituiscono uno dei banchi di prova più difficili per il diritto penale del fatto e dell'offesa al bene giudico; perché le affermazioni, anche quando assumano la forma di "parole pericolose", si collocano idealmente sotto l'ombrello protettivo della libertà di manifestazione del pensiero tutelata dall'art. 21 Cost.; perché il fenomeno in sé presenta una grande duttilità (affermazione scritta, ripresa video, ma anche condivisione di post su socialnetwork, "like" a contenuto altrui, retweet, etc.) e un notevole potenziale diffusivo; perché i numeri del fenomeno mal si conciliano con la scarsità di risorse che caratterizza il procedimento più garantito che il nostro ordinamento concepisce, quello penale, appunto.

In secondo luogo e più in particolare, per le caratteristiche dello strumento che il codice penale appresta per contrastare il fenomeno: l'art. 604-*bis* cod. pen., sulle cui criticità è particolarmente opportuno soffermarsi in questo contesto.

Com'è noto, la disposizione in esame persegue e punisce, al primo comma, la condotta di chi: *a)* propaganda idee fondate sulla superiorità o sull'odio razziale o etnico; *b)* istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Più gravemente è, invece, sanzionata, al secondo comma, la condotta di chi: *c)* in qualsiasi modo istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi. Il terzo comma dell'art. 604-*bis*, infine, vieta ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per i medesimi scopi e stabilisce – sul modello delle fattispecie associative – pene differenziate per i meri partecipi e per gli organizzatori. Il quarto comma, infine, prevede una circostanza aggravante qualora la propaganda ovvero l'istigazione e l'incitamento – commessi in modo che derivi concreto pericolo di diffusione – si fondino in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale.

Senza poter qui procedere a una compiuta disamina di tutti gli aspetti problematici della disposizione, basti osservare che la norma appena ricordata peccherebbe – a giudizio della dottrina – tanto per difetto, quanto per eccesso.

Per difetto, perché nel nostro ordinamento la sfera di operatività dei crimini fondati su atti discriminatori è limitata alle discriminazioni per motivi razziali, etnici, nazionali o religiosi; con esclusione, dunque, di altre forme di discriminazione[1] – quali quelle motivata

[1] Fatta eccezione per l'eventuale applicazione a tali condotte dell'aggravante di cui all'art. 61 co. 1 n. 1 c.p., ossia "l'aver agito per motivi abietti e futili" e, limitatamente ai reati commessi ai danni di disabili, per la circostanza aggravante prevista dall'art. 36, comma 1 L.104/1992, come modificata dall'art.3, comma 1 L.94/2009.

dal sesso, dall'identità di genere, dall'orientamento sessuale e dalle disabilità[2] – che pure sono oggetto di tutela nella maggior parte degli ordinamenti europei[3].

Per eccesso, perché la formulazione della norma incriminatrice – per molti versi infelice – presta il fianco a critiche radicali, che ne denunciano l'imprecisione, l'indeterminatezza, l'inoffensività e che – in conseguenza di ciascuno di tali vizi – ne paventano l'indiscriminata applicazione.

Più precisamente, l'art. 604-*bis* c.p. si segnala, in primo luogo, per l'eccessiva vaghezza della locuzione "atti di discriminazione", che viene in rilievo laddove l'art. 604-*bis*, primo comma, lettera a), secondo periodo, persegue e punisce l'istigazione a commettere o, *tout court*, la commissione di atti di discriminazione (per motivi razziali, etnici, nazionali, religiosi). È stato trasversalmente osservato[4] che la nozione di discriminazione, così enunciata, appare imprecisa. La discriminazione assume significati e connotazioni diverse nei vari ambiti dell'ordinamento giuridico che adoperano tale termine e, comunque, così enunciata, è un concetto troppo 'esangue': incapace di identificare livelli minimi di gravità che giustifichino l'intervento penale. Con chiarezza è stata allora affermata la necessità per il legislatore di precisare quali atti di discriminazione siano meritevoli di sanzione penale, attraverso una tecnica il più possibile casistica[5].

In secondo luogo, eccessiva appare l'anticipazione della tutela che si registra laddove l'art. 604-*bis*, primo comma, lettera b, persegue e punisce non solo l'istigazione a commettere atti di violenza, ma anche l'istigazione a commettere atti di provocazione alla violenza. Si tratta, indubbiamente, di una istigazione all'istigazione che mal si coniuga con il principio di offensività in materia penale.

Da ultimo, ma non in ordine d'importanza, le fattispecie di "propaganda di idee fondate sulla superiorità o sull'odio razziale o etnico" (art. 604-*bis*, primo comma, lettera a), prima parte), di "istigazione a commettere atti di discriminazione" (art. 604-*bis*, primo comma, lettera a), seconda parte) e "istigazione a commettere atti di violenza" (per motivi razziali, etnici, nazionali, religiosi) (art. 604-*bis*, primo comma, lettera b) – a differenza di quelle che sanzionano la materiale commissione di atti di violenza o di discriminazione – pongono tutti i problemi tipici dei reati di opinione. Oltre a presentare sfide notevolissime dal punto di vista del bilanciamento costituzionale fra

[2] Senza pretese di completezza, si vedano E. Dolcini, *Omofobia e legge penale. Note a margine di alcune recenti proposte di legge*, in «Riv. it. dir. proc. pen.» (2011), pp. 24 ss.; Id., *Omofobi: nuovi martiri della libertà di manifestazione del pensiero?*, in «Riv. it. dir. proc. pen.» (2014), p. 7 ss; G. Riccardi, *Omofobia e legge penale. Possibilità e limiti dell'intervento penale*, in «Dir. pen. cont. – Riv. trim.», 3 (2013), pp. 84 ss.; M. Pelissero, *Omofobia e plausibilità dell'intervento penale*, in «GenIUS», 1 (2015), pp. 14 ss.

[3] In forma di circostanza aggravante (Albania, Slovacchia, Regno Unito, Danimarca, Finlandia, Francia) o di fattispecie autonoma (Paesi Bassi, Svizzera, Lituania, Ungheria, Lussemburgo) o di entrambe (Norvegia, Portogallo, Romania, Spagna, Svezia, Belgio). Sul punto si veda l'*Articolato gruppo di lavoro "Delitti contro l'Umanità e l'Uguaglianza" Proposta definitiva – 20 Aprile 2020*, predisposto dall'AIPDP, consultabile sul sito dell'associazione.

[4] Riassume, da ultimo, le critiche sul punto S. Prandi, *L'uguaglianza violata. Uno studio sull'atto discriminatorio nel sistema penale*, Torino, 2024.

[5] Ivi, pp. 138 ss.

la libera espressione e contro interessi pure dotati di rilevanza costituzionale come l'uguaglianza/pari dignità di tutti gli uomini, rappresenta un fondamentale banco di prova per il diritto penale del fatto o della tutela di beni giuridici. Il bene giuridico tutelato dall'art. 604-*bis* è costituito, come si è detto, dall'uguaglianza o dalla pari dignità dei soggetti appartenenti al gruppo oggetto di discriminazione. Sul postulato, che pare confermato dagli studi sociali, di una incidenza del discorso d'odio sulla comunità *target*, le cui condizioni di subordinazione culturale vengono per questa via ribadite e mantenute. La pari dignità del gruppo *target* è, tuttavia, un bene giuridico a spiccato carattere normativo-ideale: una situazione certamente 'carica di valore', nel contesto delle sempre più multiculturali società contemporanee ma, al contempo, 'povera di danni', quantomeno tangibili o empiricamente misurabili in modo univoco. Le dinamiche dell'offesa sono inoltre, in questa materia, verosimilmente seriali o cumulative. L'offesa descritta dall'art. 604-*bis* – mutuando la semantica dei beni ambientali – realizzi una sorta di inquinamento della società in cui viviamo da parte di messaggi che – goccia dopo goccia – sono in grado di produrre la lesione del macro-bene giuridico oggetto di tutela; e che, da sole, non potrebbero ledere un bene di tali dimensioni[6].

L'insieme delle criticità ora ricordate restituisce il quadro di una norma dai confini applicativi estremamente incerti. Una incertezza – si noti incidentalmente – che l'applicazione giurisprudenziale della norma ha solo parzialmente mitigato[7].

Vi è poi da considerare che la fattispecie in questione presenta un alto grado di 'sensibilità politica' ed è in grado di generare sentimenti di netta approvazione/riprovazione nel contesto culturale in cui si inserisce, alla luce della diversa sensibilità di chi si trovi ad applicarla. Nell'estrema difficoltà, se non nell'impossibilità, di realizzare un attendibile giudizio di concreta pericolosità della singola affermazione, forte potrebbe essere la tendenza a giudicare della pericolosità del fenomeno di cui l'affermazione si fa manifesto (razzismo, intolleranza religiosa, sessismo, omofobia), in un giudizio fortemente influenzato da una percezione soggettiva di necessità/inutilità dell'intervento penale. Con l'ulteriore conseguenza di realizzare, potenzialmente, quell' 'effetto di raggelamento' (*chilling effect*) che sempre si verifica quando una norma incriminatrice che sanziona l'espressione non sia in grado di selezionare con precisione l'ambito delle condotte punite o lo faccia con modalità che fanno sì che altre condotte, diverse da quelle che si volevano sanzionare, possano rientrarvi; con ciò realizzando, quale affetto collaterale, una deterrenza del discorso, invece, lecito ed anzi espressione di un diritto fondamentale.

[6] Per un riassunto, cfr. A. Galluccio, *Punire la parola pericolosa?, Pubblica istigazione, discorso d'odio e libertà di espressione nell'era di internet*, Milano, 2020, pp. 375 ss.

[7] Non vi è qui lo spazio per una compiuta disamina della giurisprudenza sul punto. Sia consentito allora rinviare a A. Galluccio, sub *art. 604-bis*, in G. Marinucci, E. Dolcini, G.L. Gatta, *Codice penale commentato*, VI ed., 2025.

3. *Il peculiare contesto del DSA:* private enforcement *e meccanismi di compliance*

Abbiamo tratteggiato, seppur per sommi capi, la struttura e le principali criticità dell'art. 604-*bis* c.p. allo scopo di individuare quali condotte perseguibili e punibili corrispondano, nel nostro ordinamento giuridico, alla definizione di *hate speech*. Tale mappatura dovrebbe poi fornirci le coordinate essenziali per stabilire in cosa consista un "contenuto illecito" rilevante ai sensi del DSA: tale, cioè, da attivare i meccanismi di compliance che tale strumento di regolazione predispone e le eventuali sanzioni correlate.

Si tratta, com'è noto, di una dettagliata disciplina di *due diligence obligations* relative, tra l'altro, alle attività di *private enforcement* dei contenuti immessi in rete dagli utenti svolta dagli operatori digitali, costruita con un sistema di obblighi strutturato a livelli di intensità crescente in base al particolare destinatario degli stessi. Si va dalla dimensione base delle previsioni applicabili a tutti i prestatori di servizi intermediari fino all'ultimo gradino concernente le più gravose regole applicabili alle piattaforme online e ai motori di ricerca di dimensioni molto grandi[8]. Limitandosi qui agli obblighi supplementari a carico delle *Very Large Online Platforms* (VLOPs)[9] e dei *Very Large Online Search Engines* (VLOSEs) – fra i quali si collocano i più importanti *social network* (Facebook e Twitter, etc.)[10] – vengono configurati nei confronti delle *corporations*: vari obblighi di *risk assessment* e di mitigazione dei rischi (fra cui un *crisis response mechanism*[11]), la sottoposizione a un *indipendent audit* almeno una volta l'anno e l'istituzione di una specifica *compliance function* al fine di monitorare la conformità dell'organizzazione agli obblighi sanciti dal nuovo regolamento. A tali obblighi corrispondono sanzioni e meccanismi di *enforcement* potenzialmente molto efficaci[12], tali da scongiurare i rischi di *cosmetic compliance*.

Si tratta – com'è stato osservato – di una "scelta di *policy* ben precisa: quella di puntare sugli stilemi, sui paradigmi, sugli strumentari ormai classici dell'era della *corporate compliance*, già sperimentati in qualche misura in altri regolamenti europei" ma "in modo ancor più deciso, disciplinando con un particolare livello di dettaglio […] i

[8] Per una disamina dell'intero sistema di *private enforcement* cfr. E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione degli operatori*, in «Medialaws», 2/13 (2023), pp. 52 ss.

[9] A norma dell'art. 33 DSA, *corporation* che hanno un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni.

[10] In base alla prima *designation decision* resa pubblica dalla Commissione il 2 aprile 2023 si è provveduto a designare come di dimensioni molto grandi 2 motori di ricerca (Bing e Google Search) e 17 piattaforme (Alibaba, AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando).

[11] L'art. 36 del DSA disciplina una procedura particolare destinata ad applicarsi, con riferimento a piattaforme online e motori di ricerca di dimensioni molto grandi, in condizioni di crisi definite espressamente come circostanze eccezionali che comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa.

[12] Per una panoramica delle sanzioni e dei meccanismi di *enforcement* si veda R. Sabia, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in «Medialaws», 2/13 (2023), pp. 88 ss.

criteri di valutazione e gestione dei rischi, l'architettura dei sistemi e delle metodologie di controllo interno, i meccanismi di cooperazione pubblico-privato specie nella risposta alle crisi[13]". In questo contesto, le società sono chiamate dal decisore pubblico a svolgere un ruolo proattivo, non privo però di notevoli margini di personalizzazione e adattamento. Il DSA, infatti, ben lungi dal fornire una positivizzazione analitica delle cautele imposte, riserva ai soggetti regolati un'ampia discrezionalità nel costruire le proprie regole interne, con un approccio che dalla dottrina è stato ritenuto riconducibile al concetto di *meta-regulation* o *enforced-self regulation*[14].

Chiare le esigenze utilitaristiche di tale *partnership* pubblico-privato: da un lato, le *corporations* si trovano nella posizione di prossimità ottimale rispetto al fenomeno oggetto della regolamentazione e dunque meglio comprendono i fattori di rischio e le loro possibili concatenazioni in direzione degli eventi avversi penalmente rilevanti; dall'altro lato, i 'privati' possono trovarsi nelle condizioni ottimali per esercitare un controllo ampio e continuativo, materialmente impossibile per gli organi statali e, quindi, contribuire incisivamente all'effettività e della regolazione delegata[15].

Insomma, la gestione e la mitigazione dei rischi sistemici degli ambienti digitali moderni – tali da mettere a repentaglio diritti fondamentali, quali la libertà di espressione, il pluralismo dei media, l'integrità dei processi elettorali, etc. – viene in larga parte affidata agli operatori di tali ambienti istituendo dinamiche di cooperazione istituzionalizzata tra pubblico-privato, strutturate sul modello della compliance. Alle più importanti *corporation* del mondo digitale è stato assegnato da DSA un non facile compito di autonormazione e autoorganizzazione in funzione preventiva che tuttavia – come è stato osservato[16] – deve essere esercitato entro i confini di una cornice pubblicistica di riferimento in grado di delineare con sufficiente precisione le regole del gioco.

4. *Incertezze relative all'ambito di applicazione della norma e logiche preventivo-precauzionali del* private enforcement*: una stretta mortale sulla libertà di espressione?*

Abbiamo osservato come il DSA affidi ad un modello di cooperazione pubblico-privato, strutturato sul modello della *corporate compliance*, il compito di gestire e mitigare i rischi sistemici degli ambienti digitali moderni. La scelta di *policy* rappresentata

[13] E. Birritteri, *Contrasto alla disinformazione*, cit., p. 71.

[14] Si veda ancora E. Birritteri, *Contrasto alla disinformazione*, cit., p. 75.

[15] Sviluppa questa riflessione, con riferimento al più generale contesto dell'autonormazione, D. Bianchi, *Autonormazione e diritto penale. Intersezioni, potenzialità, criticità*, Torino, 2021, p. 325 s.

[16] A. Gullo, *Contenuti, scopi e traiettoria della ricerca: le nuove frontiere della compliance nel mercato digitale*, *Sezione monografica "Il Digital Services Act e il contrasto alla disinformazione: responsabilità dei provider, obblighi di compliance e modelli di enforcement"*, in «Medialaws», 2 (2023), p. 13. Nello stesso senso, E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione degli operatori*, in «Medialaws», 2/13 (2023), p. 76.

dall'*enforced self-regulation* e, dunque, l'aver investito in prima battuta sui modelli di compliance che le singole società implementeranno è tale da incidere sulla struttura del controllo sull'accesso (e il mantenimento) dei contenuti in internet. Si tratterà, com'è ovvio, di logiche di tipo preventivo: la prevenzione è infatti il pilastro centrale di qualsiasi modello organizzativo efficace nell'ambito della compliance.

La natura dei rischi da fronteggiare, tuttavia – ispirata al meccanismo della causalità psicologica, tipico della parola pericolosa, e caratterizzato da un significativo margine di incertezza – orienterà verosimilmente le *corporation* verso l'adozione di regole che più che squisitamente preventive potrebbero assumere la forma di regole precauzionali.

In effetti, sebbene sussistano differenze strutturali fra principio di precauzione e causalità di tipo psicologico[17], la complessità dei temi evocati dal meccanismo della causalità psicologica – l'efficacia del mezzo della parola, che agisce non su un oggetto ma su un soggetto autoresponsabile, l'uso delle scienze sociali o di massime di esperienza nella costruzione dei meccanismi di causabilità – può di fatto condizionare l'ampiezza e la pervasività delle regole preventivo-precauzionali adottate.

Un altro fattore in grado di incidere nel senso di dilatare l'area dei rischi e, dunque, l'ampiezza delle condotte comunicative vietate è – come si è detto – l'indeterminatezza delle condotte perseguite e punite dall'art. 604-*bis* c.p. Le criticità dell'art. 604-*bis* c.p. in punto di precisione e offensività, infatti, non possono che ripercuotersi sul tentativo di individuare – proprio a partire da questa norma – cosa rappresenti un "contenuto illecito" rilevante ai sensi del DSA.

Si tratta di un margine di incertezza ritenuto intollerabile nel contesto della punizione dei fatti di *online hate speech* ma che – a giudizio di chi scrive – può rivelarsi esiziale per la libertà di manifestazione del pensiero in internet quando lo si trasli nel contesto della prevenzione dei reati e, più ancora, della prevenzione del privato secondo le logiche della *corporate compliance*. L'ampia discrezionalità delle *corporation* nella costruzione del modello di compliance, infatti, non pare essere bilanciata da una cornice pubblicistica in grado da fornire chiare regole del gioco. Viceversa, tanto la struttura della regolamentazione penale quanto le logiche della compliance paiono muovere verso una massiccia compressione del diritto a manifestare il pensiero online.

Il rischio – già evidenziato nel contesto della lotta alla disinformazione[18] – è quello di giustificare forme private di censura rispetto al libero dibattito pubblico, realizzate da attori privati privi di legittimazione democratica che – nel regolare, in assenza di una chiara cornice pubblicistica, le condizioni d'uso del servizio – possono liberamente influire sull'esercizio di libertà fondamentali del cittadino esercitando, quanto meno, un *chilling effect* del libero confronto se non una vera e propria repressione del dissenso democratico.

[17] Si veda per tutti L. Risicato, *La causalità psichica tra determinazione e partecipazione*, Torino, 2007, pp. 1 ss. e 73 ss.

[18] Cfr. A. Gullo, G. Piccirilli, *Disinformazione e politiche pubbliche: una introduzione*, in «Dir. pen. cont. – Rivista Trimestrale», 4 (2021), p. 249.

IL REATO DISCRIMINATORIO QUALE "ILLECITO ONLINE": COORDINATE DI DIRITTO INTERNO, COMPARATO ED EUROUNITARIO[1]

Andrea Perin

1. *Le condotte discriminatorie penalmente rilevanti*

Il dibattito in materia di diritto penale antidiscriminatorio è degno di interesse, per il giurista italiano, non solo con riguardo alle fattispecie già previste dall'ordinamento interno (principalmente agli artt. 604-*bis* e 604-*ter* c.p.)[2], ma anche alla luce degli strumenti adottati dall'Italia e dall'UE intesi a rafforzare il contrasto alla violenza discriminatoria[3], nonché in ragione della clausola antidiscriminatoria spesso presente nelle convenzioni internazionali contenenti obblighi di criminalizzazione[4].

[1] Il contributo elabora la relazione svolta dell'autore nell'ambito del convegno su "La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea", tenutosi presso il Dipartimento di Scienze Giuridiche dell'Università di Bologna (29 e 30 novembre 2024).

[2] Cfr., in Italia, anche per altri riferimenti, L. GOISIS, *Crimini d'odio. Discriminazioni e giustizia penale*, Jovene, Napoli, 2019; A. GALLUCCIO, *Punire la parola pericolosa? Pubblica istigazione, "discorso d'odio" e libertà di espressione nell'era di internet*, Giuffrè, Milano, 2020; S. PRANDI, *L'uguaglianza violata. Uno studio sull'atto discriminatorio nel sistema penale*, Giappichelli, Torino, 2024; A. PERIN, *Motivi aggravanti e circostanze discriminatorie. Legittimità e limiti della sanzione penale dell'offesa alla pari dignità*, Giappichelli, Torino, 2024, spec. pp. 104 ss. dove si indicano altre ipotesi riconducibili ai reati *lato sensu* discriminatori, per es. per l'applicabilità di circostanze aggravanti rispetto alle quali ciò che rileva non è il motivo/fine discriminatorio quale elemento psichico, bensì, oggettivamente, la circostanza che la persona offesa sia un target vulnerabile per la sua effettiva condizione di fragilità, oppure in ragione delle "relazioni strette" fra agente e vittima. Quanto alle diverse declinazioni categoriali dell'odio online, anche in considerazione del tipo di effetto-pericoloso qualificante, cfr. la panoramica di I. GAGLIARDONE, *Defining Online Hate and Its "Public Lives": What is the Place for "Extreme Speech"?*, in «Intern. J. Communication», 13 (2019), pp. 3068 ss.

[3] In materia di violenza di genere, intesa come specie di violenza discriminatoria, v. la *Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica* (cd. Convenzione di Istanbul, 2011); strumento già ratificato dall'Italia (L. 77 del 27 giugno 2013) e al quale dal 1° ottobre 2023 ha aderito l'UE. Cfr. inoltre la più recente *Direttiva 2024/1385 del Parlamento europeo e del Consiglio sulla lotta alla violenza contro le donne e alla violenza domestica*, del 24 maggio 2024.

[4] Per es., l'art. 2 della cd. Convenzione MEDICRIME (*Convenzione del Consiglio d'Europa sulla contraffazione dei prodotti sanitari e reati affini che rappresentano una minaccia per la salute pubblica*, Mosca, 2011), che prevede

Non è però agevole definire, di volta in volta, già con riguardo alle figure previste dal legislatore interno, i contorni di ciò che potremmo definire "tipicità discriminatoria"[5]; e il problema riemerge di fronte al Regolamento (UE) 2022/2065, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali (cd. *Digital Services Act*)[6], che, nel ricorrere ad una nozione ampia di «illecito online»[7], si riferisce anche al «discorso d'odio» e, più in generale, alle «azioni discriminatorie» che possano essere commesse in rete. Così, per es., già al *Considerando 12* troviamo un richiamo all'«illecito incitamento all'odio» e ai «contenuti discriminatori illegali»; mentre al *Considerando 40* si mette in rilievo l'opportuna adozione di strumenti a tutela degli «utenti particolarmente esposti al rischio di essere vittima di discorsi d'odio, molestie sessuali o altre azioni discriminatorie», fra cui i minori.

Ciò premesso, il presente contributo è inteso a offrire spunti in due direzioni. La prima parte (sez. 2-3) riguarda i controversi margini della tutela penale dell'eguaglianza alla luce dell'oggetto di tutela (principalmente con riguardo agli artt. 604-*bis* e 604-*ter* c.p., ma anche in ottica generale e comparatistica). In secondo luogo (sez. 4), qualche considerazione è dedicata a tecniche di tutela, rinvenibili in altre esperienze e dettate da strumenti sovranazionali, idonee a suggerire alternative all'impostazione che, in materia antidiscriminatoria e di tutela della vulnerabilità, promette protezione rafforzata mediante il ricorso a circostanze aggravanti[8].

obblighi di tutela penale in materia di contraffazione di prodotti sanitari e che sarà ripresa in seguito, recita quanto segue: *Principle of non-discrimination*: «*The implementation of the provisions of this Convention by the Parties, in particular the enjoyment of measures to protect the rights of victims, shall be secured without discrimination on any ground such as sex, race, colour, language, age, religion, political or any other opinion, national or social origin, association with a national minority, property, birth, sexual orientation, state of health, disability or other status*». Si rinvia ai contributi raccolti in AA.VV., *La Convenzione MEDICRIME sulla contraffazione dei prodotti sanitari e la tutela della salute pubblica in Italia*, in «Sist. pen.», n. spec., a cura di O. Alarcón-Jiménez, L. Masera, A. Perin, L. Salazar (2024).

5 Cfr. i contributi cit. *supra* in nota 2.

6 V., per una lettura d'insieme e altri riferimenti, A. TURILLAZZI, M. TADDEO, L. FLORIDI, F. CASOLARI, *The digital services act: an analysis of its ethical, legal, and social implications*, in «Law, Innovation and Technology», 15/1/83 (2023), spec. pp. 93 ss., 101-102, criticamente, sulla nozione indeterminata di «*illegal content*» («*the DSA is unclear whether the focus must be on illegal – and/or harmful – content. There is no clear definition of what is harmful and what is illegal*»), anche in considerazione delle diverse discipline (penalistiche) degli Stati dell'UE, e sull'approccio del *DSA* relativo agli obblighi di rimozione di tali contenuti (per es. perché ritenuti discriminatori o comunque di incitamento all'odio e/o alla violenza) di fronte al principio della libertà di espressione.

7 L'art. 3, lett. *h*, si riferisce invero alla vaga nozione di «*illegal content*» («contenuto illegale», nella versione italiana), con riguardo a «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto». V. la nota precedente.

8 In materia di circostanze, cfr. fra gli altri G. DE VERO, *Circostanze del reato e commisurazione della pena*, Giuffrè, Milano, 1983; A. MELCHIONDA, *Le circostanze del reato: origine, sviluppo e prospettive di una controversa categoria penalistica*, CEDAM, Padova, 2000; A. PECCIOLI, *Le circostanze privilegiate nel giudizio di bilanciamento*, Giappichelli, Torino, 2010; I. MERENDA, *Le circostanze del reato tra prevenzione generale e speciale*, Giappichelli, Torino, 2023.

2. *Che cos'è penalmente discriminatorio, che cosa non lo è: una discussione aperta*

Come si configura il diritto penale a tutela dell'eguaglianza?

La logica tradizionalmente sottesa al diritto antidiscriminatorio, anche quando applicata al diritto penale, risponde al seguente schema bi-fasico: il legislatore (si pensi agli artt. 604-*bis* e 604-*ter* c.p.) individua fattori discriminatori (razza o etnia, religione, nazione; volendo, *de lege ferenda*: sesso/genere, orientamento sessuale, identità di genere, disabilità, età, ecc.); e questi fattori, generalmente rilevanti sul piano dei moventi o dei fini sottesi alla condotta, vengono intesi a offrire una tutela rafforzata-selettiva alle persone appartenenti a gruppi o collettivi minoritari e/o vulnerabili.

Per cui, per es., pronunciare frasi gravemente offensive e minacciose con riferimento al colore della pelle, all'indirizzo di una persona di pelle nera, può integrare – oltre al fatto base (poniamo per ipotesi, una violenza privata), anche – l'aggravante dell'odio razziale. Mentre invece si esclude l'applicabilità del regime aggravato se la persona offesa, di pelle bianca, non appartiene ad un gruppo percepito come vulnerabile.

Perché?

Perché, secondo un orientamento che potremmo definire "tradizionale", in Italia prevalente, l'identità definita (anche) dall'essere bianco non sarebbe «correlata ad una situazione di inferiorità suscettibile di essere discriminata»; l'offesa, nel caso di frasi offensive all'indirizzo di una persona di pelle bianca, riguarderebbe soltanto «la persona singola verso la quale si abbia disistima», non il collettivo di riferimento, che non avrebbe alcun bisogno di tutela rafforzata[9].

Pertanto, in quest'ottica, non è la dignità del singolo (di chiunque) ad essere tutelata; bensì la *dignità associata alla vulnerabilità del gruppo* a cui appartiene la persona offesa (in base ad una sua certa caratteristica), una *dignità che si ritiene non sufficientemente riconosciuta* sul piano generale (sociologico, culturale) e che quindi richiede un intervento compensativo. L'obiettivo politico-criminale consisterebbe nel riequilibrare per mezzo della pena rapporti strutturalmente diseguali fra determinati gruppi umani (l'argomento è speso e ripetuto spesso, in letteratura, anche in materia di violenza di genere *contro le donne*). La pena, dunque, si presta ad essere intesa come "azione positiva" e ad essere ricondotta all'alveo dell'art. 3, co. 2, Cost. (l'eguaglianza sostanziale assumerebbe una funzione aggravante o criminalizzante)[10].

[9] Cass. pen., Sez. V, 28 gennaio 2010 (25 marzo 2010), 11590.

[10] Per una critica a questa impostazione, per certi versi paradossale, inutile e dai risvolti illiberali, contrari al principio di personalità della responsabilità penale (art. 27, co. 1, Cost.), si rinvia a quanto argomentato in PERIN, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 293 ss., spec. 304 ss.

3. *Spunti per un superamento dell'impostazione compensativa (e della logica binaria che separa "normale" e "diverso"): verso una ri-configurazione universalistica della tutela dell'eguaglianza?*

L'impostazione "tradizionale" pone almeno due classi di problemi.

All'atto pratico, attesi determinati fattori discriminatori (fattori la cui predeterminazione legislativa solleva, come noto, un dibattito in sé[11]), occorre definire: *a)* le *categorie soggettive vulnerabili* (per es.: gruppi etnici, identità di genere, gruppi religiosi, ecc.), e *b) chi* vi possa concretamente essere ricondotto, cioè le caratteristiche personali idonee a ricomprendere fatto e vittima all'interno dello spettro di tutela dell'eguaglianza.

Questo profilo, rilevante in sede di accertamento giudiziale, spiega – ma, a giudizio di chi scrive, non giustifica – la scelta del legislatore spagnolo, adottata mediante la *Ley Orgánica 8/2021*, di rendere imputabile l'aggravante antidiscriminatoria di cui all'art. 22.4 del *Código penal*, a prescindere dal fatto che le condizioni o circostanze a cui si riferiscono i motivi discriminatori sussistano effettivamente nella persona su cui ricade la condotta[12].

L'aggravante è infatti data dal:

> *Cometer el delito por motivos racistas, antisemitas, antigitanos u otra clase de discriminación referente a la ideología, religión o creencias de la víctima, la etnia, raza o nación a la que pertenezca, su sexo, edad, orientación o identidad sexual o de género, razones de género, de aporofobia o de exclusión social, la enfermedad que padezca o su discapacidad, con independencia de que tales condiciones o circunstancias concurran efectivamente en la persona sobre la que recaiga la conducta.*

Il motivo aggravante è quindi imputabile non solo benché non sia accertata l'appartenenza della vittima a un determinato gruppo discriminato per i motivi indicati dalla norma (accertamento richiesto dalla giurisprudenza spagnola prima della riforma), ma anche qualora il fattore identitario sia meramente *putativo*, in quanto ritenuto erroneamente esistente dall'agente. Sotteso a questa soluzione, quindi, si vede l'obiettivo di superare uno scoglio probatorio, altrimenti posto dalla necessità di dimostrare l'appartenenza della vittima ad un gruppo determinato (ciò che ancor prima impone la definizione di quali gruppi o collettivi siano riconducibili alla tutela promessa dal rilievo

[11] Anche su questo dibattito, per altri richiami, sia consentito rinviare a PERIN, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 118 ss.

[12] La prima versione dell'art. 22.4 c.p.es., introdotto dalla *LO 4/1995* (norma succeduta a sua volta all'art. 10.17 c.p.es. previgente), prevedeva che costituisse circostanza aggravante: «*Cometer el delito por motivos racistas, antisemitas u otra clase de discriminación referente a la ideología, religión o creencias de la víctima, la etnia, raza o nación a la que pertenezca, su sexo u orientación sexual, o la enfermedad o minusvalía que padezca*».

aggravante assegnato ad un determinato fattore discriminatorio) e di rendere applicabile l'aumento di pena anche in ipotesi di errore sull'identità della persona offesa[13].

Chiaramente, quindi, questa scelta svela che ciò che conta (giustificando, nella prospettiva del legislatore spagnolo, il regime più severo) è soltanto il *disvalore etico/morale del movente* e la riprovevolezza dell'intenzione[14]. Non vi è una maggiore offensività tangibile a fondare l'aumento della pena.

Sul piano teorico, a monte di soluzioni di questo genere, ci si può tuttavia legittimamente domandare se l'impostazione focalizzata sulla tutela del "diverso", della "minoranza", del soggetto "vulnerabile", sia obbligatoria, o comunque sempre accettabile e compatibile con una corretta declinazione dell'oggetto di tutela. Si tratta di un profilo particolarmente delicato in termini astratti, ma anch'esso presenta notevoli risvolti pratici.

La matrice dell'oggettività giuridica di riferimento, in effetti, non è affatto chiara.

Il codice penale italiano qualifica le figure di cui agli artt. 604-*bis* e 604-*ter* c.p. come delitti contro l'eguaglianza e le inserisce fra i delitti contro la libertà individuale. L'impostazione adottata dal legislatore suggerisce quindi che i *delitti contro l'eguaglianza* possono essere intesi come *delitti contro la libertà*.

In letteratura si ricorre talvolta, in vario modo, all'idea dell'integrità collettiva, per cui la tipicità discriminatoria (a seconda delle figure di riferimento) sarebbe segnata dall'idoneità della condotta a generare il rischio di una successiva escalation di violenza ai danni delle persone appartenenti ai gruppi discriminati; e anche a generare in altri componenti di quel gruppo (minoritario, vulnerabile, protetto) il timore di essere vittime di reati simili. Quindi*:* ci si muove sul terreno di un pericolo poco concreto e guardando a un bene giuridico che assume le sembianze dell'ordine pubblico (del resto, l'ordine pubblico è richiamato anche dall'art. 8, sulla *Istigazione alla violenza o all'odio online*, della citata Direttiva 2024/1385, sulla lotta alla violenza contro le donne e alla violenza domestica).

Ciò premesso, pare lecito domandarsi se la tutela penale della *pari dignità* possa invece riguardare *chiunque*, a prescindere dal gruppo o dai collettivi di appartenenza, benché soltanto per certe ragioni predefinite dal legislatore (i fattori discriminatori). La

[13] Cfr. la sent. del *Tribunal Supremo*, n. 66/2022, cit. da A. Doval Pais, *Víctima del delito y víctima de la discriminación. La relevancia de la víctima en la circunstancia agravante del art. 22.4ª del Código Penal*, in «Rev. victimología», 18/133 (2024), p. 153.

[14] Sul rapporto fra motivi aggravanti e colpevolezza, cfr. anzitutto P. Veneziani, *Motivi e colpevolezza*, Giappichelli, Torino, 2000, pp. 318-319 e *passim*, il quale argomenta e sostiene l'idoneità dell'indagine motivazionale ad «illuminare il significato del fatto», «colorandolo in termini di maggiore o minore disvalore» (purché, specifica l'autore, detta valutazione non valga «per altre caratteristiche dell'autore, avulse rispetto al fatto: esempio, il carattere»); per argomenti ritenuti invece idonei a escludere il rilievo autonomo dei motivi abietti sul piano della colpevolezza e della pena, Perin, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 151 ss., spec. 195 ss.; in sintesi, si tratterebbe di considerare il carattere assorbente del dolo (*ne bis in idem*) e, se del caso, il rilievo possibilmente attenuante o scusante della personalità socio-culturalmente immatura mostrata dall'inclinazione motivazionale dell'autore del fatto (cfr. Corte cost. 364/1988, specie con riguardo al rilievo dell'art. 3, co. 2, Cost).

questione, in altri termini, consiste nel chiedersi se un'aggravante come quella prevista all'art. 604-*ter* c.p., e figure come quelle coperte dall'art. 604-*bis* c.p., possano essere applicate anche a fatti commessi a danno di chi non appartenga a gruppi "minoritari" o "vulnerabili"; o in contesti nei quali quel determinato collettivo non appaia in quanto tale vulnerabile. Le due persone di cui sopra, quella di pelle bianca e quella di pelle nera, verrebbero tutelate penalmente alle stesse condizioni. E sul piano comunicativo la pena agirebbe in senso egualitario, non in senso compensativo.

L'ipotesi affacciata, intesa a evitare discriminazioni alla rovescia sul piano penalistico (non dimentichiamo che grazie all'art. 27 co. 1 Cost. la responsabilità penale è personale, non identitaria), si scontra però con la giustificazione tradizionale di questa classe di tutela, che viene per lo più ricondotta alla necessità di protezione rafforzata e compensativa – la pena come "azione positiva" – a favore delle persone appartenenti a certi gruppi (atteso, si badi bene, soltanto un loro carattere identitario).

3.1. *Una re-interpretazione "universalistica" (neutra sul piano identitario) è ostacolata da ragioni di diritto positivo?*

Dipende.

Alcune disposizioni penali antidiscriminatorie (si pensi per es. alle ipotesi di incitamento o istigazione di cui all'art. 510 c.p. spagnolo; ai fatti discriminatori in senso stretto puniti ai sensi degli artt. 511, 512, 314 dello stesso c.p.es.; oppure, alle figure di "femminicidio" disciplinate come fattispecie autonome o configurabili mediante la previsione di circostanze aggravanti motivazionali applicabili al tipo-base di omicidio[15]) indicano fattori discriminatori – rilevanti sul piano dei fini o dei moventi – costruiti attorno a *gruppi umani concreti e specifici* (non solo a categorie di pregiudizi): per es. l'*antisemitismo* (contro gli ebrei), l'*antiziganismo* (contro i popoli rom, sinti o altri gruppi), o la *aporofobia* (contro le persone prive di mezzi materiali).

In questi casi non c'è spazio per interpretazioni alternative: la tutela rafforzata non riguarda genericamente il discorso o il fatto razzista (mosso da razzismo o con fine razzista, a seconda dei casi) commesso nei confronti di chicchessia, ma il discorso o il fatto commesso contro la persona ebrea, contro la persona rom, contro la persona priva di mezzi.

Altre norme però – è il caso per es. del codice italiano – sono *neutre sul piano identitario*, perché associano la rilevanza del discorso o del fatto discriminatorio (604-*bis* c.p.) o l'inasprimento della pena (604-*ter* c.p.) a un certo *fattore o motivo o fine* discriminatorio *generalizzabile*. Per cui la scelta interpretativa di ritenere tipica o aggravata l'offesa *solo* se rivolta ad una persona nera e non anche se rivolta contro una persona bianca (laddove il fattore rilevante sia l'etnia o la razza) è discutibile ed emendabile.

[15] Per alcune annotazioni ulteriori su questi riferimenti normativi, si rinvia nuovamente a PERIN, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 83 ss. Sul "femminicidio", v. *infra*, nota 21.

3.2. (Segue) *Oppure da ragioni concettuali dirimenti?*

Qui il discorso si fa più complesso e si tratta di capire se, laddove non vi siano ostacoli sul piano del diritto positivo oppure *de iure condendo*, vi sia spazio per riflettere sull'opportunità di applicare l'apparato sanzionatorio a tutela dell'eguaglianza *anche* al fatto commesso, per es., per ragioni legate al sentimento religioso, pur quando quel tratto culturale, che definisce l'identità della vittima, sia *prevalente* o *non minoritario* o *non generalmente/strutturalmente discriminato* in un contesto sociale e/o in un momento storico determinato.

L'ipotesi sarebbe quella di configurare una tutela penalistica non più riferibile solo a identità contestualmente "protette" (la tutela del "diverso"), perché tutelata sarebbe qualunque identità, ma solo per certe ragioni predefinite dal legislatore (per es.: origine, etnia o nazionalità, condizione socioeconomica, età o abilità, religione, cultura politica e identità sessuale)[16].

Quali possibili argomenti in questa direzione?

Una ragione riguarderebbe il contenuto della "pari dignità" quale oggetto di tutela, il cui senso potrebbe essere colto, non tanto nella presunta/strutturale vulnerabilità su base identitaria, bensì nel principio di autodeterminazione quale obiettivo "mediato" dalla tutela "mediante" delle pari opportunità: tutelata sarebbe la "*libertà di*" (essere chi si è) in una società pluralistica nella quale – almeno con riguardo ad alcuni fattori – "*normale*" e "*diverso*" smettano di esistere[17].

E poi, all'atto pratico, si supererebbero anche aporie evidenti derivanti dall'applicazione delle logiche antidiscriminatorie al diritto penale: aporie che si mostrano nel momento in cui si pretende di applicare un trattamento differenziato (aggravante) in base alla probabilità presunta che un individuo, ricondotto ad un certo gruppo per una sua caratteristica fra molte, abbia di essere vittima di un certo tipo di illecito. Giustamente ci si chiede: dovremmo «condannare lo stupratore [eterosessuale] Tizio ad una pena più consistente perché le sue vittime sono soltanto donne, e il suo quindi è considerato anche un atto sessista, contro le donne, mentre invece dovremmo condannare ad una pena più lieve lo stupratore bisessuale Caio, anche se il numero di vittime di violenza è il medesimo per Tizio e Caio»?[18]

[16] Così, nella proposta di riformulazione – sul terreno di un'offensività tangibile – avanzata Ivi, p. 312, secondo cui sarebbe configurabile la circostanza aggravante «*[…] se il fatto è commesso cagionando volontariamente una coercizione della persona offesa, la quale, a prescindere dal gruppo o collettivo di appartenenza, risulti concretamente discriminata per la sua origine, etnia o nazionalità, per la sua condizione socio-economica, età o abilità, per la sua religione, cultura politica o identità sessuale*».

[17] Ivi, pp. 286 ss.

[18] G. Maniaci, *Aporie e distorsioni del femminismo radicale*, in «Dir. & Quest. pubbl.», 16/2, pp. 342-343.

4. *Tutela dell'eguaglianza e protezione della vulnerabilità*

Quanto detto però non porta ad escludere la possibilità, in alcune ipotesi, di configurare forme di tutela "dedicata" e basata sulla individuazione di categorie vulnerabili. L'ipotesi di studio, piuttosto, potrebbe essere quella di separare – e configurare diversamente sul piano del diritto positivo – due ambiti distinti di tutela (che oggi vengono generalmente confusi o sovrapposti):

a) da una parte, quello della *tutela antidiscriminatoria*, cioè della tutela della "pari dignità" come eguale autodeterminazione, a prescindere dall'appartenenza della persona offesa ad un gruppo/collettivo "protetto";
b) dall'altra, quello della *tutela della vulnerabilità*, che invece può opportunamente riferirsi a gruppi "protetti"; e il *DSA*, per quanto qui interessa, mette un accento pronunciato sulla tutela dei minori, quali utenti particolarmente esposti al rischio di essere vittime di discorso d'odio, molestie o altre condotte discriminatorie online (già ai *Considerando 40, 62* e *104*, e poi all'art. 28).

Su questo secondo terreno si tratta di riflettere su quale possa essere la tecnica di tutela più sensata.

Sul piano penalistico-sanzionatorio, l'interrogativo riguardante la tecnica più opportuna a protezione della "vulnerabilità" potrebbe essere posto nei seguenti termini: *che cosa significa offrire "tutela rafforzata"?*

Tradizionalmente, al di là del ricorso a figure *ad hoc*, come il delitto di circonvenzione di incapaci (art. 643 c.p.), si procede mediante la previsione di circostanze aggravanti[19], quindi la tutela appare "rafforzata", in ottica general-preventiva, ma anche simbolico-comunicativa, perché più severo è il regime sanzionatorio associato a un illecito *se qualificato* dall'offesa a una persona vulnerabile (o dal suo coinvolgimento). Questo cammino è preso, per es., nel prevedere l'aggravante comune di cui all'art. 604-*ter* c.p.; nonché le ulteriori aggravanti rispetto alle quali ciò che rileva è la fragilità della persona offesa[20]; oppure, tramite la previsione di fattispecie autonome qualificate e aggravante, rispetto alla figura base, dall'identità della vittima – in quanto appartenente ad un gruppo/collettivo storicamente discriminato – e dal sotteso movente discriminatorio (è il caso, di nuovo, del delitto di "femminicidio", previsto da tempo in alcuni ordinamenti – generalmente quale uccisione dolosa di una donna qualificata

[19] Sulle numerose ipotesi aggravanti previste a tutela del minore, rappresentando criticamente un quadro normativo scoordinato e disorganico, v. D.M. Schirò, *Circostanze del reato e tutela del minore*, in «Riv. it. dir. proc. pen.», 1 (2020), p. 107, spec. pp. 111 ss.

[20] Si pensi all'aggravante di cui all'art. 61, co. 1, n. 5, c.p., data dall'aver «profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età [elemento inserito dalla stessa L. 94/2009], tali da ostacolare la pubblica o privata difesa»; quella di cui al n. 11-*ter*, data dall'aver «commesso un delitto contro la persona ai danni di un soggetto minore all'interno o nelle adiacenze di istituti di istruzione o di formazione»; il n. 11-*quinquies*, imputabile per «avere, nei delitti non colposi contro la vita e l'incolumità individuale e contro la libertà personale, commesso il fatto in presenza o in danno di un minore di anni diciotto ovvero in danno di persona in stato di gravidanza».

dal *motivo di genere*, talvolta quale reato proprio dell'agente di sesso maschile – e ora introdotto anche in Italia)[21].

Una figura rilevante in questo senso è quella prevista all'art. 153.1 c.p. spagnolo, che prevede una forma aggravata (ma limitatamente al minimo edittale) di maltrattamenti e percosse[22] applicabile, fra l'altro

> *cuando la ofendida sea o haya sido esposa, o mujer que esté o haya estado ligada a él* [l'autore del fatto] *por una análoga relación de afectividad aun sin convivencia.*

Tuttavia, esistono alternative (all'inasprimento del regime sanzionatorio), tra le quali quella di ricorrere – non all'effetto aggravante, bensì – a un arretramento della soglia del pericolo come elemento di tipicità.

Un esempio significativo si rinviene nuovamente nel codice penale spagnolo (c.p.es.), laddove è stato riformato per dare attuazione alla citata Convenzione MEDICRIME del Consiglio d'Europa in materia di falsificazione di prodotti sanitari e tutela della salute pubblica[23].

La figura di riferimento è quella prevista dall'art. 361-*bis* c.p.es., aggiunta dalla *Ley orgánica 8/2021*, che si inserisce in un apparato di disposizioni incriminatrici relative a condotte di produzione e commercio di prodotti sanitari contraffatti accomunate dal requisito del pericolo concreto o quantomeno "astratto-concreto" (richiedendo che si «*genere un riesgo para la vida o la salud de las personas*»[24]).

[21] Dalla L. 2 dicembre 2025, n. 181, che prevede il nuovo art. 577-bis c.p. Sul carattere per nulla liberale e men che meno solidaristico di questa figura aggravante, inutile sul piano preventivo-repressivo e paradossale su quello comunicativo, configurata anche nello schema di d.d.l. approvato dal Consiglio dei Ministri n. 117 del 7 marzo 2025 (nuovo art. 577-*bis* co. 1 c.p., previsto dall'art. 1), facendo leva su una categoria di motivi abietti («… quando il fatto è commesso come atto di discriminazione o di odio verso la persona offesa in quanto donna o per reprimere l'esercizio dei suoi diritti o delle sue libertà o, comunque, l'espressione della sua personalità»), cioè "motivi di genere" o fini di discriminazione di genere, e punibile con l'ergastolo, sia consentito rinviare alle considerazioni svolte, in chiave comparatistica, in PERIN, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 7 ss., 20 ss. (sul nesso storico-concettuale fra motivi e pericolosità), 123 ss. (sul cd. motivo di genere), 140 ss. (sulle ipotesi aggravate vigenti già riconducibili al medesimo ambito criminologico), 188 ss. (criticamente sulle tesi che giustificano l'effetto aggravante dei motivi sul piano della concezione normativa della colpevolezza), 308 ss., spec. 316-317 (contro la configurabilità di una fattispecie autonoma di omicidio-qualificato aggravata da motivi/fini o da effetti discriminatori).

[22] Al riguardo, per ulteriori note critiche e riferimenti, PERIN, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 88 ss. Si noti che la fattispecie-base (art. 153.2 c.p.es.) richiede comunque che fra agente e vittima vi siano (stati) rapporti stretti.

[23] V. *supra*, nota 4. Inoltre, nella manualistica spagnola, S. ROMEO MALANDA, *Delitos contra la seguridad colectiva II. Delitos contra la salud pública*, in *Derecho penal. Parte especial*, a cura di C.M. Romeo Casabona, E. Sola Reche, M.A. Boldova Pasamar, Comares, Granada, 2023[3], pp. 671 ss., 677 ss., specie sulla riforma attuata dalla *Ley orgánica 2015/1* all'apparato dei cd. «*delitos farmacológicos*» (artt. 361, 362, 362-*bis*, 362-*ter*, 362-*quater*, c.p.es.).

[24] Per es., l'art. 361 c.p.es., che riguarda le ipotesi di medicinali non autorizzati o quelli (originariamente genuini) deteriorati, e punisce (con la reclusione da 6 mesi a 3 anni, una sanzione pecuniaria e l'interdizione dalla professione o dall'ufficio da 6 mesi a 3 anni) chiunque «*fabrique, importe, exporte, suministre, intermedie, comercialice, ofrezca o ponga en el mercado, o almacene con estas finalidades, medicamentos, incluidos los de uso humano y veterinario, así como los medicamentos en investigación, que carezcan de la necesaria autorización exigida por la ley,*

L'art. 361-*bis* c.p.es. riguarda invece condotte contro persone vulnerabili (per età o disabilità) e punisce (in modo relativamente meno severo rispetto ad altre fattispecie: con pena pecuniaria e con la reclusione da 1 a 3 anni) la diffusione online di contenuti diretti a promuovere il consumo, fra minori e disabili, di prodotti (*productos, preparados o sustancias o la utilización de técnicas de ingestión o eliminación de productos alimenticios*) «*cuyo uso sea susceptible de generar riesgo para la salud de las personas*»[25].

Da notare, al riguardo, due aspetti: l'attinenza, pacifica, di questa figura alla nozione ampia di «contenuto illecito online» (il *Considerando 12* del *DSA* fa esplicito riferimento anche alla «vendita di prodotti non conformi o contraffatti»; il *Considerando 80* ai «prodotti pericolosi o contraffatti»); inoltre, in ragione delle condotte sanzionate e del tipo di vittima, il pericolo richiesto è di tipo astratto: basterebbe infatti l'*idoneità a generare pericolo per la salute delle persone.* La tutela "anticipata" è, quindi, potremmo dire, *collettivamente selettiva* in quanto configurata in funzione di *categorie di vittima.*

5. *Coordinate di tipicità discriminatoria a tutela della pari dignità e a protezione della vulnerabilità*

Da questi appunti pare possibile, in conclusione, indicare due possibili coordinate generali utili a guidare la configurazione positiva e interpretativa della "tipicità discriminatoria", anche quale residuale e composito sottoinsieme-intersezione della "illiceità online".

Da un lato, emerge la possibilità di intendere in senso universalistico la tutela dell'eguaglianza di cui agli art. 604-*bis* e *ter* c.p. (una tutela neutra sul piano identitario, ma predefinita quanto ai fattori rilevanti): il che implica una potenziale espansione di quella "tipicità discriminatoria"[26], che andrebbe bilanciata – e in realtà notevolmente

o productos sanitarios que no dispongan de los documentos de conformidad exigidos por las disposiciones de carácter general, o que estuvieran deteriorados, caducados o incumplieran las exigencias técnicas relativas a su composición, estabilidad y eficacia», richiede inoltre che la condotta «*genere un riesgo para la vida o la salud de las personas*».

[25] La fattispecie punisce la «*distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover o facilitar, entre personas menores de edad o personas con discapacidad necesitadas de especial protección, el consumo de productos, preparados o sustancias o la utilización de técnicas de ingestión o eliminación de productos alimenticios cuyo uso sea susceptible de generar riesgo para la salud de las personas*».

[26] Il rischio sotteso al modello "selettivo", che promette tutela rafforzata a determinati gruppi (minoritari, vulnerabili, discriminati), è quello di mettere in secondo piano il disvalore del fatto basato su ragioni discriminatorie e di assegnare implicitamente – o di avallare letture in base alle quali i loro membri sarebbero titolari di – una dignità qualificata all'appartenenza al gruppo o collettivo. Ecco perché il «diritto penale antidiscriminatorio, se non applicabile *a tuttə e a tutela di tuttə*, ancorché *solamente per le ragioni identificate dal legislatore*, diviene uno strumento esso stesso irragionevolmente discriminatorio: a danno degli *autori* di fatti riconducibili alla tutela rafforzata, da una parte; e delle *vittime* di fatti offensivi che, non appartenendo a gruppi protetti o non essendo inquadrate da generalizzanti fotografie criminologiche e automatizzanti massime di esperienza, non si vedono riconosciuta la medesima dignità, dall'altra» (Perin, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 120, 301-302).

limitata – dalla selezione delle sole figure dell'art. 604-*bis* c.p. compatibili con il canone di concreta offensività[27] e tenendo conto della definizione del bene giuridico in rilievo come eguale autodeterminazione[28].

Dall'altro, si coglie la possibilità di anticipare la soglia della rilevanza penale del fatto, quando si tratti di target vulnerabili (per età o abilità): quindi, anche qui, avremmo una espansione "collettivamente selettiva" dell'ambito di "tipicità discriminatoria", mediante arretramento della soglia del pericolo rilevante (a tutela della salute pubblica); espansione mirata che, come ha opportunamente fatto il legislatore spagnolo (art. 361-*bis* c.p.es.), andrebbe bilanciata sul piano del regime sanzionatorio, calibrandolo al ribasso.

[27] Su questa discussione, cfr. gli Atti pubblicati in AA.VV., *La riforma dei delitti contro la persona. Proposte dei gruppi di lavoro dell'AIPDP. Atti dei seminari di discussione in collaborazione con il DiPLaP*, Edizioni DiPLaP, 2023, pp. 762 ss.; inoltre, GALLUCCIO, *Punire la parola pericolosa?*, cit., *passim*; PRANDI, *L'uguaglianza violata*, cit., *passim*.

[28] La riconfigurazione dei delitti di parola di cui all'art. 604-*bis* c.p. potrebbe seguire, *mutatis mutandis*, la proposta *de lege ferenda* elaborata con riguardo all'art. 604-*ter* c.p. in PERIN, *Motivi aggravanti e circostanze discriminatorie*, cit., pp. 307 ss., spec. 312 (*supra*, nota 16).

PUNIRE LA MENZOGNA "POLITICA" NELLO SPAZIO VIRTUALE? IL RUOLO DEL DIRITTO PENALE NEL CONTRASTO ALLA DISINFORMAZIONE E ALLA MANIPOLAZIONE DEL CONSENSO ELETTORALE

Anna Costantini

1. *Le nuove dinamiche della disinformazione nel cyberspazio: tra post-verità,* social network *e intelligenza artificiale*

Tra i contenuti circolanti nell'etere virtuale, che sembrano manifestare un bisogno d'attenzione da parte del diritto penale, una considerazione particolare meritano quelli di tipo disinformativo. Anche la *notizia falsa* potrebbe, infatti, rientrare nel perimetro del materiale digitale *pericoloso* rispetto a cui riferire non solo l'operatività dei nuovi meccanismi di rimozione e sanzione predisposti a livello europeo, ma persino la reazione punitiva, come già avvenuto in alcuni ordinamenti esteri e come ripetutamente oggetto di discussione a livello parlamentare interno.

A sollecitare l'interesse penalistico, in particolare, è il fenomeno dell'impiego delle c.d. *fake news* – termine impropriamente invalso nel linguaggio giornalistico e comune per indicare la disinformazione online – quale strumento di manipolazione delle decisioni di voto dei cittadini, soprattutto nel quadro di campagne propagandistiche orientate da forze politiche o da Stati esteri con l'obiettivo di distorcere i processi elettorali democratici e destabilizzare le istituzioni interne.

Certo il problema del condizionamento dell'opinione pubblica tramite la deliberata falsificazione di notizie precede la nascita di *internet*, dei *social media*, dell'intelligenza artificiale, ma attiene allo stesso rapporto tra potere e informazione[1]: eppure, l'imporsi della dimensione "virtuale" dello spazio in cui si svolgono gli scambi comunicativi ha mutato l'essenza del fenomeno, o almeno la sua percezione. Da un lato, infatti, lo

[1] Evidenzia le interazioni tra reti informative e strutture di potere (democratiche o autoritarie), in prospettiva storica, Y.N. HARARI, *Nexus. Breve storia delle reti di informazione dall'età della pietra all'IA*, trad. it., Bompiani, Milano, 2024.

spostamento del "cuore" dei processi informativi (ma anche delle stesse campagne elettorali) nell'agorà digitale ha trascinato al suo interno buona parte dei tentativi di inquinamento del dibattito politico e della pubblica opinione; dall'altro, nelle maglie della rete sembrano annidarsi pericoli inediti di manipolazione del pensiero individuale e collettivo, tanto da compromettere le stesse fondamenta delle società democratiche[2].

Sono diversi i fattori che spiegherebbero questa più accentuata insidiosità della disinformazione "di ultima generazione", rispetto a quella tradizionale[3]: i *social network* aumentano la quantità e la velocità di propagazione delle notizie false, rese immediatamente disponibili a un enorme numero di persone a livello globale; i contenuti immessi in rete possono sottrarsi al filtro di "intermediazione" del giornalismo qualificato[4], a sua volta depotenziato da una diffusa crisi di credibilità; al contempo, la stessa promessa dell'aprirsi di uno spazio libero per le idee (un *free marketplace of ideas*) che aveva accompagnato la nascita di *internet* sembra ormai tradita dal prevalere di logiche oligopolistiche e di condizionamento da parte di poteri politici ed economici[5].

A quanto detto si aggiunge la maggiore permeabilità all'inganno di chi riceve le informazioni, una sorta di diffusa propensione del pubblico a credere alle falsità e a dubitare delle verità. Le decisioni di voto si affidano in prevalenza a impulsi emozionali e narrazioni polarizzate, mentre aumentano la sfiducia nei confronti del pensiero scientifico e il rifiuto delle "verità" bollate come ufficiali. Si tratta di processi forse epocali – così, almeno, sostengono i teorici della "post-verità"[6] – e che travalicano il rapporto con il mondo digitale, ma trovano in quest'ultimo un terreno fertile per il loro ulteriore approfondirsi. Per un verso, infatti, la profilazione algoritmica chiude gli utenti in "bolle" selettive, camere dell'eco disegnate per far filtrare solo le verità desiderate e rafforzative di opinioni preesistenti[7], sfruttando il meccanismo psico-

[2] S. Sassi, *Disinformazione e costituzionalismo*, Napoli, Edizioni Scientifiche Italiane, 2021; M. Ruotolo, *Riflessioni interlocutorie su verità, fiducia e democrazia rappresentativa. Si può combattere la menzogna nel c.d. mercato politico?*, in «Diritto e società», 1 (2022), pp. 43 ss.

[3] Li si richiama qui solo brevemente e senza pretesa di esaurire la complessità del fenomeno. Diffusamente sul tema v. T. Guerini, Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020, pp. 20 ss. Si rinvia anche all'analisi criminologica di A. Visconti, *Alcune considerazioni criminologiche e politico-criminali sulle c.d. 'Fake News'*, in «JUS», 1 (2020), pp. 43 ss.

[4] Sulla c.d. disintermediazione dell'informazione P. Stringa, *Che cos'è la disintermediazione*, Roma, Carocci, 2017. Osserva come internet abbia mutato l'assetto dell'informazione G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in «Rivista di diritto dei media», 1 (2018), pp. 22 ss.

[5] Osserva come, nell'epoca di internet, il mercato delle idee sia tutt'altro che libero, O. Pollicino, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in *Parole e potere. Libertà di espressione,* hate speech *e* fake news, a cura di G. Pitruzzella, O. Pollicino, S. Quintarelli, Milano, Egea editore, 2017, p. 49. La prospettiva del potere delle piattaforme è indagata, in prospettiva costituzionalistica, da F. Paruzzo, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Napoli-Torino, ESI, 2022.

[6] Su cui v. M. Ferraris, *Postverità e altri enigmi*, Bologna, il Mulino, 2017; A.M. Lorusso, *Postverità*, Editori Laterza, Roma-Bari, 2018; L. Mcintyre, *Post-Truth*, Cambridge, 2018.

[7] A. Nicita, *Il mercato delle verità. Come la disinformazione minaccia la democrazia*, il Mulino, Bologna, 2021, pp. 7 ss., che stravolge la metafora del "*free marketplace of ideas*" della tradizione liberale sostituendola con quella di "un *mercato delle verità*", all'interno del quale si domandano e si offrono "fatti verosimili" che sanno suscitare emozioni e che corrispondono alle nostre "verità desiderate" (p. 11).

logico dei *confirmation bias*[8]. Per altro verso, l'uso dei mezzi tecnologici incentiva il "pensiero veloce"[9] nel rapportarsi alle enormi masse di dati che si riversano sui *social network*, e impatta sui meccanismi cognitivi che determinano la formazione delle opinioni (si è parlato di stupidità indotta da internet, e talvolta di vera e propria "demenza digitale"[10]). Elemento ulteriore, non di poco conto, viene dallo sviluppo della intelligenza artificiale c.d. generativa[11], che potrebbe alterare lo stesso rapporto con la verità: sia perché costituisce uno strumento di *verità fallibile* (un congegno con vesti oracolari che può però produrre errori di cui gli utenti sono inconsapevoli), sia perché diventa un formidabile strumento di fabbricazione di *falsità verosimili* (pensiamo ai *deepfake*). In definitiva consolida quella percezione, tipica della post-verità, di sfiducia generalizzata nella stessa possibilità di distinguere tra realtà e finzione, tra verità e falsità: in un mondo dove tutto può essere falso, nessuna notizia è più vera o quantomeno può essere creduta tale.

Questo quadro spiega la crescente discussione intorno alla possibilità di introdurre meccanismi di regolamentazione (o auto-regolamentazione) della rete, orientati a contrastare la circolazione di contenuti falsi, soprattutto nei periodi pre-elettorali, quando a essere minacciata è la stessa genuinità delle opinioni espresse nel voto. In questo quadro, anche il piano della *repressione penale* viene chiamato in causa tra le possibili strategie con cui lo Stato si propone di presidiare la "purezza" dell'agorà virtuale. Si tratta, dunque, di interrogarsi su quale possa essere il ruolo (se vi sia) e quali siano i limiti di una tutela penale della "verità" dell'informazione all'interno dello spazio digitale[12].

[8] D. Palano, Bubble Democracy. *La fine del pubblico e la nuova polarizzazione*, Editrice Morcelliana, Brescia, 2020; W. Quattrociocchi, A. Vicini, *Misinformation. Guida alla società dell'informazione e della credulità*, Franco Angeli, Milano 2016; più di recente, degli stessi autori, *Polarizzazioni. Informazioni, opinioni e altri demoni nell'infosfera*, Franco Angeli, Milano, 2023.

[9] Per richiamare la categoria elaborata da D. Kahneman, *Pensieri lenti e veloci* (2011), trad. it. di L. Serra, Milano, Mondadori, 2012.

[10] N. Carr, *Internet ci rende stupidi? Come la Rete sta cambiano il nostro cervello*, Raffaello Cortina Editore, Milano, 2011; M. Spitzer, *Demenza digitale*, trad. it. M.A. Petrelli, Corbaccio, Milano, 2019.

[11] In argomento, O. Pollicino, P. Dunn, *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*, Egea, Milano, 2024.

[12] Sia consentito rinviare, per ulteriori considerazioni, ad A. Costantini, *Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso*, in «Diritto penale contemporaneo-Rivista trimestrale», 2 (2019), pp. 60 ss. Tra i contributi che si interrogano sul tema, è centrale il lavoro monografico di T. Guerini, *Fake news e diritto penale*, cit.; v. inoltre C. Perini, Fake news *e post-verità tra diritto penale e politica criminale*, in «Diritto penale contemporaneo», 20 dicembre 2017, pp. 1 ss.; F. De Simone, *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in «Archivio penale», I (2018), pp. 1 ss.; M. Lamanuzzi, *La disinformazione ai tempi dei social media: una nuova sfida per il diritto penale?*, in «Archivio penale», I (2020); A. Visconti, *Alcune considerazioni criminologiche e politico-criminali sulle c.d. 'Fake* News', cit.; E. Birritteri, *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato*, in «Diritto penale contemporaneo – Rivista trimestrale», 4 (2021), pp. 304 ss.; A. Spena, A. Vallini, *Criminalizzare la postverità? Un dialogo postvero*, in *Studi in onore di Carlo Enrico Paliero*, a cura di Aa.Vv., Giuffrè, Milano, 2022, 237 ss.

2. *Tassonomia della disinformazione "manipolativa" del consenso elettorale.*

Per rispondere alla domanda proposta, risulta essenziale circoscrivere le tipologie di fatti che concretamente descrivono il fenomeno della disinformazione, rispetto a cui può porsi un tema di assoggettabilità a reazione punitiva. Si tratta, dunque, di selezionare, nell'ambito del *mare magnum* delle *fake news* presenti nella "infosfera", quelle che siano connotate da profili di offesa rilevanti e che si prestino a essere descritte in termini tassativi all'interno di precetti normativi. L'opera di costruzione tassonomica dovrebbe essere funzionale a verificare se i comportamenti così individuati siano già coperti dalla tutela del diritto penale e se la risposta punitiva sia adeguata ai bisogni di protezione; la stessa delimitazione concettuale potrebbe poi servire, *de lege ferenda*, come punto di partenza per la tipizzazione di nuovi reati. Va premesso che, sebbene le distorsioni informative si osservino in ambiti disparati, ci si limiterà qui a considerare quelle che coinvolgono il condizionamento delle decisioni di voto o degli esiti delle consultazioni elettorali.

Ebbene, quando ci si accosta alla descrizione della fenomenologia disinformativa, ci si trova di fronte a una tassonomia sfuggente e caleidoscopica.

La difficoltà definitoria emerge già se si guarda alla prima componente essenziale del concetto di disinformazione, che è la natura *oggettivamente falsa* del contenuto diffuso (l'"oggetto materiale", in termini penalistici). Stabilire che cosa debba considerarsi "falso" si rivela tutt'altro che scontato: oltre che fatti del tutto o in parte inventati, mai esistiti, potrebbero infatti rilevare quelli *falsificati* tramite l'alterazione o la deformazione di un nucleo di verità, e così pure notizie in sé veritiere, ma esposte in modo tendenzioso e manipolatorio (attraverso decontestualizzazioni, associazioni capziose, false connessioni tra titoli e contenuti, e così via)[13].

Diversificate sono anche le possibili *condotte* rilevanti. "Disinformare" richiede, in generale, una catena di azioni, che vanno dalla creazione del messaggio falso, alla sua pubblicazione online e alla sua ulteriore diffusione: rispetto a questa ultima fase del processo, peraltro, risulta spesso essenziale l'apporto sinergico di una pluralità di soggetti che, attraverso la condivisione dei contenuti, contribuiscono (anche inconsapevolmente) alla loro propagazione incontrollata. I singoli momenti dell'*iter* disinformativo, d'altro canto, sono realizzabili sia in forma monosoggettiva, sia concorsuale, sia nel contesto di vere e proprie strutture organizzative; può, poi, essere coinvolto l'utilizzo di meccanismi automatizzati (come i bot, eventualmente basati su IA), riducendosi in tal caso l'intervento umano alla programmazione iniziale o al controllo successivo dello strumento artificiale.

Per destare preoccupazione (e dunque interessare la prospettiva penalistica), la disinformazione dovrebbe implicare anche una componente di manipolazione o inganno quale *risultato* ("evento") della condotta. Il falso dovrebbe, cioè, effettivamente riuscire

[13] Ulteriori precisazioni in T. GUERINI, Fake news *e diritto penale*, cit., p. 36 s.

a indurre in errore il destinatario, per poi condizionarne le opinioni e le conseguenti decisioni di voto: si tratta, evidentemente, di concatenazioni causali di tipo psichico difficilissime da provare *ex post*, sia perché articolate su diversi passaggi (falsa notizia >> induzione in errore >> determinazione di specifiche scelte politiche), sia per la difficoltà di rinvenire leggi scientifiche di copertura in questo campo[14]. In alternativa, il comportamento disinformativo potrebbe essere selezionato sulla base della sua *potenzialità* ingannatoria/manipolativa del consenso elettorale (a sua volta "presunta" alla luce di ragionevoli generalizzazioni eziologiche, oppure accertata in concreto, di nuovo non senza criticità di ordine probatorio).

La componente decettiva può legarsi, oltre che alla modalità della distorsione (un falso grossolano è privo di capacità ingannatoria, mentre una esposizione capziosa di un fatto vero può essere estremamente ingannevole), anche alla provenienza soggettiva della notizia: una comunicazione autorevole e qualificata, perché espressa da un giornalista o da un esperto, può risultare ben più persuasiva di quella proferita dal *quivis ex populo*[15]. Ulteriore variabile è che il contenuto falso sia creato o comunque artatamente strumentalizzato all'interno del discorso politico, da parte di soggetti candidati alle elezioni oppure con ruoli negli organi di rappresentanza o di governo: pratica, questa, che evidenzia l'esistenza di una zona di stretta contiguità tra disinformazione e propaganda politica. Un fenomeno ancora diverso è la condivisione di verità alternative da parte dei *leader* e dei membri di "culti settari" che utilizzano tecniche di "plagio" per orientare il comportamento degli adepti (con dinamiche che in parte sembrano riproporsi all'interno di gruppi "complottisti")[16]: le credenze così introiettate possono incidere sulle scelte politiche ed essere sfruttate da terzi a fini di condizionamento del voto.

Anche la *dimensione offensiva* della disinformazione, in cui va individuato il termine di riferimento del danno o del pericolo, si sviluppa in molteplici direzioni. A fronte di forme di manipolazione cognitiva, capaci di plasmare le decisioni elettorali, a risultare turbata può essere la libertà di autodeterminazione individuale nell'esercizio del diritto di voto[17], oppure un più generico "diritto a informarsi" in modo corretto e senza essere ingannati, riconducibile al novero di quei "diritti aletici" che, secondo una certa

[14] M. Lamanuzzi, *La disinformazione ai tempi dei social media*, cit., pp. 22 ss.

[15] Ivi, p. 23; sulla distinzione tra pensiero "alto" e pensiero "basso" v. A. Galluccio, *Punire la parola pericolosa?*, Milano, Giuffrè, 2020, pp. 29 ss.

[16] Si rinvia all'interessante prospettiva di indagine sviluppata da M. Mattia, *"Gruppalità" no-vax, movimenti settari smaterializzati e infodemie digitali: il problema della criminalizzazione della disinformazione all'interno del cyberspace*, in «Archivio penale», 1 (2023). Su questo profilo, si segnala che un recente disegno di legge (A.S. 1496/2025) propone l'introduzione all'art. 613-*quater* c.p. di un nuovo reato di "manipolazione mentale", volto a punire con la reclusione tra tre a diciotto anni chiunque, "nell'ambito di un gruppo che promuove o pratica attività finalizzate a creare o a sfruttare una condizione di dipendenza psicologica o fisica dei partecipanti, induce taluno in un perdurante stato di soggezione tale da escludere, o da limitare in modo rilevante, la libertà di autodeterminazione o la capacità di discernimento".

[17] A. Spena, A. Vallini, *Criminalizzare la postverità?*, cit., p. 254.

impostazione filosofica, dovrebbero essere garantiti dall'ordinamento[18]. A un livello "macro-offensivo", sono poi le stesse istituzioni democratiche a essere minacciate dalle operazioni di falsa informazione dirette a pilotare i risultati delle consultazioni o a seminare confusione e diffidenza nella popolazione[19]; in caso di ingerenze straniere, viene in gioco la sicurezza nazionale. In via mediata, la manipolazione del consenso elettorale può inoltre incidere sulla reputazione individuale (per esempio, dei personaggi pubblici colpiti da *fake news* diffamatorie) o sul diritto alla salute (si pensi a chi compia scelte dannose per sé o terzi, sulla base di credenze antiscientifiche indotte o rafforzate da campagne disinformative che le strumentalizzino allo scopo di catalizzare il consenso); ancora, all'interno di strategie propagandistiche l'impiego di notizie false può essere funzionale a veicolare messaggi con contenuto discriminatorio e di odio[20] (è quanto accade nei processi di criminalizzazione-vittimizzazione dell'immigrato[21]).

Infine, le condotte di produzione e diffusione di false conoscenze possono connotarsi diversamente rispetto al profilo *soggettivo*: occorre infatti distinguere le azioni deliberate (disinformazione in senso stretto), dai casi di trasmissione inconsapevole o addirittura in buona fede (c.d. *misinformazione*), sicuramente insuscettibili di essere coinvolti dal rimprovero penale. Nel caso di contegni intenzionali, inoltre, può essere indicativa la presenza di finalità ulteriori, ad esempio di tipo economico o politico[22].

3. *Il contrasto alle* fake news *tramite il diritto penale*

Ricostruire le dinamiche dell'informazione e della disinformazione nell'attuale contesto storico, senza scadere nell'approssimazione, costituisce un compito arduo, che presuppone l'apporto conoscitivo delle scienze sociologiche e politologiche e un approfondimento ben più ampio di quello che può essere svolto in questa sede. La mappatura qui sommariamente approntata, tuttavia, consente almeno di intravvedere l'estrema eterogeneità delle manifestazioni rientranti nel concetto di disinformazione, a sua volta difficilmente sintetizzabile in una definizione unitaria.

Questa prima constatazione evidenzia già uno dei limiti che possono frapporsi a una strategia di contrasto *penale* alla disinformazione, ossia la complessità di tradurre

[18] F. D'Agostini, M. Ferrera, *La verità al potere. Sei diritti aletici*, Giulio Einaudi editore, Torino, 2019.

[19] A. Nicita, *Il mercato delle verità*, cit., passim. La menzogna nel "mercato politico" tradisce la fiducia alla base della rappresentanza democratica secondo M. Ruotolo, *Riflessioni interlocutorie su verità, fiducia e democrazia rappresentativa*, cit., pp. 54 ss.

[20] Sulla sinergia tra *fake news* ed *hate speech* v. F. De Simone, *'Fake news', 'post truth', 'hate speech'*, cit., pp. 5 ss.

[21] A. Spena, A. Vallini, *Criminalizzare la postverità?*, cit., p. 253.

[22] Le finalità di diffusione danno pregnanza al concetto di disinformazione per C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in «Quaderni costituzionali», 3 (2023), p. 550: «Il fenomeno della disinformazione può essere inteso, allora, come costante processo volontario di alterazione digitale della realtà, finalizzato a incidere sulle dinamiche di governo della sfera pubblica».

le specificità del fenomeno (o dei fenomeni) considerati nella tipizzazione di fattispecie effettivamente rispondenti al principio di precisione in materia penale.

Una seconda criticità riguarda l'esigenza di delimitare l'intervento a fatti offensivamente pregnanti: obiettivo tanto più ostico, quanto più il ricorso (parrebbe, inevitabile) al modello dell'offesa di pericolo si combini con beni giuridici generici e rarefatti (quali la democrazia, la sicurezza nazionale o l'ordine pubblico). La concretizzazione degli scopi di tutela è d'altronde essenziale per evitare di introdurre forme patenti o mascherate di punizione della menzogna in quanto tale, inaccettabili in un ordinamento laico: solo uno Stato etico potrebbe ammettere l'imposizione, tramite minaccia di sanzione penale, di un *obbligo generalizzato di verità* in capo ai consociati. In effetti, se si guarda ai casi in cui il diritto penale tradizionalmente indirizza la sanzione a chi "dice il falso" (si pensi ai delitti contro la fede pubblica, alla falsa testimonianza, alla calunnia)[23], risulta che non è mai la pura menzogna a rilevare, bensì il fatto che da questa derivi la lesione o messa in pericolo del bene giuridico di volta in volta tutelato: se ne deduce che la *verità* non è oggetto di tutela diretta e immediata da parte del diritto penale, ma se ne ammette la protezione solo in via strumentale rispetto alla tutela di *altri interessi*, anch'essi compromessi dalla falsità della comunicazione.

Da considerare, poi, la possibile tensione con la libertà di manifestazione del pensiero di un intervento punitivo che colpisca comportamenti, pur in ipotesi offensivi, di manipolazione comunicativa in materia politico-elettorale: a prescindere dalla questione della riconducibilità del falso intenzionale sotto la sfera protettiva dell'art. 21 Cost., infatti, la "menzogna" politica si muove in un campo contiguo e spesso difficilmente distinguibile da quello delle opinioni, sicché la sua repressione potrebbe tradursi in uno strumento di incriminazione del dissenso, e potrebbe altresì incentivare forme di auto-censura preventiva del libero pensiero (c.d. *chilling effect*).

Tutti questi profili devono essere tenuti in considerazione nel momento in cui si ragioni di possibili nuove incriminazioni in materia di tutela penale della verità dell'informazione. D'altra parte, si tratta di problemi presenti da tempo all'interno della riflessione penalistica, che tradizionalmente si confronta con fattispecie dirette a punire la creazione o trasmissione di contenuti comunicativi falsi.

4. *Gli attuali contorni della disinformazione penalmente rilevante*

In effetti, pur mancando ad oggi incriminazioni *ad hoc*, esattamente riferite al fenomeno della "moderna" disinformazione, molte delle possibili estrinsecazioni di quest'ultima risultano già imbrigliabili nelle maglie di tipicità di reati esistenti. Potrà

[23] D. Pulitanò, *Cura della verità e diritto penale*, in *Verità del precetto e della sanzione penale alla prova del processo*, a cura di G. Forti, G. Varraso, M. Caputo, 2014, Napoli, Jovene, p. 90; C. Perini, Fake news *e post-verità tra diritto penale e politica criminale*, cit., p. 3.

essere allora utile richiamarle brevemente, sia per verificare come si è finora svolto, in questo campo, il rapporto del potere punitivo con i principi-limite già evocati (determinatezza, libertà del pensiero e offensività), sia per capire se dall'attuale area di rilevanza penale effettivamente residuino spazi vuoti, tali da giustificare la richiesta di un ulteriore intervento punitivo.

Limitandoci qui a considerare le sole fattispecie che possono risultare di utilità nel contrasto alla disinformazione politico-elettorale, va anzitutto menzionato, in un'ottica di tutela individuale, il delitto di diffamazione (art. 595 c.p.): sebbene per la sua integrazione sia in via di principio irrilevante che l'addebito sia vero o falso[24], il reato risulterà sicuramente applicabile rispetto alle condotte di immissione sul *web*, in modo visibile a più persone, di contenuti che, per la loro falsità, offendono la reputazione di specifici soggetti[25]. Potrebbero quindi ricondursi a tale fattispecie i tentativi di manipolazione dell'opinione pubblica che si avvalgono della diffusione di testi o immagini recanti informazioni false su singoli individui (ad es. su personaggi con ruoli politici). Peraltro, all'ipotesi di divulgazione online delle notizie offensive risulta pacificamente applicabile l'aggravante dell'uso di un qualunque altro mezzo di pubblicità diverso dalla stampa, di cui all'art. 595, comma 3, c.p., trattandosi di una modalità diffusiva che consente di raggiungere un numero indeterminato o comunque quantitativamente apprezzabile di persone[26].

La falsità della notizia, inoltre, può rilevare nel senso di escludere la possibilità per l'autore del reato di invocare l'esimente dell'esercizio del diritto di cronaca *ex* art. 51 c.p.: la *verità* (oggettiva) del fatto esposto, accanto alla continenza e alla pertinenza della narrazione, costituisce infatti il presupposto perché il diritto a informare (estrinsecazione della libertà di pensiero) sia riconosciuto prevalente rispetto alla tutela della dignità individuale (artt. 2 e 3 Cost.), con conseguente liceità della trasmissione di notizie lesive dell'altrui reputazione.

La natura dolosa del delitto esclude dall'area della rilevanza penale le condotte di propagazione solo colposa delle comunicazioni diffamatorie. Nondimeno, occorre segnalare come l'errore colposo del giornalista sulla "verità" della notizia riportata, a causa di una non adeguata verifica preventiva delle fonti, sia considerato in giurisprudenza ostativo al riconoscimento della scriminante putativa del diritto di cronaca, nonostante l'art. 59 c.p. consenta la punibilità per errore colposo solo in caso di delitto punibile a titolo di colpa[27].

[24] T. PADOVANI, *Menzogna e diritto penale*, Pisa, Pisa University Press, 2019, p. 273.

[25] Sul tema della diffamazione online, V. PEZZELLA, *La diffamazione*, UTET Giuridica, 2020, pp. 805 ss.

[26] Da ultimo, cfr. Cass. pen., Sez. V, 7 maggio 2024, n. 34057. Prima della dichiarazione di incostituzionalità dell'art. 13 l. n. 47/1948, la giurisprudenza ne aveva esteso l'applicabilità alle notizie pubblicate su testate telematiche, allargando a queste ultime – con discutibile operazione interpretativa *in malam partem* – la nozione di "stampa" di cui all'art. 1 della stessa legge (cfr. Cass. pen., Sez. V, 11 gennaio 2019, n. 1275).

[27] In dottrina, si segnala l'impropria trasformazione della diffamazione in un delitto rispondente a criteri di imputazione anche colposa: G. FIANDACA, *Nuove tendenze repressive in tema di diffamazione a mezzo stampa?*, in «Foro italiano», II, (1984), c. 534; in tema v. G. DE VERO, *Le scriminanti putative. Profili problematici e fondamento*

Quanto alla disinformazione con contenuti discriminatori, potrà rilevare la fattispecie di propaganda istigatoria *ex* art. 604-*bis*, o l'istigazione a delinquere *ex* art. 414 c.p. (anche in tali casi, d'altra parte, la falsità della notizia non è elemento costitutivo del reato)[28]. Da segnalare anche l'aggravante del negazionismo (art. 604-*bis* comma 3), che attribuisce rilievo a ipotesi peculiari di falsità informative, quelle cioè relative alla negazione di fatti storicamente avvenuti di particolare gravità (il genocidio degli ebrei durante la Seconda guerra mondiale e i crimini internazionali di cui agli artt. 6, 7 e 8 dello Statuto della Corte penale internazionale).

L'ordinamento italiano, poi, comprende una fattispecie *generale* contro la propagazione di false informazioni: si tratta della contravvenzione di cui all'art. 656 c.p., che punisce con l'arresto fino a tre mesi o l'ammenda fino a 309 euro, se il fatto non costituisce più grave reato, la pubblicazione o diffusione di notizie "false, esagerate o tendenziose" atte a turbare l'ordine pubblico. A tale figura criminosa è possibile ricondurre gran parte delle condotte disinformative, grazie in particolare all'ampiezza con cui sono definiti i contenuti vietati: non solo le notizie sicuramente *false*, cioè difformi dal vero, ma anche quelle meramente *esagerate*, vale a dire che contengono verità amplificate, ingigantite o iperboliche, nonché quelle *tendenziose*, in cui la realtà è presentata in modo deformato e ingannevole. Trattandosi di una contravvenzione, inoltre, sotto il profilo soggettivo è sufficiente che l'autore sia in colpa rispetto alla falsità della notizia, in tal modo configurandosi in capo ai consociati un onere di controllo circa la correttezza e la provenienza delle informazioni diffuse.

L'ampia formulazione dell'art. 656 c.p. risente della originaria *ratio* liberticida della disposizione, inquadrabile tra i reati di opinione largamente utilizzati dal regime fascista come mezzo di contrasto agli oppositori politici: nella logica del legislatore del 1930, infatti, il riferimento alle notizie "esagerate" e a quelle "tendenziose" costituiva il veicolo per colpire opinioni di dissenso. La sopravvivenza della contravvenzione anche nel sistema democratico è stata resa possibile dalla Corte costituzionale (sentenza n. 19 del 1962), che l'ha reinterpretata per renderla compatibile con la libertà di espressione. Questa operazione ha coinvolto, sul piano del contenuto oggetto di diffusione, la delimitazione delle notizie tendenziose alle sole «che, pur riferendo cose vere, le presentino tuttavia […] in modo che chi le apprende possa avere una rappresentazione alterata della realtà», in definitiva non distinguendosi dalle notizie false: sono quindi prive di rilievo penale «interpretazioni, valutazioni, commenti, ideologicamente qualificati, e persino tendenziosi, relativi a cose vere» (tutti rientranti nell'area costituzionalmente tutelata delle libere opinioni). In secondo luogo, la "disinformazione" rilevante per l'art. 656 c.p. è solo quella in concreto pericolosa per l'ordine pubblico, inteso quest'ultimo nell'accezione c.d. ideale di «ordine legale su cui poggia la convivenza

della disciplina, in «Rivista italiana di diritto e procedura penale», III, (1998), p. 779; A. GULLO, *Diffamazione e legittimazione dell'intervento penale: contributo a una riforma dei delitti contro l'onore*, Aracne, Roma, 2013, pp. 32 ss.

[28] E. BIRRITTERI, *Punire la disinformazione*, cit., p. 313.

sociale», quale interesse «immanente al sistema costituzionale»: il giudice deve quindi accertare che le notizie propagate, alla luce del loro contenuto o dei tempi o modi della loro diffusione, risultino «idonee a determinare un turbamento consistente nell'insorgenza di un completo ed effettivo stato di minaccia dell'ordine stesso».

Nonostante questa rilettura, l'art. 656 c.p. mantiene una legittimazione problematica in rapporto all'art. 21 Cost.: la scarsa pregnanza del concetto di ordine pubblico lo rende inidoneo a delimitare le condotte punibili; di discutibile operatività è, poi, la restrizione del contenuto incriminato, stante la difficoltà di discriminare tra mere interpretazioni "tendenziose" del vero e notizie "falsate" per il modo in cui sono rappresentate. Si tratta di preoccupazioni peraltro stemperate dalla scarsa effettività della norma sul piano applicativo, dovuta all'irrisorietà del compendio sanzionatorio previsto.

L'art. 656 c.p. riveste natura sussidiaria rispetto a ulteriori, più gravi, fattispecie di reato che possono essere integrate dalla diffusione, anche tramite *internet*, di false notizie. Si pensi alla contravvenzione di procurato allarme (art. 658 c.p.), relativa alla condotta di «chiunque, annunziando disastri, infortuni o pericoli inesistenti, suscita allarme presso l'Autorità». In rapporto di specialità con l'art. 656 c.p. è pure il delitto di disfattismo politico (art. 265 c.p.), che punisce con la reclusione fino a cinque anni chi, in tempo di guerra, «diffonde o comunica voci o notizie false, esagerate o tendenziose, che possano destare pubblico allarme o deprimere lo spirito pubblico o altrimenti menomare la resistenza della nazione di fronte al nemico». Sempre nell'ambito della tutela della personalità dello Stato, vi sono altri delitti che consentirebbero di regolare alcuni casi di interferenza "informativa" sul funzionamento delle istituzioni: si pensi all'art. 284 c.p., che potrebbe essere invocato a fronte dell'impiego di false notizie per promuovere un'insurrezione armata contro i poteri dello Stato (paradigmatica, in questo senso, la vicenda statunitense dell'assalto a Capitol Hill)[29].

Si tratta, ad ogni modo, di fattispecie dalla rilevanza applicativa molto circoscritta. In pratica, in disparte la protezione garantita agli interessi personalistici coinvolti dalla diffusione di false notizie, per le condotte disinformative in materia politico-elettorale è disponibile solo la tutela "generalizzata" offerta dalla contravvenzione di cui all'art. 656 c.p., tuttavia di scarsa efficacia general-preventiva. Si aggiungono tutte le difficoltà – che in questa sede non è possibile analizzare – di riferire alle comunicazioni digitali il regime di responsabilità penale previsto in materia di stampa (*ex* art. 57 c.p.)[30] e, più in generale, di imputare ai gestori delle piattaforme il mancato controllo *ex ante* o la mancata rimozione *ex post* di contenuti integranti fattispecie di reato.

È poi qui possibile solo accennare alla ulteriore questione della rilevanza "mediata" della condotta disinformativa, qualora questa induca il destinatario a porre in essere azio-

[29] A. Spena, A. Vallini, *Criminalizzare la postverità?*, cit., p. 256.

[30] Cfr. Cass. pen., Sez. V, 12 gennaio 2021, n. 7220: «l'amministratore di un sito internet non è responsabile ai sensi dell'art. 57 c.p., in quanto tale norma è applicabile alle sole testate giornalistiche telematiche e non anche ai diversi mezzi informatici di manifestazione del pensiero (forum, blog, newsletter, newsgroup, mailing list, facebook), salvo che sussistano elementi che denotino la compartecipazione dell'amministratore alla attività diffamatoria.

ni autolesive o criminose: si pensi a campagne politico-elettorali che, sfruttando argomenti antiscientifici, spingano un singolo alla scelta di non vaccinarsi, o a somministrare cure omeopatiche al figlio minore affetto da una patologia tumorale. Si tratterebbe di interrogarsi sulla configurabilità di una responsabilità penale del "disinformatore" per l'evento lesivo finale, ovvero per la commissione del reato del terzo "indotto" dalla falsa credenza: ma le difficoltà di una simile ipotesi ricostruttiva sono evidenti tanto sul piano dell'accertamento causale (rispetto alla prova del nesso di condizionamento psichico tra la comunicazione e la decisione del destinatario di tenere una determinata condotta attiva o omissiva), quanto su quello del riscontro dell'elemento soggettivo doloso o colposo[31]. La questione, ad ogni modo, risulta in questa sede secondaria, investendo maggiormente il problema dell'incidenza della disinformazione sull'ambito della salute individuale.

4.1. *La disinformazione incidente sul libero esercizio di voto: la rilevanza penale della manipolazione elettorale*

Le ipotesi precedentemente evocate, come si è visto, non traducono lo specifico disvalore insito nella valenza ingannatoria che le comunicazioni digitali possono assumere nella sfera del discorso pubblico, quando cioè esse siano parte di strategie di manipolazione psichica volte a "piegare" la formazione del libero consenso degli elettori e, in via mediata, i risultati delle consultazioni di voto. La dimensione offensiva attinta da questi fatti è più puntuale rispetto a quella latamente riferibile all'ordine pubblico o alla personalità dello Stato: può essere infatti pregiudicata la libertà nell'esercizio del diritto di voto dei singoli cittadini e, con essa, la stessa "democraticità" del sistema politico-costituzionale, che la concreta espressione delle scelte elettive serve a garantire[32].

Occorre allora verificare se le comunicazioni decettive delle scelte elettorali possano essere inquadrate nel sistema di fattispecie penali che consentono di tutelare l'esercizio del diritto di voto e la regolarità dello svolgimento delle elezioni[33].

Il libero formarsi delle decisioni di voto è tutelato, in primo luogo, dal delitto di attentato ai diritti politici del cittadino (art. 294 c.p.), che punisce, tra le altre condotte, anche quella di chi, mediante inganno, determini taluno a esercitare un diritto politico in modo difforme dalla sua volontà. La norma, pertanto, potrebbe risultare configurabile nei casi in cui la disinformazione incida sulle opzioni di voto, manipolando la libertà decisoria dell'elettore. La difficoltà di un'applicazione in tal senso, tuttavia, deriva dalla costruzione dell'art. 294 c.p.[34] come reato ad evento, che richiede

[31] In tema v. M. Lamanuzzi, *Causalità e determinatezza nelle interazioni psichiche penalmente rilevanti*, Giappichelli, Torino, 2024, pp. 614 ss.

[32] L. Buscema, *Reati elettorali e principio di democraticità dell'ordinamento: profili assiologici e ricostruttivi*, in «Diritto penale contemporaneo», 28 ottobre 2013, pp. 4 ss.

[33] M. Mazzanti, *Reati elettorali* (voce), in *Enc. Dir.*, XIV vol., Milano, 1965. Sul problema dell'estensibilità ai *social network* della normativa in tema di silenzio elettorale v. T. Guerini, Fake news *e diritto penale*, cit., pp. 157 ss.

[34] La l. n. 132/2025 ha introdotto nell'art. 294 c.p. una circostanza aggravante, configurabile quando l'inganno sia posto in essere mediante l'impiego di sistemi di intelligenza artificiale.

la prova del nesso causale tra la condotta ingannevole e l'effettivo impedimento del diritto di voto o il suo esercizio difforme dalla reale volontà del cittadino. Per l'integrazione dell'inganno, inoltre, la giurisprudenza esclude la rilevanza di mere suggestioni e richiede l'utilizzo di mezzi fraudolenti equiparabili alla violenza e alla minaccia «in ordine all'idoneità ad esercitare sull'elettore una pressione di tale intensità da indurlo a determinarsi nell'esercizio di un diritto politico in modo contrario alla sua reale volontà»[35]: un'interpretazione restrittiva che rende la fattispecie sostanzialmente inservibile per il contrasto di condotte di disinformazione[36].

Nemmeno rilevanti rispetto al fenomeno in esame sono le altre ipotesi tese a presidiare la libertà della formazione del consenso elettorale, come lo scambio elettorale politico mafioso (art. 416-*ter* c.p.), oppure la corruzione elettorale (art. 96 T.U. delle leggi elettorali, D.P.r. 30 marzo 1957, n. 361 e successive modifiche).

Più attinente sembra invece la previsione di cui all'art. 97 T.U. delle leggi elettorali, che punisce anche il fatto di chi, «con notizie da lui conosciute false, con raggiri od artifizi, ovvero con qualunque mezzo illecito atto a diminuire la libertà degli elettori, esercita pressione per costringerli a firmare una dichiarazione di presentazione di candidatura od a votare in favore di determinate liste o di determinati candidati, o ad astenersi dal firmare una dichiarazione di presentazione di candidatura o dall'esercitare il diritto elettorale». L'impiego di notizie false (purché conosciute come tali dal soggetto attivo) compare quindi espressamente tra le possibili modalità di condizionamento del voto, suscettibili di assumere rilevanza penale. La fattispecie è di più facile configurabilità rispetto all'art. 241 c.p., poiché la tutela del bene giuridico – la genuinità del processo di formazione della volontà degli elettori – viene anticipata a un momento precedente rispetto alla sua effettiva lesione: si tratta, cioè, di reato di pericolo, che si limita a sanzionare ogni condotta che comporti una forma di pressione sulla libera determinazione della volontà dell'elettore, senza richiedere una concreta compromissione della sua libertà di voto o un'alterazione del risultato elettorale[37]. Altre ragioni, però, conducono a dubitare circa l'utilità della previsione nel reprimere la disinformazione online: la rilevanza penale, anzitutto, dovrebbe essere circoscritta alle ipotesi in cui l'azione comunicativa esprima un'idoneità di manipolazione o inganno descrivibile nei termini dell'esercizio di una vera e propria *pressione*; in secondo luogo, l'art. 97 richiede che il condizionamento sia esercitato su "singoli elettori", il che pare implicare l'inquadramento del fatto nell'ambito di un rapporto interpersonale, o comunque una comunicazione specificamente indirizzata al soggetto passivo, difficilmente integrabile da contenuti rivolti a un pubblico indeterminato (salvo ritenere che la profilazione algoritmica sui *social network* equivalga al raggiungimento di singoli elettori).

[35] Cass. pen., Sez. I, 26 giugno 1989, n. 11835; Cass. pen., Sez. I, 20 dicembre 2018, n. 16381.

[36] In questo senso anche T. Guerini, Fake news *e diritto penale*, cit., p. 154.

[37] In termini, Cass. pen., Sez. III, 23 settembre 2005, n. 39554.

5. *I possibili modelli di incriminazione. Cenni comparatistici e proposte* de iure condendo

Sulle indicazioni tratte dall'analisi *de iure condito* si può adesso provare a fondare qualche considerazione *de iure condendo*, guardando criticamente alle possibili direzioni in cui potrebbe orientarsi la criminalizzazione delle condotte di disinformazione, almeno in ambito politico-elettorale.

Non si condivide l'opzione, accolta da alcune proposte di legge molto discusse[38], di "restaurare" l'idealtipo del reato di opinione di cui all'art. 656 c.p. – di cui già si sono evidenziate le criticità rispetto agli assetti della nostra democrazia costituzionale – per trarne una figura criminosa volta alla repressione *in sé e per sé* della diffusione di false notizie su piattaforme online, a prescindere dalla messa in pericolo di ulteriori interessi[39], oppure sulla base della idoneità a ledere beni giuridici dal contenuto impalpabile, come quello "democratico" latamente inteso[40]. È già di per sé significativo come questo schema di punizione abbia attecchito in Stati autoritari (penso alla Russia o alla Cina, o a paesi del sud-est asiatico come Malesia, Singapore, Vietnam)[41], ma anche in paesi europei (Turchia o Ungheria, ad esempio)[42] non esattamente noti per la tutela della libertà di espressione e della libertà di stampa: il che dimostra come l'incriminazione di *fake news* in quanto tali possa rivelarsi uno strumento di repressione mascherata delle espressioni di dissenso politico o ideologico (di chi non aderisce alla verità "di Stato", o comunque maggioritaria, in un certo contesto politico). Né questo pericolo può essere arginato da proiezioni teleologiche verso beni vaghi e manipolabili, sorrette da una causalità indimostrabile. Per non dire, infine, di come la diffusione di falsità, mezze verità, pregiudizi ideologici e artifici retorici sia fisiologica in ogni dibattito democratico, e comunque coperta dalla garanzia dell'art. 21 Cost.

Per rispettare i principi di offensività e determinatezza, e superare le tensioni con la libertà di manifestazione del pensiero, si sono allora immaginati modelli di incriminazione costruiti su elementi più pregnanti, tali da esprimere un disvalore particolarmente

[38] Si fa riferimento, in particolare, ad alcune proposte presentate durante la XVII legislatura, poi non approvate, per il cui esame rinvio ad A. COSTANTINI, *Istanze di criminalizzazione delle* fake news, cit., pp. 70 ss.

[39] A tutela della verità in quanto tale si poneva, ad esempio, l'art. 656-*bis* c.p. proposto dal d.d.l. Gambaro (A.S. 2688 del 7 febbraio 2017), che prevedeva di punire chiunque «pubblica o diffonde, attraverso piattaforme informatiche destinate alla pubblicazione o diffusione di informazione presso il pubblico, con mezzi prevalentemente elettronici o comunque telematici, notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o falsi».

[40] Nel progetto Gambaro, ad esempio, si proponeva di punire la diffusione di notizie aventi a oggetto lo svolgimento di «un'attività tale *da recare nocumento agli interessi pubblici o da fuorviare settori dell'opinione pubblica*, anche attraverso campagne con l'utilizzo di piattaforme informatiche destinate alla diffusione online» (art. 265-*bis* c.p.), nonché il rendersi responsabili «di campagne volte a *minare il processo democratico, anche a fini politici*» (art. 265-*ter* c.p.).

[41] Per l'esame di queste legislazioni-"bavaglio", v. T. GUERINI, Fake news *e diritto penale*, cit., pp. 88 ss.

[42] La c.d. "legge sulla disinformazione" turca del 12 ottobre 2022 (n. 7418), prevede l'introduzione di un nuovo reato relativo alla diffusione pubblica di notizie "fuorvianti" per il pubblico, all'art. 217/A del codice penale turco.

accentuato sul piano oggettivo e soggettivo. Spena e Vallini, ad esempio, suggeriscono di incriminare le forme più estreme di propalazione intenzionale di *fake news*, in particolare sostenute sul piano del disvalore d'azione da una marcata "artificiosità" della condotta diffusiva e da uno specifico orientamento alla distorsione del dibattito democratico o scientifico[43].

Ulteriori correttivi potrebbero essere, da un lato, la delimitazione del concetto di falso punibile, dall'altro la perimetrazione del *contesto di diffusione* del contenuto decettivo.

Nel primo senso, si segnalano le iniziative legislative che vanno nel senso di punire i c.d. *deepfake*, il cui contenuto di falsità appare indiscutibile, e la cui idoneità decettiva (specialmente quando si utilizzino tecnologie di intelligenza artificiale) è particolarmente spiccata[44]. La mera falsità del contenuto non sarebbe del resto sufficiente a giustificare un generale divieto penalmente sanzionato, il quale, oltre a essere impraticabile, si porrebbe in conflitto con la libertà di espressione, in particolare con il diritto di critica e di satira. Al fine di legittimare l'opzione incriminatrice, dunque, non verrebbe comunque meno l'esigenza già segnalata di individuare ulteriori profili di offensività della condotta diffusiva. Il recente d.d.l. in tema di intelligenza artificiale propone di introdurre all'art. 612-*quater* c.p. un reato di «Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale», la cui punibilità viene subordinata all'effettiva lesione (secondo il modello del reato ad evento) di un bene personalistico: più precisamente, si vuole punire con la reclusione da uno a cinque anni chiunque cagioni «un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità»[45]. Nella materia della manipolazione elettorale, invece, si segnala una proposta di legge da poco presentata[46], che suggerisce di introdurre un delitto per punire, con la reclusione da uno a quattro anni, «chiunque, al fine di alterare il libero svolgimento delle campagne elettorali o referendarie o di manipolarne il risultato, cede, pubblica o altrimenti diffonde contenuti ingannevoli o manipolati generati in tutto o in parte con sistemi di IA».

Nella seconda direzione indicata, relativa al "contesto" della diffusione, si potrebbe considerare una delimitazione "temporale" coincidente con il periodo elettorale, trattandosi di un momento specialmente "sensibile", in cui potrebbe non esserci più

[43] A. Spena, A. Vallini, *Criminalizzare la postverità?*, cit., pp. 252 ss.

[44] Discipline di carattere penale per regolamentare i *deepfake* sono state approvate, ad esempio, in Cina e negli Stati Uniti: per una panoramica, v. A. Orlando, *La regolamentazione del deepfake in Europa, Stati Uniti e Cina*, in «Rivista di diritto dei media», numero speciale (2024).

[45] Nelle more della pubblicazione di questi scritti, il disegno di legge è stato approvato (l. 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»). Per un commento al d.d.l., v. L. Scollo, *L'intelligenza artificiale entra nel Codice penale*, in «Diritto penale e processo», 6 (2025), pp. 698 ss.

[46] A.C. n. 2212, presentata il 23 gennaio 2025, relativa alla «Modifica alla legge 4 aprile 1956, n. 212, e altre disposizioni per prevenire l'alterazione o la manipolazione delle campagne elettorali e referendarie attraverso la diffusione di contenuti ingannevoli prodotti mediante sistemi di intelligenza artificiale».

tempo per la pubblicizzazione di una "contro-notizia" che smentisca la precedente falsità. Questo elemento di perimetrazione offrirebbe il vantaggio di agganciare l'incriminazione alla *concretizzazione del pericolo* per la libertà di esercizio del diritto di voto e per lo svolgimento dei processi elettorali in assenza di condizionamenti esterni. Aderisce a questo modello l'art. 264 del Codice penale austriaco, che punisce «chiunque dissemini false informazioni su una circostanza capace di influenzare l'esercizio di voto, in un punto nel tempo in cui una contro-affermazione non può più essere efficacemente diffusa». In alcuni sistemi angloamericani, sono previste fattispecie che incriminano, nel periodo delle elezioni, la diffusione di false notizie relative a qualità personali o comportamenti di soggetti candidati alle elezioni[47]: in questi casi, accanto al "tempo" elettorale è l'incidenza sulla reputazione personale e politica del singolo a costituire criterio di selezione delle condotte punibili.

Un elemento molto evanescente, dunque difficilmente verificabile, è quello che collega la condotta di disinformazione a "ingerenze straniere", come proposto in un recente disegno di legge presentato al Senato, che prevede di punire con la reclusione da uno a sei anni (e la sanzione amministrativa da 50 mila a 20 milioni di euro) «chiunque ponga in essere attività di disinformazione riconducibili a ingerenze straniere volte ad alterare le competizioni elettorali e a pregiudicare l'integrità del processo democratico, ovvero contribuisca ad esse»[48].

Un'altra questione considerata in dottrina (Schünemann) attiene all'esigenza – non solo per ragioni di legittimità, ma anche di opportunità e praticabilità dell'intervento penale – di evitare quella criminalizzazione "di massa", quale deriverebbe dalla punizione indiscriminata delle condotte di mera diffusione di notizie false online, ampiamente diffuse a livello sociale e poco caratterizzate in termini di disvalore. A tal fine si è proposta la creazione di un reato proprio, riferito a soggetti pubblici, i quali pubblicamente dichiarino un fatto falso capace di influenzare il comportamento elettorale dei votanti[49].

Si orienta, ancora, verso la responsabilizzazione di soggetti qualificati posti in una posizione privilegiata, rispetto alla possibilità di preservare le dinamiche democratiche, il modello cui corrispondono le legislazioni tedesca (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken – c.d. NetzDG*, del 2018) e francese (leggi nn. 1201 e 1202 del 2018, *relative à la lutte contre la manipulation de l'information*), che spostano sul piano del gestore della piattaforma il *focus* della repressione, sanzionando (rispettivamente in via amministrativa e penale) la violazione di una serie di obblighi di trasparenza, di controllo o di rimozione dei contenuti illeciti[50].

[47] Nel Regno Unito, ad esempio, cfr. la sezione 106 del *Representation of the People Act* (1983); in Canada, v. la sezione 91 dell'*Elections Modernization Act* (come modificato nel 2018).

[48] D.d.l. A.S. 1473, «Istituzione di uno scudo democratico a difesa delle libertà costituzionali e dell'integrità del processo democratico dalle ingerenze straniere», presentato su iniziativa dei senatori Lombardo e Calenda il 30 aprile 2025.

[49] B. Schünemann, *Gefährden Fake News die Demokratie, wächst aber im Strafrecht das Rettende auch?*, in «Goltdammer's Archiv» (2019), p. 639.

[50] Per l'esame dettagliato di tali disposizioni si rinvia a T. Guerini, Fake news *e diritto penale*, cit., pp. 75 ss.

6. *Diritto penale, verità, democrazia: brevi note conclusive*

Ciascuna di queste proposte meriterebbe un'analisi di dettaglio, impraticabile in questa sede. Limitandomi, dunque, ad alcune considerazioni conclusive di carattere generale, che tengono a mente i più volte richiamati principi di offensività e determinatezza, mi sembra che la prospettiva di una criminalizzazione delle *fake news* in materia elettorale (e/o in tempo di elezioni) presenti delle criticità intrinseche, che nessun intervento correttivo o contenitivo riesce a risolvere. Esse sono essenzialmente due: *(i)* la difficoltà di delimitare sul piano oggettivo il contenuto di falsità "decettiva" da incriminare, laddove le forme più pericolose di disinformazione politica (realmente capaci di orientare l'opinione pubblica, perché difficili da smascherare in tempi ragionevoli) si avvalgono della torsione di dati di realtà, più che di bugie macroscopiche o fatti totalmente inventati: ne consegue il rischio – reso manifesto da talune delle proposte di legge in discussione – di costruire delle fattispecie completamente sbilanciate sui profili soggettivi del fatto (ad es., il fine di manipolare l'opinione pubblica e di condizionare i risultati elettorali); *(ii)* il secondo motivo di perplessità riguarda il ricorso allo schema del reato di pericolo (*a fortiori* risultando impraticabili reati incentrati sulla causazione di un evento lesivo), che se inteso in concreto lascia dubbi sulla possibilità di provare l'effettiva capacità condizionante delle *fake news* rispetto al consenso elettorale; di contro, il paradigma del pericolo in senso astratto risentirebbe della dubbia capacità selettiva dei beni giuridici richiamati, con il rischio riproporre in forma indiretta una tutela mascherata della verità[51].

Al di là, poi, di condividere o meno queste e altre proposte dal punto di vista delle loro implicazioni tecniche, e del loro atteggiarsi rispetto alle esigenze di offensività e determinatezza, la questione fondamentale attiene alla stessa necessità di una tutela penale del vero in via strumentale alla protezione dei processi democratici e della libertà dell'esercizio del diritto di voto.

Ora, è senz'altro indubbio che la partecipazione dei cittadini alla vita democratica richiede che ciascuno sia messo nelle condizioni di formarsi liberamente delle opinioni, in modo da poter esercitare altrettanto liberamente il proprio diritto di voto (art. 48 Cost.): mentre la menzogna politica «altera il gioco democratico»[52], precludendo il formarsi di idee consapevoli perché autenticamente informate. D'altra parte, le premesse democratiche delineate nella Carta fondamentale, insieme con il valore primario della diffusione di libere manifestazioni di pensiero (art. 21 Cost.), reclamano la protezione non tanto della verità, come valore in sé – concetto che immediatamente evoca tensioni eticizzanti e assolutistiche – bensì di *strumenti, condizioni* e *libertà* perché la verità possa

[51] Condivisibile la riflessione di H. SOARES, *Strafrechtliche Bekämpfung von Fake News? Zum Umgang der Kriminalisierungstheorie mit der Wahrheit*, in AA.VV., *Strafrecht und Demokratie*, Nomos, Baden Baden, 2023, p. 179 ss., secondo cui, se la messa in pericolo non è più concreta, la protezione di quel bene contro le falsità non si distingue più dalla protezione diretta della verità.

[52] M. RUOTOLO, *Riflessioni interlocutorie su verità, fiducia e democrazia rappresentativa*, cit., pp. 44 ss.

essere ricercata all'interno del dibattito pubblico, come premessa per una partecipazione libera, effettiva ed eguale alla vita democratica. È questo il senso profondo dei diritti aletici di cui si parlava: il diritto a vivere in una società dove è riconosciuta l'importanza della verità, e dove esistono le condizioni per lo sviluppo di un discorso pubblico aperto e partecipato, fondato su basi di verità e orientato al riconoscimento di verità.

Ebbene, per raggiungere questo obiettivo, è dubbia l'utilità di un intervento penale diretto a epurare l'agorà politica dei contenuti menzogneri. Non si tratta tanto (o comunque non solo) di garantire che il diritto punitivo sia mantenuto in una logica sussidiaria e di *extrema ratio*, dunque recessiva rispetto a interventi positivi, tesi a rimuovere – secondo logiche di uguaglianza sostanziale – ostacoli culturali, tecnologici, economici che si frappongono a una partecipazione paritaria alla vita democratica. Il punto, piuttosto, è che la logica dell'intervento punitivo sembra in questo caso pericolosa o controproducente. Si tratterebbe infatti di affidare al giudice penale (il quale non è detto sia a sua volta scevro da condizionamenti politici) il compito di imporsi al dibattito pubblico per sancire una volta per tutte cosa sia vero e cosa no, quale contenuto di pensiero comunicato sia lecito o illecito: si sposterebbero cioè le dinamiche di falsificazione/verificazione di "verità" di rilevanza scientifica o politica dai luoghi del dibattito scientifico o politico a quelli del processo penale, concepiti però per tutt'altro fine e, per di più, connotati da un rapporto di squilibrio tra individuo e autorità. Queste obiezioni, già sollevate nella discussione sulla criminalizzazione del negazionismo[53], si ripropongono a maggior ragione rispetto a un'incriminazione che sarebbe ancora più ampia e pervasiva. Per una sorta di eterogenesi dei fini, lo strumento penale potrebbe facilmente convertirsi in un meccanismo di repressione del dissenso, dell'opinione contraria a quella dominante.

Ancora, nell'opzione sanzionatoria sembra implicita una prospettiva paternalistica, inconciliabile con l'ideale dell'eguale partecipazione alla vita politica prevista dalla Costituzione: il presupposto da cui essa muove è, infatti, che gli utenti siano tendenzialmente indifesi di fronte ai tentativi di manipolazione delle loro opinioni, incapaci di pensare autonomamente nello spazio digitale e, più in generale, di partecipare responsabilmente al pubblico confronto.

In una prospettiva autenticamente liberale, quel che risulta fondamentale garantire è il rispetto delle "regole" del gioco democratico, ossia i contorni esterni dell'agorà in cui si svolge la dialettica politica: il gioco potrà nutrirsi anche di falsità e menzogne, purché sia assicurato il loro antidoto, che non è la rimozione o la sanzione, bensì la possibilità di essere smentite e contestate, *quindi* falsificate. Forse solo in quest'ottica si intravvede uno spazio per un impiego plausibile (pur sussidiario e minimo) della sanzione penale: l'intervento punitivo potrebbe cioè riguardare non tanto le condotte che alterano i contenuti che circolano nel dibattito pubblico, se non quando ciò accada in contesti temporali che non lasciano possibilità di smentita (sul modello dell'art. 264 öStGB);

[53] E. Fronza, *Il negazionismo come reato*, Giuffrè, Milano, 2012, pp. 153 ss.

piuttosto, si potrebbe immaginare una tutela penale contro comportamenti che impediscono di accedere all'agorà politica (ad esempio, tramite manomissioni *ab externo* dello spazio virtuale o la violazione da parte dei gestori delle piattaforme di obblighi di trasparenza circa la provenienza delle fonti o la loro sponsorizzazione commerciale) o, ancora, che impediscono la stessa partecipazione alle consultazioni elettorali (ad es., diffondendo false notizie sui luoghi, i tempi delle elezioni o sull'identità dei candidati che vi partecipano)[54]. Una prospettiva di questo tipo andrebbe nel senso di tutelare l'esigenza democratica di verità senza tradursi in un'imposizione illiberale di verità.

[54] Si veda la prospettiva proposta da J. HORDER, *Criminal Fraud and Electoral Disinformation*. *Law and Politics*, Oxford University Press, Oxford, 2022, secondo cui occorre distinguere tra "*political viewpoint disinformation*", da ritenersi ammessa nel contesto della dialettica democratica, dalla "*electoral participation disinformation*", rispetto a cui invece è non solo opportuno, ma auspicabile indirizzare l'intervento punitivo.

SEZIONE 3

VIOLENZA ONLINE E PROTEZIONE DELLE VITTIME: TRA TUTELA E RIPARAZIONE

LA TUTELA "INTEGRATA" DELLA VITTIMA DI VIOLENZA ONLINE NELLO SPAZIO EUROUNITARIO

Marco Venturoli

SOMMARIO: 1. Premessa: la cifra *vittimocentrica* del diritto dell'Unione europea tra ombre *securitarie* e luci *solidaristiche*. – 2. La persona offesa dal reato online quale soggetto *vulnerabile* della *postmodernità*. – 3. La tutela delle vittime di violenza digitale nel quadro della direttiva 2024/1385/UE. – 4. (*Segue*) I limiti dell'approccio *victim oriented* adottato dalla direttiva – 5. Considerazioni conclusive: *input* europei e politiche nazionali.

1. *Premessa: la cifra* vittimocentrica *del diritto dell'Unione europea tra ombre* securitarie *e luci* solidaristiche

È circostanza nota che l'ordinamento dell'Unione europea esibisca una spiccata sensibilità per le istanze della vittima di reato[1]: all'interno dello stesso si può invero riconoscere un vero e proprio corpus normativo dedicato alla protezione delle vittime degli illeciti penali, i cui primi tasselli sono stati posati più di quarant'anni or sono, nel contesto dell'allora Comunità economica europea.

Un corpus che si è vieppiù espanso soprattutto dalla nascita dell'Unione europea, con l'istituzione di una politica criminale della stessa, e con il Trattato di Lisbona grazie alla previsione dei «diritti delle vittime della criminalità» tra le materie su cui il Parlamento europeo e il Consiglio possono adottare direttive di armonizzazione penale (art. 82 §. 2, lett. c, TFUE)[2]. D'altra parte, proprio quest'ultima disposizione del Trattato costituisce la principale base giuridica sulla quale è stata varata la direttiva 2012/29/UE, che rappresenta all'oggi il testo dell'Unione più ampio dedicato alla tutela delle

[1] In argomento v., per esempio, S. ALLEGREZZA, *La riscoperta della vittima nella giustizia penale europea*, in *Lo scudo e la spada. Esigenze di protezione e poteri delle vittime nel processo penale tra Europa e Italia*, a cura di S. Allegrezza, H. Belluta, M. Gialuz, L. Lupária, Giappichelli, Torino, 2012, p. 1 ss.; M. DEL TUFO, *La vittima di fronte al reato nell'orizzonte europeo*, in *Punire, mediare, riconciliare. Dalla giustizia penale internazionale alla rielaborazione dei conflitti individuali*, a cura di G. Fiandaca e C. Visconti, Giappichelli, Torino, 2009, p. 107 ss.; M.L. LANTHIEZ, *La clarification des fondaments européens des droits des victimes*, in *La victime sur la scène pénale en Europe*, a cura di G. Giudicelli-Delage e C. Lazerges, Puf, Parigi, 2008, p. 145 ss.

[2] Per una panoramica sulla nascita e sullo sviluppo di questo corpus normativo v. D. SAVY, *La vittima dei reati nell'Unione europea. Le esigenze di tutela dei diritti fondamentali e la complementarietà della disciplina penale e civile*, Milano, Giuffrè, 2013, p. 19 ss.; volendo, M. VENTUROLI, *La vittima nel sistema penale. Dall'oblio al protagonismo?*, Jovene, Napoli, 2015, p. 96 ss.

vittime di reato da una prospettiva generale[3]. È la direttiva stessa a fornire, all'art. 2, una definizione *estesa* di vittima[4], capace di ricomprendere al proprio interno diverse figure della tradizione giuridica nostrana (soggetto passivo del reato, persona offesa dal reato, danneggiato dal reato e parte civile)[5].

Dalla direttiva in questione emerge, poi, in maniera esplicita la portata vittimocentrica del diritto penale europeo, là dove – nel preambolo della stessa – si afferma che «un reato è non solo un torto alla società ma anche una violazione dei diritti individuali delle vittime». L'illecito penale in tal modo si *concretizza*, si *individualizza* sul suo versante passivo, in prospettiva complementare alla definizione di vittima fatta propria dalla direttiva stessa. Un concetto che si affranca dunque dalla nozione di reato, dal tenore "oggettivo-limitativa", quale *offesa ad un bene giuridico*, con cui il penalista è abituato a misurarsi da circa due secoli[6]. In altri termini, si capovolge la prospettiva di intervento del diritto penale, sempre più coincidente con la politica criminale, che diviene per l'ordinamento dell'Unione la *magna charta* della vittima.

La sensibilità per le istanze della vittima di reato si sposa poi ideologicamente con la promozione da parte dell'Unione stessa della *sicurezza* quale valore "costituzionale" autonomo, di *hobbesiana* memoria[7], e non semplicemente come bene *strumentale* al godimento di altri diritti secondo la tradizione liberale[8]: all'interno del preambolo

[3] A commento della direttiva v., tra gli altri, E.M. CATALANO, *La tutela della vittima nella direttiva 2012/29/UE e nella giurisprudenza della Corti europee*, in «Riv. it. dir. proc. pen.» (2014), p. 1789 ss.; S. ALLEGREZZA, *Il ruolo della vittima nella direttiva 29/12/UE*, in *Lo statuto europeo delle vittime di reato. Modelli di tutela tra diritto dell'Unione e buone pratiche nazionali*, a cura di L. Luparia, Wolters Kluwer-CEDAM, Milano, 2015, p. 3 ss.; M. BARGIS, H. BELLUTA, *La direttiva 2012/29/UE: diritti minini della vittima nel processo penale*, in ID. (a cura di), *Vittime di reato e sistema penale. La ricerca di nuovi equilibri*, Giappichelli, Torino, 2017, p. 15 ss..

[4] Secondo l'art. 2 §. 1 della direttiva, la vittima è «i) una persona fisica che ha subito un danno, anche fisico, mentale o emotivo, o perdite economiche che sono stati causati direttamente da un reato; ii) un familiare di una persona la cui morte è stata causata direttamente da un reato e che ha subito un danno in conseguenza della morte di tale persona».

[5] Tuttavia, solo di recente, con il d.lgs. n. 150/2022 (c.d. riforma Cartabia), l'espressione "vittima del reato" è stata acquisita dall'ordinamento italiano – peraltro limitatamente al comparto della giustizia riparativa – per tradizione restio all'impiego di un concetto di origine criminologica, dai confini tanto indefiniti. Sul punto sia consentito rinviare a M. VENTUROLI, *La vittima del reato tra riconoscimenti formali e nuovi orizzonti sanzionatori*, in *Riforma Cartabia. La nuova giustizia penale*, a cura di D. Castronuovo, M. Donini, E.M. Mancuso, G. Varraso, Wolters Kluwer, Milano, 2023, p. 509 ss.

[6] Cfr., per tutti, M. ROMANO, *Commentario sistematico del codice penale*, vol. I, Milano, Giuffrè, 2004, p. 12. Si è affermata tuttavia anche nella dottrina italiana un'autorevole voce incline a rileggere i reati contro la persona in termini di offesa a diritti soggettivi delle vittime, segnatamente con un intento di ripensare al ruolo della vittima nella teoria del reato (F. VIGANÒ, *Diritto penale e diritti della persona*, in *Studi in onore di Carlo Enrico Paliero*, Tomo II, a cura di G. Mannozzi, C. Perini, M.M. Scoletta, C. Sotis, S.B. Taverriti, Giuffrè, Milano, 2022, p. 845 ss.; in risposta critica a questa lettura v. A. CAVALIERE, *'Diritti' anziché 'beni giuridici' e 'principi' in diritto penale? A proposito di un saggio di Francesco Viganò*, in «Sist. pen.», 16 ottobre 2023).

[7] In merito ai retaggi *hobbesiani* dell'europeismo penale v. C. CUPELLI, *Hobbes europeista? Diritto penale europeo*, auctoritas *e controlimiti*, in «Criminalia» (2013), p. 359.

[8] Per una puntuale panoramica sulle differenti espressioni del concetto di sicurezza nella materia penale v., per esempio, D. PULITANÒ, *Sicurezza e diritto penale*, in «Riv. it. dir. proc. pen.» (2009), p. 547 ss.; in argomento

del Trattato UE, la sicurezza è invero declinata in senso *privatistico*[9], come "elemento costitutivo" dello spazio giuridico dell'Unione[10]; del pari, del resto, alla propensione della giurisprudenza della Corte di Strasburgo – anch'essa segnata da marcati accenti vittimocentrici – a riconoscere a favore dei cittadini ("vittime potenziali") un *diritto alla sicurezza* che lo Stato è chiamato a salvaguardare attraverso politiche penali allo scopo adeguate[11].

In ogni caso, nell'ordinamento eurounitario se da un canto la tutela delle vittime si estrinseca, *prima facie*, attraverso l'impiego "muscolare" dello strumento penale[12], in particolare esibito con obblighi di incriminazione non sempre ineccepibili sul fronte della rispettiva tenuta legalitario-garantistica[13]; dall'altro canto, si manifesta tramite un ampio corredo di misure di dissimile natura (processuali, risarcitorie, "amministrative", ecc.), destinate ad offrire alle vittime una protezione "a largo spettro", tanto *ex ante* (quindi alle vittime potenziali) quanto *ex post* (ovverosia alle vittime effettive).

In breve, si può dunque affermare che il diritto dell'Unione europea configuri un sistema di tutela delle vittime di reato dalla portata *olistica* o *pluridirezionale*[14], che combina istanze socialdifensive e solidaristiche in vista di un obiettivo comune.

cfr., altresì, A. BERNARDI, *Il proteiforme concetto di sicurezza: riflessi in ambito penale*, in *Per il 70. Compleanno di Pierpaolo Zamorani. Scritti offerti dagli amici e dai colleghi di facoltà*, a cura di L. Desanti, P. Ferretti, A.D. Manfredini, Giuffrè, Milano, 2009, p. 1 ss.

[9] Sulla trasformazione del concetto di sicurezza in senso "privatistico" cfr. T. PITCH, *Il malinteso della vittima*, Edizioni Gruppo Abele, Torino, 2022, p. 10 ss.

[10] Nel preambolo del TUE è specificato l'intento di «agevolare la libera circolazione delle persone, garantendo nel contempo la sicurezza dei popoli, con l'istituzione di uno spazio di libertà, sicurezza e giustizia». Sempre quale strumento di difesa dalla criminalità è richiamata la sicurezza nel preambolo della Carta dei diritti fondamentali dell'Unione europea, dove, al § 2, è previsto che «… l'Unione […] pone la persona al centro della sua azione […] creando uno spazio di libertà, sicurezza e giustizia». Critico verso la dimensione securitaria dell'Unione è, ad esempio, D. NEGRI, *Dallo 'scandalo' della vicenda* Taricco *risorge il principio di legalità processuale*, in *Il caso Taricco e il dialogo tra le Corti. L'ordinanza 24/2017 della Corte costituzionale*, a cura di A. Bernardi e C. Cupelli, Jovene, Napoli, 2017, p. 297.

[11] Cfr. V. VALENTINI, *Diritto penale intertemporale, Logiche continentali ed ermeneutica europea*, Giuffrè, Milano, 2012, p. 53, il quale osserva che «Secondo i giudici di Strasburgo, insomma, è il diritto fondamentale alla sicurezza e alla prevenzione (*Menschenrecht auf Sicherheit*) dei cittadini-potenziali vittime, a radicare il dovere fondamentale degli Stati di tranquillizzare-prevenire-proteggere (*grundrechtliches Schutzflicht*), a ciò funzionalizzando le strategie politico criminali, le attività investigative e l'interpretazione del quadro normativo positivizzato: solo la punizione effettiva del reo, infatti, sembra capace di ricomporre il "cerchio della fiducia" (*Rund-um-Vertrauens*) e ristabilire una sensazione di sicurezza».

[12] Denuncia lo spirito "espansivo" del diritto penale europeo F. GIUNTA, *Europa e diritto penale. Tra linee di sviluppo e nodi problematici*, in «Discrimen», 26 marzo 2020, p. 17, secondo cui «la politica criminale promossa dall'UE ha a cuore l'allineamento delle legislazioni lungo lo standard di tutela più elevato, trascurando di promuoverne un simmetrico adeguamento ai migliori livelli nazionali di garanzia».

[13] Cfr., per esempio, L. FOFFANI, *Il "Manifesto sulla politica criminale europea"*, in «Criminalia» (2010), p. 657 ss.; C. PAONESSA, *Gli obblighi di tutela penale. La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari*, Edizioni ETS, Pisa, 2009, p. 193 ss.

[14] Cfr., volendo, M. VENTUROLI, *La tutela delle vittime nelle fonti europee*, in «Dir. pen. cont. – Riv. trim.», 3/4 (2012), p. 100.

2. *La persona offesa dal reato online quale soggetto* vulnerabile *della* postmodernità

Destinataria preferenziale di questa strategia integrata di tutela è la vittima *vulnerabile* o *particolarmente debole*, che è stata qualificata come «supervittima»[15], giustappunto per rimarcare la posizione nodale dalla stessa ricoperta nel diritto dell'Unione[16].

Sennonché, il legislatore europeo si è finora astenuto dal tratteggiarne una definizione, verosimilmente a causa del carattere sfaccettato di questo concetto social-criminologico, declinabile da differenti angolature, come del resto testimoniato dalle diverse scelte adottate dagli Stati membri in materia[17]; nonché della volontà – emersa in particolare nella direttiva 2012/29/UE – di stabilire la vulnerabilità della vittima alla luce delle peculiarità del caso concreto (c.d. *individual assessment*), da cui possono emergere con maggior precisione i bisogni di volta in volta manifestati dalla singola persona offesa[18].

Ebbene, due sono le principali forme di vulnerabilità della vittima rilevanti in sede penale[19].

In primo luogo, si allude ad una vulnerabilità in senso *soggettivo-relazionale* (oppure *ex ante*), dove la debolezza della vittima è insita in particolari condizioni *bio-fisiologiche* di cui la stessa è portatrice (quali, per esempio, l'età, il genere, l'orientamento sessuale e la disabilità).

In secondo luogo, si richiama una vulnerabilità in senso *oggettivo-situazionale*, ove sono l'illecito penale, le relative modalità di realizzazione e le finalità criminose perseguite a determinare una condizione di debolezza nella persona offesa dal reato (ad esempio, il terrorismo, la criminalità organizzata, la circolazione stradale, la tortura e gli infortuni sul lavoro)[20].

[15] ALLEGREZZA, *La riscoperta della vittima nella giustizia penale europea*, cit., p. 13.

[16] In argomento v., per esempio, F. TRAPELLA, *La tutela del vulnerabile. Regole europee, prassi devianti, possibili rimedi*, in «Arch. pen.» (web), 3 dicembre 2019; C. AMALFITANO, *La vittima vulnerabile nel diritto internazionale e dell'Unione europea*, in «Riv. it. med. leg.» (2018), p. 523 ss.; M. GIALUZ, *Lo statuto europeo delle vittime vulnerabili*, in *Lo scudo e la spada. Esigenze di protezione e poteri delle vittime nel processo penale tra Europa ed Italia*, a cura di S. Allegrezza, H. Belluta, M. Gialuz, L. Lupària, Giappichelli, Torino, 2012, p. 59 ss.

[17] Cfr. S.O. VALL-LLOVERA, *Manifestaciones del derecho a la protección de la seguridad e integridad de la víctima menor*, in *La víctima menor de edad. Un estudio comparado Europa/America*, a cura di T. Armentadeu e S.O. Vall-Llovera, Editorial Colex, Madrid, 2010, p. 202. Tali ragioni sono state peraltro riconosciute nelle conclusioni della Presidenza nella *Conference for the protection of vulnerable victims and their standing in criminal proceedings* svoltasi a Praga nel marzo 2009.

[18] Infatti, l'art. 22 della direttiva in oggetto stabilisce che «La valutazione individuale tiene conto, in particolare, degli elementi seguenti: a) le caratteristiche personali della vittima; b) il tipo o la natura del reato e; c) le circostanze del reato».

[19] Sulle differenti declinazioni della vulnerabilità nel diritto penale v. F. PALAZZO, *Soggetti vulnerabili e diritto penale*, in *La fragilità della persona nel processo penale*, a cura di G. Spangher e A. Marandola, Giappichelli, Torino, 2021, p. 94 ss.

[20] Per un maggior approfondimento delle differenti forme di manifestazione della vulnerabilità della vittima nella legislazione penale sia consentito a rinviare a M. VENTUROLI, *La vulnerabilità della vittima di reato quale categoria "a geometria variabile" del diritto penale*, in «Riv. it. med. leg.» (2018), p. 553 ss.

Queste due espressioni della particolare debolezza della vittima sono del resto compendiate all'art. 90-*quater*, c.p.p., introdotto nel 2015, il quale – senza fornire una definizione generale – si limita a riconoscere la condizione di specifica vulnerabilità della persona offesa alla luce di «tre tipologie di indici, riferibili rispettivamente alle caratteristiche della persona offesa (età, stato di infermità, deficienza psichica, eventuale dipendenza dall'autore del reato), a quelle del reato (tipo di illecito, modalità dell'azione, circostanze del fatto, violenza nel praticare la condotta) e alla finalità criminosa dell'agente (odio razziale, terrorismo, criminalità organizzata, discriminazione)»[21]. Viene in tal guisa a manifestarsi una categoria oltremodo elastica idonea a consentire l'esercizio della più piena discrezionalità – sotto il profilo processuale – da parte dei giudici nell'individuazione delle persone offese in concreto bisognose di specifiche forme di protezione, nonché – sotto il profilo sostanziale – da parte dei legislatori nelle proprie scelte di incriminazione.

Peraltro in particolari circostanze le due tipologie di vulnerabilità possono finanche combinarsi: si pensi alle varie forme di riduzione in schiavitù, che si caratterizzano per annientare la personalità della vittima, già talora contraddistinta da una intrinseca debolezza soggettiva (legata, ad esempio, all'età o alla condizione di disabilità).

La categoria della vulnerabilità appare in sostanza *storicizzata*, giacché il suo perimetro è venuto nel corso del tempo ad espandersi in ragione delle *trasformazioni socio-culturali* che hanno modificato la sensibilità comune verso precipue categorie di soggetti, e delle *trasformazioni tecnologico-produttive* capaci di generare nuove situazioni di pericolo per beni di differente natura. Con conseguenze nello specifico percepibili sul campo penale: con riferimento alle prime, può rammentarsi la differenza tra le forme di tutela accorate dal codice Rocco alla donna e il volto attuale della legislazione penale a protezione della stessa[22]; nonché l'esperienza di numerosi Paesi dell'area occidentale, dove si è passati in un arco temporale non troppo ampio dall'incriminazione delle relazioni omosessuali alla previsione di forme rafforzate di tutela nei confronti delle persone appartenenti alla comunità LGBTQ+[23]. Quanto alle seconde invece, si può ad esempio citare la risposta punitiva sempre più severa adottata nei confronti della criminalità stradale[24].

[21] Così Trapella, *La tutela del vulnerabile. Regole europee, prassi devianti, possibili rimedi*, cit., p. 9. Sulla nozione di cui all'art. 90-*quater*, c.p.p., v., tra gli altri, S. Quattrocolo, *Vulnerabilità e individual assessment*, in *Vittima di reato e sistema penale. La ricerca di nuovi equilibri*, a cura di M. Bargis e H. Belluta, Giappichelli, Torino, 2017, p. 301, secondo cui in generale «il concetto di vulnerabilità ha cominciato a delinearsi attraverso le sue conseguenze».

[22] In argomento cfr., per esempio, F. Basile, *Violenza sulle donne e legge penale: a che punto siamo?*, in «Criminalia» (2018), p. 463 ss.; A. Costantini, *Diritto penale e discriminazioni di genere*, in «GenIUS», 4 ottobre 2024, p. 1 ss.

[23] Al riguardo M. Nussbaum, *Disgusto e umanità. L'orientamento sessuale di fronte alla legge*, Il Saggiatore, Milano, 2011, pp. 66 ss., parla di un passaggio da una politica criminale del «disgusto», inteso come «un rifiuto fondamentale della piena umanità dell'altro», ad una «politica dell'umanità», contraddistinta da un atteggiamento che «coniuga il rispetto con la curiosità e la capacità di immaginare l'altro».

[24] In argomento v., per esempio, A. Roiati, *L'introduzione dell'omicidio stradale e l'inarrestabile ascesa del diritto penale delle differenziazioni*, in «Dir. pen. cont.», 1 giugno 2016.

Nei decenni più recenti l'evoluzione tecnologica ha financo generato una nuova figura di vittima vulnerabile, ovverosia la persona offesa dall'illecito realizzato grazie ai supporti informatici e telematici, la quale esibisce una forma di debolezza che potrebbe a primo acchito sfuggire all'osservatore. Più precisamente, il *cyber* delinquente può per un verso sfruttare una pregressa condizione di vulnerabilità della vittima, la cui minorata capacità di difesa risulta aggravata proprio dallo spazio virtuale dove viene commesso il reato (si pensi all'adescamento di minori online a fine di sfruttamento sessuale o di pedopornografia); oppure per altro verso può avvalersi della *rete* per la consumazione di illeciti penali a danni di individui privi di una pregresso *status* di debolezza (per esempio, truffe online e clonazione dei mezzi di pagamento elettronici). Tant'è che si è osservato come le vittime del cybercrime incarnino spesso il "cittadino medio", vale a dire quell'individuo le cui condizioni socioeconomiche e culturali lo collocano nella media nazionale[25]. In altre parole, si tratta una vulnerabilità che si *generalizza*: forse provocatoriamente, lo spazio virtuale potrebbe essere assimilato ad un novello *status di natura*, dove la vulnerabilità rappresenta una condizione *ontologica* di ogni essere umano[26].

Tornando alla dimensione eurounitaria, se si osservano in prospettiva sinottica i testi penali dell'Unione dedicati alla protezione di specifiche categorie di vittime, ci si può accorgere come i riferimenti alla modalità di realizzazione del reato online siano nel tempo incrementati, poiché la comunicazione digitale ha conosciuto forme sempre più sofisticate, utilizzabili con le più disparate finalità criminali[27].

In ogni modo, le due fonti penali dell'Unione in cui ricorre più spesso l'espressione "online" sono la direttiva 2019/713/UE concernente la lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti (dove la suddetta espressione compare otto volte)[28] e la recente direttiva 2024/1385/UE sulla lotta alla violenza

[25] Cfr. M. TONELLOTTO, *Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità*, in «Riv. vitt. crim. sic.», vol. XVI (2022), p. 13, il quale riporta gli studi in materia dei criminologi Yunger e Montoya. Questi ultimi rilevano come la condizione di vittima in questo contesto sia trasversale al genere e all'età, anche se per le frodi online si registra un maggiore scostamento verso le donne di età più avanzata rispetto alle vittime delle frodi tradizionali.

[26] Del resto, il superamento della vendetta privata a favore della monopolizzazione dell'uso della forza da parte dello Stato, che scaturisce dal *contratto sociale*, si verrebbe per l'appunto a giustificare nella condizione di debolezza in cui versa ciascun individuo. In argomento cfr., *amplius*, O. GIOLO, *Conclusione. La vulnerabilità e la forza: un binomio antico da ritematizzare*, in *Vulnerabilità, etica, politica, diritto*, a cura di M.G. Bernardini, B. Casalini, O. Giolo, L. Re, If Press, Roma, 2018, p. 347.

[27] Sul punto v., *amplius*, G. MAROTTA, *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, in «Riv. vitt. crim. sic.», vol. VI, 2012, p. 93, secondo cui «Le nuove tecnologie, da un lato, hanno prodotto indubbi effetti positivi, dall'accelerazione della diffusione culturale alla comunicazione tra "mondi" prima sconosciuti, dall'altro sono diventate anche strumento di nuove modalità devianti e criminali». Cfr., altresì, E. MAESTRI, *Stupri digitali: una questione di governance del cyberspazio*, in «Annali online della Didattica e della Formazione Docente», vol. 16, 27 (2024), p. 27.

[28] In argomento, con particolare riguardo alla trasposizione del testo eurounitario, v. G. JUCAN SICIGNANO, *Recenti innovazioni in tema di frodi e falsificazioni di strumenti di pagamento diversi dai contanti*, in «Sist. pen.», 9 (2022), p. 5 ss.

contro le donne e alla violenza domestica (dove tale espressione è impiegata ben cinquantotto volte)[29].

Rispetto alla direttiva in materia di frodi e falsificazione dei mezzi di pagamento viene in rilievo una vulnerabilità della vittima in senso *oggettivo-situazionale*, una vulnerabilità "diffusa" in quanto capace di coinvolgere chicchessia, spesso con un evento singolo; mentre nella direttiva 2024/1384 viene principalmente a manifestarsi una vulnerabilità in senso *soggettivo-relazionale*, che è sfruttata e acuita dal mezzo *telematico*, spesso attraverso plurimi episodi. Ed è proprio su quest'ultimo testo che si focalizzerà la lente d'ingrandimento nel prosieguo della trattazione, giacché tale scelta consente di riflettere in ordine al concetto di "violenza online", il quale ha acquisito nei tempi recenti una rilevanza fattuale vieppiù significativa[30], con il coinvolgimento di categorie soggettivamente deboli (minori, donne), alla cui tutela è per l'appunto rivolta la direttiva 2024/1385.

3. *La tutela delle vittime di violenza digitale nel quadro della direttiva 2024/1385/UE*

Muovendo dalla componente strettamente penalistica del testo, si può constatare che ben quattro dei sei obblighi di incriminazione previsti dallo stesso sono contraddistinti da una modalità online della condotta: condivisione non consensuale di materiale intimo o manipolato (art. 5), stalking online (art. 6), molestie online (art. 7), istigazione alla violenza o all'odio online (art. 8). Si tratta di una scelta politico-criminale empiricamente fondata, stante che lo spazio digitale ha reso possibili forme di offesa alla persona, in particolare contro le donne, talvolta estranee al perimetro di tipicità delle più tradizionali incriminazioni contro la libertà morale e sessuale, pensate per l'universo offline.

Da un profilo criminologico si può riscontrare una contiguità divenuta vieppiù stretta fra lo spazio digitale e quello reale: tanto è vero che forme di violenza iniziate nell'uno possono proseguire nell'altro e viceversa, magari pure intensificandosi nella loro potenzialità offensiva all'interno del *cyberspace* a causa appunto delle caratteristiche "esistenziali" di quest'ultimo, di cui la norma penale dovrebbe tenere conto[31]. Del resto, questa *intersezione* tra mondo reale e mondo virtuale sembra riprodursi sulla fisionomia stessa delle vittime della violenza online, le quali si incarnano essenzialmente in tre differenti figure: «quelle che sono state o sono abusate nell'ambito del proprio

[29] Per un puntuale commento della direttiva v. A. Massaro, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica: il possibile impatto sull'ordinamento italiano*, in «Sist. pen.», 3 (2025), p. 107 ss.

[30] https://www.istat.it/wp-content/uploads/2023/10/ESPOSITO-22Novembre-2023.pdf.

[31] Cfr. Maestri, *Stupri digitali: una questione di governance del cyberspazio*, cit., p. 28, il quale osserva che «Pur essendo una costruzione immateriale, il cyberspazio può essere percepito, udito e interagito. È caratterizzato da dinamicità, indefinito e in costante espansione; non esiste in isolamento ma è strettamente interconnesso con il mondo fisico. Le attività precedentemente svolte nello spazio fisico sono state trasferite nel cyberspazio, portando alla scoperta di nuove forme di criminalità che mirano alle fasce vulnerabili della società».

ambiente relazionale-sociale, le cui immagini di abusi sono distribuite attraverso i new media; quelle che sono adescate online e che successivamente sono abusate nel contesto reale; quelle che sono adescate ed abusate online»[32].

Negli anni più recenti si è statisticamente registrato un rapido incremento degli episodi di violenza via *web* ai danni delle donne, soprattutto durante l'emergenza pandemica, che ha indotto il legislatore europeo a predisporre una risposta preventivo-repressiva "mirata" verso tale fenomeno, anzitutto mediante obblighi d'incriminazione specifici, non ricompresi nella Convenzione di Istanbul[33]. Peraltro, proprio gli obblighi di penalizzazione connessi al mezzo digitale sembrano essere quelli supportati da una base giuridica più pacifica all'interno del TFUE, ovverosia riconoscibile nel concetto di «"criminalità informatica" che, essendo riferibile tanto ai reati informatici propri quanto ai reati informatici impropri, comprende senza difficoltà le forme di violenza online contro le donne»[34].

Le vittime della violenza online possono esibire sul piano personologico una vulnerabilità *rafforzata*, che la direttiva *de qua* sembra valutare: invero, nel *considerando* n. 17 della medesima, si afferma che i mezzi digitali sono capaci di «amplificare in modo significativo la gravità dell'impatto dannoso del reato», che può coinvolgere persone già di per sé vulnerabili (per genere, come nel testo in oggetto, muovendo dalla visione più tradizionale che riconnette *ex ante* al sesso femminile una vulnerabilità ontologica)[35]. Lo stesso *considerando* enuncia poi alcune categorie di donne più frequentemente destinatarie di questa forma di violenza, vale a dire le rappresentanti politiche, le giornaliste e difensore dei diritti umani e, dunque, figure *socialmente* più esposte ed affrancate dalle logiche culturali che alimentano i reati di genere.

In ragione della sua "insidiosità", la violenza digitale può provocare nelle corrispondenti vittime offese *multiple* – ovverosia alla tranquillità individuale, alla integrità psicofisica, alla libertà sessuale e, financo, alla dignità delle stesse – innescando talvolta un processo di "autovittimizzazione" nei suoi destinatari: a titolo di esempio, «La consapevolezza, da parte della vittima, soprattutto adolescente, di aver innescato, per ingenuità o imprudenza, il processo di diffusione delle proprie immagini intime porta, quasi sempre, a cambiamenti improvvisi nel comportamento, come ad esempio alterazioni delle abitudini alimentari (anoressia, bulimia), fobie, malesseri psicosomatici, atteggiamenti isterici

[32] G. Marotta, *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, cit., p. 97.

[33] Cfr. M. Ferrari, *Violenza contro le donne: l'Unione europea adotta finalmente la direttiva (UE) 2024/1385*, in «Eurojus.it rivista», 17 giugno 2024, p. 4. Sugli obblighi d'incriminazione della Convenzione di Istanbul v., tra gli altri, T. Vitarelli ed E. La Rosa, *L'attuazione della Convenzione di Istanbul nell'ordinamento italiano: profili di rilevanza penale*, in *Ordinamento internazionale diritto umani*, 2019, p. 1 ss.

[34] Massaro, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., p. 111.

[35] Cfr., al riguardo, le interessanti considerazioni di A. Massaro, *Il malinteso della donna come vittima vulnerabile: il diritto penale di fronte ai* gender-based crimes, in «GenIus», 3 gennaio 2025, p. 16, la quale critica l'idea diffusa di una vulnerabilità "intrinseca" della donna, affermando che «La donna, in conclusione, non è (giuridicamente) vulnerabile in quanto (ontologicamente) debole, ma solo se in quanto si trova ad essere vittima di determinati reati».

e di ribellione, disturbi del sonno, atti di autolesionismo e tentativi di suicidio»[36]. Senza contare, poi, che la distanza fisica esistente tra gli autori di siffatte condotte e le rispettive vittime può favorire una "de-personalizzazione" di queste ultime agli occhi dei primi; come pure che l'anonimato, di cui beneficiano spesso i *cyber* delinquenti (celati dietro *nikename*), può alimentare un timore generalizzato delle vittime verso il prossimo.

La violenza online incarna quindi un fenomeno criminoso *complesso*, in continuo divenire, rispetto al quale deve essere fornita una risposta *stratificata*, ripetutamente soggetta a rinnovamento, che passa attraverso la convergenza sinergica di strumenti preventivo-repressivi di differente natura[37], anche con riferimento alla protezione delle vittime.

E giustappunto in tale direzione sembra muoversi la direttiva 2024/1385, sulla scorta di quell'approccio *olistico* da tempo sperimentato dal diritto dell'Unione europea in materia. Infatti, accanto ai succitati obblighi d'incriminazione, essa stabilisce forme di tutela effettiva rivolte alle donne vittime di *cyber* violenza: più in particolare, gli Stati membri sono invitati a disporre canali accessibili e prontamente disponibili per denunciare atti di violenza, compresa la possibilità di sporgere denuncia e di presentare prove online almeno per i reati informatici; nonché a dotarsi di strumenti investigativi efficienti. Sulla falsariga del modello fatto proprio dalla direttiva 2012/29/UE, è previsto poi un *individual assessment* delle esigenze di protezione e assistenza delle vittime, mediante la predisposizione di appositi servizi di supporto, compresa la possibilità di emettere ordini urgenti di allontanamento e di protezione. Sono inoltre contenute nel testo alcune disposizioni per l'adozione di misure dirette alla rimozione del materiale online, per la limitazione delle prove sul comportamento sessuale passato della vittima e sul risarcimento integrale del danno.

Sono così le nuove tecnologie stesse a ricoprire un ruolo prezioso in quest'azione di tutela verso le vittime della violenza digitale, disvelando in tal modo una loro duplice fisionomia: strumento *criminogeno* da un lato e di *supporto* delle vittime di comportamenti violenti posti magari in essere servendosi delle medesime tecnologie dall'altro lato[38]. In ossequio agli insegnamenti oramai consolidati della vittimologia[39], la direttiva insiste poi sulla necessità che gli Stati provvedano alla *formazione* e all'*informazione* dei

[36] MAROTTA, *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, cit., p. 98.

[37] Lo stesso considerando 73 della direttiva evidenza una dimensione ampia della prevenzione del fenomeno in oggetto valorizzata dalla stessa, comprensiva di una prevenzione primaria, secondaria e terziaria. Secondo la direttiva, «Le misure preventive primarie dovrebbero mirare a prevenire il verificarsi della violenza e potrebbero includere azioni come campagne di sensibilizzazione e programmi educativi mirati per migliorare, presso il grande pubblico, la comprensione delle diverse manifestazioni di tutte le forme di violenza e delle loro conseguenze e per aumentare la conoscenza della nozione di consenso nelle relazioni interpersonali in età precoce. Le misure preventive secondarie dovrebbero mirare a individuare tempestivamente la violenza e a impedirne la progressione o l'escalation in una fase precoce. La prevenzione terziaria dovrebbe concentrarsi sulla prevenzione della recidiva e della rivittimizzazione e sulla corretta gestione delle conseguenze della violenza e potrebbe comprendere la promozione dell'intervento degli astanti, dei centri di intervento precoce e dei programmi di intervento».

[38] MASSARO, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., p. 109.

[39] Cfr., tra gli altri, S. SICURELLA, *Lo studio della vititmologia per capire il ruolo della vittima*, in «Riv. crim. vitt. sic.», 3 (2012), p. 69.

funzionari, come gli agenti di polizia e il personale giudiziario, che hanno la probabilità di entrare in contatto con le tipologie di vittime in parola. Si tratta di una esigenza più che mai avvertita rispetto alla persona offesa dall'illecito online, la quale è particolarmente esposta al rischio di *vittimizzazione secondaria*, che può essere appunto alimentato da un'inadeguata competenza degli appartenenti alle forze dell'ordine e alla magistratura a rapportarsi con le persone che hanno subìto questi "nuovi" reati, capaci d'intaccare la dimensione più intima dell'individuo.

4. (Segue) *I limiti dell'approccio* victim oriented *adottato dalla direttiva*

Si può in definitiva riconoscere una caratura *vittimologica* integrale al testo in parola, che orienta – come si è accennato – le modalità di risposta alla violenza contro le donne fornite dallo stesso. Ma proprio questa vocazione *victim oriented* della direttiva 2024/1385 se da un lato ne rappresenta un pregio, dall'altro lato alimenta verosimilmente alcune criticità dello stesso che agli occhi del penalista non possono sfuggire.

In primo luogo, come sovente accade nelle incriminazioni nate con esigenze di tutela delle vittime, anche gli obblighi di penalizzazione ricompresi nella direttiva *de qua* sono talora descritti con espressioni lessicali di origine sociologica, che dovrebbero riprodurre i fenomeni in termini "realistici, non sempre tuttavia capaci di assicurare le esigenze di determinatezza connesse al fondamento legalitario del nostrano diritto penale costituzionale[40]. Un esempio in tal senso emblematico si ritrova nello *stalking online* (art. 6 della direttiva), là dove è condizionata al carattere *continuativo* la penale rilevanza delle condotte con cui il soggetto agente sottoponga un'altra persona a sorveglianza tramite tecnologie dell'informazione e della comunicazione[41]. Si impiega un concetto temporale dal significato indefinito, il cui perimetro di tipicità deve essere in sostanza ricostruito dall'interprete.

In secondo luogo, la norma incriminatrice vittimocentrica si caratterizza talora per impiegare formule linguistiche non solo scarsamente determinate, ma anche deficitarie sul fronte dell'offensività[42], a cui il legislatore ricorre con un intento preventivo di anticipazione della soglia di tipicità dei fatti. Nel testo in esame potrebbero risultare problematiche in tal senso le ipotesi in cui la direttiva circoscrive l'illiceità penale delle condotte alla

[40] Sul punto sia consentito rinviare a M. VENTUROLI, *La "centralizzazione" della vittima nel sistema penale contemporaneo tra impulsi sovranazionali e spinte populistiche*, in «Arch. pen.» (web), 6 maggio 2021, p. 24. In merito alla dimensione costituzionale del principio di determinatezza v., per tutti, G. MARINUCCI, E. DOLCINI, G.L. GATTA, *Manuale di diritto penale. Parte generale*, Giuffrè, Milano, 2024, p. 82.

[41] Cfr. MASSARO, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., p. 120.

[42] Si tratta di un campionario piuttosto vasto, che spazia dalla materia del terrorismo ad alcune forme di negazionismo, passando attraverso la tutela penale dei "sentimenti"; sul punto v. M. DONINI, "*Danno" e "offesa" nella c.d. tutela penale dei sentimenti. Note su morale e sicurezza come beni giuridici, a margine della categoria dell'"offense" di Joel Feinberg*, in *Laicità, valori e diritto penale, The Moral Limits of the Criminal Law, in ricordo di Joel Feinberg*, a cura di A. Cadoppi, Giuffrè, Milano, 2010, p. 93.

loro attitudine a provocare «un danno grave» alle persone; circostanza, questa, espressiva di un disvalore di azione non sempre chiaramente riconoscibile, su cui si può dunque pervenire a soluzioni differenti a seconda delle diverse sensibilità dei giudici coinvolti[43]. Nondimeno, la direttiva in questione si mostra sul punto più prudente rispetto a precedenti testi penali dell'Unione, che si caratterizzano per incriminazioni assolutamente carenti in termini di offensività: il caso più significativo al riguardo è con verosimiglianza quello della pedopornografia virtuale, secondo quanto previsto all'art. 2, lett. c) *iii*, della direttiva 2011/92/UE, dove manca financo l'offesa ad una vittima in carne e ossa[44].

In terzo luogo, la fonte in esame non sembra adeguatamente promuovere le politiche preventive, diverse da quelle di natura penale, rivolte agli autori delle condotte di violenza contro le donne (anche online). Essa prevede certo da un canto (agli artt. 34 e ss.) l'obbligo, per gli Stati membri, di adottare misure capaci di contrastare gli stereotipi di genere dannosi, agevolando cambiamenti comportamentali in tutta la società (art. 34), compresi quelli radicati nei rapporti di potere storicamente iniqui tra uomini e donne o basati su ruoli stereotipati di donna e uomo (art. 35); tuttavia, dall'altro canto, omette per esempio di richiamare i programmi di recupero per uomini violenti (specie se indagati o imputati), che al contrario le legislazioni nazionali cominciano a predisporre, tra cui finanche quella italiana (per esempio, in rapporto agli obblighi cui può essere subordinata la sospensione condizionale della pena)[45].

È stato peraltro osservato che la direttiva, pur se nel *considerando* dieci riconosce nella violenza in oggetto «una manifestazione persistente della discriminazione strutturale nei confronti delle donne, derivante da rapporti di potere storicamente iniqui tra donne e uomini», non sembra adeguatamente valorizzare, nelle sue disposizioni, «il carattere strutturale e culturale della violenza contro le donne e della violenza domestica»[46], che imporrebbe un intervento mirato proprio per incidere sul retroterra culturale che favorisce il fenomeno[47].

[43] Perplessità sollevata al riguardo pure da MASSARO, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., p. 120.

[44] Forma d'incriminazione in cui – come osserva D. BRUNELLI, *Il diritto penale delle fattispecie criminose. Strumenti e percorsi per uno studio avanzato*, Giappichelli, Torino, 2019, p. 46 – «fa difetto qualunque offesa anche potenziale alla persona reale del minore, ma si punisce unicamente un '*tipo*' d'autore proclive all'immoralità, pedofilo virtuale, che manifesta appetiti sessuali disgustosi e riprovevoli».

[45] Cfr. MASSARO, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., p. 112. Quanto all'obbligo per gli autori di alcuni reati nelle relazioni strette di partecipare a specifici percorsi di recupero per poter beneficiare della sospensione condizionale della pena v. E. BIAGGIONI, *La nuova disciplina della sospensione condizionale della pena ex art. 165 co. 5 c.p.: prime indicazioni operative*, in *Osservatorio contro la violenza sulle donne*, n. 4/2021, in «Sist. pen.», 2 novembre 2021, § 4. Tuttavia M. DOVA, *La riforma Cartabia e il contrasto alla violenza contro le donne*, in «Sist. pen.», 6 marzo 2024, osserva che nel d.lgs. n. 150/2022, «Anziché scommettere sulla pena detentiva, si sarebbe potuto potenziare, in modo più coerente, la partecipazione ai programmi per maltrattanti, per valutarne, in modo più compiuto, gli effetti specialpreventivi».

[46] MASSARO, *La direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica*, cit., p. 112.

[47] In via generale COSTANTINI, *Diritto penale e discriminazioni di genere*, cit., p. 16, rileva condivisibilmente che «La ipervalorizzazione della componente "criminalizzante" delle fonti sovranazionali può finire, così, per

La promozione dei programmi di recupero per uomini maltrattanti, magari corredati a strumenti sanzionatori a carattere non detentivo (preferibilmente di natura *prescrittiva*)[48], verrebbe a valorizzare una dimensione solidaristico-risocializzativa della pena, trascurata dalle scelte punitive (perlopiù carcerarie) dell'Unione rispetto ai reati oggetto di armonizzazione[49], in ossequio alla vocazione spiccatamente generalpreventiva del diritto penale europeo[50].

A nostro avviso, pure attraverso il binario della sanzione penale si dovrebbe invece incoraggiare un intervento sui fattori di natura sociale lato *sensu* "causali" rispetto alla criminalità di genere, diretto a promuovere la comprensione dei gravi pregiudizi arrecati alle vittime della stessa, spesso *de-umanizzate* dagli autori; senza volere certo trascurare le esigenze di neutralizzazione del delinquente pericoloso più che mai imprescindibili nel contesto in oggetto, la cui dimensione artificiale consente al reo di "occultarsi" con facilità, e conseguentemente di reiterare i propri comportamenti violenti.

Nella succitata prospettiva di "revisione culturale" e di riconoscimento delle vittime si dovrebbe per esempio valutare l'ingresso della giustizia riparativa tra le strategie messe in campo nella risposta ai reati in discussione; ponderando, beninteso, le comprensibili resistenze manifestate verso l'applicazione della *restorative justice* al fenomeno della violenza nelle relazioni strette, in ragione della difficile compatibilità tra le caratteristiche strutturali di quest'ultima (in particolare, la sopraffazione dell'autore verso la vittima)[51] e gli elementi costitutivi del paradigma *dialogico-conciliativo* (specie la volontarietà della partecipazione ai programmi)[52].

offuscarne il messaggio più importante, costituito dalla necessità di incidere sulla matrice (ancora) fortemente culturale della violenza di genere». Rimarca altresì una non adeguata valorizzazione delle forme di prevenzione extrapenale nella legislazione dedicata al contrasto della violenza contro le donne M. BERTOLINO, *Violenza e famiglia: attualità di un fenomeno antico*, in «Riv. it. dir. proc. pen.» (2015), p. 1740; nella stessa direzione T. VITARELLI, *Violenza contro le donne e bulimia repressiva*, in «Dir. pen. cont. – Riv. trim.», 3 (2020), p. 478.

[48] Cfr., sul punto, E. CORN, Victimam non laedere. *Verso nuove pene per i reati commessi in contesto di relazioni strette tra autore e vittima*, Editoriale Scientifica Italiana, Napoli, 2023, p. 185 ss.

[49] Cfr. A. MARTUFI, *La potestà punitiva nel diritto UE. Differenziazione dei modelli di tutela e modulazione delle garanzie penalistiche*, Giappichelli, Torino, 2024, p. 229, il quale sottolinea «la tendenziale marginalizzazione delle sanzioni non custodiali nell'ambito delle pene edittali comminabili per i reati oggetto di armonizzazione».

[50] Cfr., volendo, M. VENTUROLI, *Modelli di individualizzazione della pena. L'esperienza italiana e francese nella cornice europea*, Giappichelli, Torino, 2020, p. 211 ss.

[51] Tant'è che secondo G. MANNOZZI, G.A. LODIGIANI, *La giustizia riparativa. Formanti, parole e metodi*, Torino, 2017, p. 358, «la vittima "ideale" rispetto a una gestione mediatoria del conflitto sia non già una vittima *debole*, bensì, ci si conceda il paradosso, una vittima *forte*».

[52] In argomento v., per esempio, A.AV.V., *Giustizia riparativa e violenza di genere: un relazione pericolosa?*, in «Sist. pen.», 9 dicembre 2024, raccolta di scritti che affrontano con accenti diversi il controverso rapporto tra i reati espressivi di una violenza di genere e la *restorative justice.*

5. *Considerazioni conclusive:* input *europei e politiche nazionali*

Al netto delle sue criticità, in larga misura espressive di una più generale cifra *ideologia* della legislazione penale europea, la direttiva 2024/1385 sembra predisporre un armamentario piuttosto articolato per la tutela delle vittime della violenza online, con cui viene a perfezionarsi una strategia di intervento già da tempo collaudata dall'Unione.

Sovrapponendo idealmente il testo della direttiva con l'ordinamento domestico, le carenze di quest'ultimo non sembrano particolarmente gravi, quantomeno sulla carta.

Senza potere in questa sede procedere ad un'analisi puntuale della normativa nazionale in materia, ci si limiterà a poche riflessioni di sintesi.

Il legislatore del nostro Paese si è già apparentemente mosso nella direzione tracciata dalla direttiva 2024/1385, ovverosia verso una tutela *integrata* delle vittime femminili (reali e potenziali) dei reati posti in essere attraverso le tecnologie dell'informazione e della comunicazione, al fine di rispondere ai numerosi bisogni di cui esse sono portatrici, sulla falsariga peraltro di quanto già in larga misura previsto dalla Convenzione di Istanbul.

Anzitutto, sul piano strettamente penale, solo alcuni sono gli obblighi di incriminazione fissati dalla direttiva rispetto ai quali l'ordinamento nostrano non risulta in tutto o in parte adempiente (per esempio, lo stalking online e le molestie online), con l'auspicio che siffatto adempimento avvenga tramite soluzioni capaci di contemperare le esigenze sottese agli obblighi stessi e i principi penalistici propri della tradizione costituzionale italiana.

Anche rispetto alle diversificate forme di supporto previste dalla direttiva a favore delle vittime dei reati di genere commessi online, la disciplina domestica sembra in buona misura già in linea con le prescrizioni europee: a titolo di esempio, pure in Italia è stata prevista l'istituzione di piattaforme informative *in rete*, di iniziative di sensibilizzazione attraverso i social media, di linee di ascolto telefonico, di siti web per le denunce, nonché la rimozione di immagini o video sessualmente espliciti su segnalazione della vittima, nel quadro di una più generale strategia di contrasto alla violenza contro le donne. In ogni caso, è necessario che tali strumenti di tutela siano effettivamente operativi, onde evitare che si verifichi una dissociazione tra le previsioni normative e la loro concretizzazione, come è stato rilevato giustappunto sul campo della tutela delle vittime della violenza nelle relazioni strette dal rapporto del Grevio; il quale ha riscontrato la principale criticità dell'ordinamento italiano nelle strategie di contrasto alla violenza contro le donne proprio nella distanza tra le disposizioni adottate in materia e la rispettiva attuazione, evidenziando segnatamente un'applicazione disomogenea delle stesse sul territorio nazionale e una carenza di finanziamenti necessari per garantirne l'effettività[53].

[53] Sul punto v. N.M. Cardinale, *Il rapporto del GREVIO sull'applicazione in Italia della Convenzione di Istanbul: il lavoro ancora da fare*, in https://www.criminaljusticenetwork.eu/it/post/il-rapporto-del-grevio-sull-applicazione-in-italia-della-convenzione-di-istanbul-il-lavoro-ancora-da-fare, 13 maggio 2021.

Tornando alla parte introduttiva di queste note, si può osservare che gli *input* dell'Unione europea hanno certo contribuito ad imprimere quella manifesta svolta vittimocentrica alla legislazione penale domestica dei decenni più recenti. Tuttavia, gli aspetti di quest'ultima ispirati alle più retrive logiche neoretribuzionistiche, osservati con preoccupazione dalla dottrina[54], non costituiscono prevalentemente il frutto di impulsi provenienti dall'Unione, ma rappresentano la risposta a quotidiane istanze di penalità che originano dall'"interno", vale a dire dalla *comunità*, veicolate dai mezzi di comunicazione e recepite a livello istituzionale per fini d'integrazione sistemica[55].

In definitiva i vincoli sovranazionali sono stati determinanti per lo sviluppo di una tutela "amministrativa" a favore della vittima di reato, terreno su cui il nostro legislatore ha tradizionalmente mostrato una scarsa attenzione. E forse l'esempio più significativo è sul punto offerto dall'istituto dell'indennizzo pubblico delle vittime dei reati intenzionali violenti, a cui si è giunti con estremo ritardo rispetto alle principali esperienze europee e solo a seguito di ripetute censure della Corte di giustizia, che hanno rilevato l'inadempimento delle prescrizioni contenute nella direttiva 20024/80/CE, per vero ancora oggi non del tutto rispettate[56]. Per giunta i vuoti di tutela sul campo dell'assistenza alle vittime di reato non sono mai stati adeguatamente denunciati dagli organi di informazione e dalle istituzioni (a cominciare dall'assenza di sportelli pubblici di ascolto omogeneamente distribuiti in tutte le regioni).

La tanto sbandierata attenzione *politico-mediatica* verso la vittima di reato si riduce invero in "litanie" standardizzate sull'inattitudine del sistema penale ad appagare quell'istanza di giustizia che sarebbe rivendicata da ogni persona offesa in nome di semplicistiche assolutizzazioni concettuali. D'altronde, una sensibilità *progettuale* verso i bisogni della vittima, espressiva di un umanesimo solidaristico di matrice costituzionale, non si presta ad una gestione "pubblicitaria" del tema, elettoralmente conveniente e a costo zero.

[54] Cfr., per esempio, C. BERNASCONI, *Dalla vittimologia al vittimocentrismo: cosa resta della tradizione reocentrica?*, in «Criminalia» (2021), p. 209 ss.; G. MINICUCCI, *Il diritto penale della vittima. Ricadute sistematiche e interpretative*, in «Discrimen», 17 ottobre 2020, p. 1 ss.

[55] Cfr. F. SGUBBI, *Il diritto penale totale. Punire senza legge, senza verità, senza colpa. Venti tesi*, il Mulino, Bologna, p. 33.

[56] Si veda, da ultimo, CGUE, sez. V, sent. 7 novembre 2024, U.D., in C-126/23; per un commento di tale pronuncia sia consentito rinviare a M. VENTUROLI, *Il sistema italiano di indennizzo pubblico a favore delle vittime dei reati intenzionali violenti nuovamente al vaglio della Corte di giustizia*, in «Riv. it. dir. proc. pen.» (2025), p. 382 ss.

RIPARARE L'ILLECITO ONLINE: IL RUOLO DELLA GIUSTIZIA RIPARATIVA

Elena Mattevi

SOMMARIO: 1. La giustizia riparativa applicata all'illecito online. – 2. Esperienze applicative. – 3. Le risposte riparative all'illecito online nella disciplina organica della *restorative justice*. – 4. La giustizia riparativa come modello autonomo/alternativo: il ruolo dei fornitori delle piattaforme online.

1. *La giustizia riparativa applicata all'illecito online*

Nell'ambito di una categoria ampia e sfuggente come quella di illecito online, uno spazio importante è occupato dai reati commessi attraverso le piattaforme digitali, che consentono a chiunque si crei un *account* di produrre contenuti e di interagire. L'ampiezza di questi fenomeni è ormai evidente. Il mese di dicembre 2009 ha rappresentato un momento decisivo in quanto, per la prima volta a livello mondiale, social *network* e *blog* sono diventati la destinazione più popolare per quanto riguarda il tempo trascorso nella rete, superando motori di ricerca, siti di informazione e di acquisto, giochi online e portali che per lungo tempo hanno rappresentato il punto di riferimento per il popolo di internet[1].

Visto che lo scopo di questo intervento è quello di riflettere sulle potenzialità della giustizia riparativa di fronte ai reati commessi in questo contesto, ci concentreremo sugli illeciti caratterizzati da una più chiara connotazione personalistica, e in particolare su quelli che consentono di puntare l'attenzione sulla relazione interpersonale esistente – e nella maggior parte dei casi compromessa dal reato – tra autore e persona offesa[2].

Si tratta di reati caratterizzati da modalità di offesa nuove ai beni giuridici tradizionalmente tutelati, come la libertà morale, l'onore o la reputazione e che sono in grado di produrre effetti dirompenti in conseguenza della natura immediata e pervasiva della comunicazione digitale.

Se ci riferiamo, solo a titolo di esempio, al cyberstalking, ai reati riconducibili al cyberbullismo, all'*hate speech*, alla pedopornografia online o alla condivisione non consensuale di immagini o video a contenuto sessualmente esplicito, entrano in gioco

[1] S. PASTA, *Razzismi 2.0. Analisi socio-educativa dell'odio online*, Schloé, Brescia, 2018, p. 60.

[2] R. BARTOLI, *Verso una rifondazione personalistica della querela. Spunti preziosi dall'ordinanza della Corte Costituzionale n. 106/2024*, in «Sist. Pen.», 11 (2024), p. 45.

condotte finalizzate a interferire, o che comunque finiscono per interferire negativamente, in modo significativo, nella vita quotidiana e sul benessere della vittima, che tuttavia si colloca spesso ad una significativa distanza, sul piano spaziale, dall'autore e, come tale, anche per questa ragione finisce per essere percepita come "de-umanizzata".

Dal lato dell'autore, alcune caratteristiche dell'agire online favoriscono infatti meccanismi di disinibizione e di deresponsabilizzazione: ci si percepisce come non identificabili, anonimi, in relazione al contesto di appartenenza, anche quando si usa il proprio nome, e progressivamente sempre di più nell'ipotesi in cui si usi un *nickname*, si utilizzino dati falsi o procedure ancora più complesse che garantiscono anonimato totale (come TOR, che permette una navigazione anonima sul web); a causa della menzionata distanza fisica, poi, si fa più fatica a percepire l'offesa arrecata alla vittima perché non la si vede, non la si guarda in faccia[3].

È decisiva, in particolare, la circostanza che il mezzo tecnologico – che dà vita ad un'interazione mediata che sostituisce la fisicità del corpo – non consente di regola di cogliere le emozioni altrui e quindi di reagire adeguatamente alle stesse e ai comportamenti che ne scaturiscono; per le sue intrinseche caratteristiche questo mezzo non permette di relazionarsi con esse e favorisce una sorta di analfabetismo emotivo. É proprio l'osservazione della risposta della persona offesa, con possibile condivisione della sua sofferenza, che al contrario – nel "mondo reale" – spesso causa, sul piano psicologico, effetti di inibizione dell'agire[4].

Dal lato della vittima alcuni effetti negativi che un reato di solito produce risultano addirittura amplificati in questo contesto e non solo per la rapidità con cui le notizie possono circolare. La mancata conoscenza o comunque il dubbio sull'identità dell'autore suscitano nuovi sentimenti di timore, causati dall'idea per cui il responsabile del reato potrebbe essere davvero chiunque, anche qualcuno di familiare; taluno che, peraltro, potrebbe abbandonare il mondo virtuale per materializzarsi in quello reale, in qualsiasi momento[5].

Se questo è l'orizzonte entro il quale la giustizia punitiva è chiamata ad offrire qualche risposta, è facile intuire perché invece molti dei reati sopra descritti potrebbero essere particolarmente adatti ad essere trattati con gli strumenti della giustizia riparativa, dando corso ad un processo «che consente alle persone che subiscono pregiudizio a seguito di un reato e a quelle responsabili di tale pregiudizio, se vi acconsentono liberamente, di partecipare attivamente alla risoluzione delle questioni derivanti dall'illecito, attraverso l'aiuto di un soggetto terzo formato e imparziale (da qui in avanti 'facilitatore')»[6].

[3] M. Lamanuzzi, *Il "lato oscuro della rete": odio e pornografia non consensuale. Ruolo e responsabilità dei gestori delle piattaforme social oltre la net neutrality*, in «LP», 24 maggio 2021, pp. 4 ss.

[4] S. Pasta, *Razzismi 2.0. Analisi socio-educativa dell'odio online*, cit., pp. 90 ss.

[5] A. Zizzola, *Restorative Justice Responses to Cyber Harm Cyberbullying, Cyberstalking and Online Abuse/ Harassment*, in https://www.euforumrj.org/restorative-justice-responses-cyber-harm.

[6] Questa definizione è offerta dalla Raccomandazione Rec(2018)8 del Comitato dei Ministri agli Stati membri sulla giustizia riparativa in materia penale, par. 3 dell'Appendice.

La letteratura internazionale offre alcune conferme a questa prima intuizione.

Si registrano, infatti, alcune esperienze interessanti che testimoniano l'uso di programmi riparativi in questi contesti, per quanto riguarda il cyberbullismo e il cyberstalking, l'*hate speech* nonché la condivisione di immagini a contenuto sessualmente esplicito, destinate a rimanere private.

La descrizione di queste sperimentazioni è accompagnata dai risultati delle indagini di vittimizzazione e dai dati raccolti in merito a ciò che le vittime provano e a ciò che si aspettano dal sistema giudiziario in tali circostanze. Si descrivono in particolare sentimenti quali la paura, il senso di colpa, l'impotenza, la vergogna o la rabbia – particolarmente accentuati nel caso di diffusione di materiale sessualmente esplicito[7] – che possono trovare tuttavia un luogo di espressione e accoglienza più idoneo nell'ambito di un programma di giustizia riparativa, piuttosto che in seno al sistema di giustizia penale formalizzato e istituzionale.

Un incontro realizzato anche a distanza – se ci sono ostacoli materiali per un incontro in presenza – tra *offender* e vittima di un reato commesso con le tecnologie dell'informazione e della comunicazione, allora, può essere vantaggioso innanzitutto per quest'ultima che può essere "riconosciuta" nella sua dimensione umana, esprimendo le proprie aspettative, le proprie debolezze e la propria sofferenza e dando finalmente un volto all'autore del reato.

Anche quest'ultimo, però, potrebbe uscire dall'incontro "riconosciuto" nei suoi limiti, nelle sue motivazioni e nelle sue opportunità riparatorie e più facilmente responsabilizzato, dopo aver guardato in faccia la vittima e compreso anche per tale via la portata dell'offesa che ha causato[8].

I programmi di giustizia riparativa, infatti, consentono alle vittime di avere uno spazio ed un tempo adeguato per descrivere al presunto autore della condotta illecita le conseguenze che il reato ha determinato nella loro vita e di sentirsi accolte in un contesto sicuro e idoneo a ricevere alcune risposte e magari anche una forma di riparazione; allo stesso tempo questi strumenti, grazie all'incontro, creano le condizioni affinché i colpevoli possano maturare una nuova consapevolezza in merito al disvalore della propria condotta; una coscienza, questa, che di regola riduce la probabilità di ricadere nel reato e quindi la recidiva[9].

Come in tutte le pratiche di giustizia riparativa, pure gli incontri che seguono la commissione di un illecito online devono essere ben preparati da facilitatori formati e hanno luogo solo se sono accettati volontariamente da tutte le parti.

[7] T.L.A.S. Robalo, R.B.B. Abdul Rahim, *Cyber Victimisation, Restorative Justice and Victim-Offender Panels*, in «Asian J. Criminol.», 18 (2023), pp. 61 ss.

[8] M. Button, C.M. Nicholls, J. Kerr, R. Owen. *Online fraud victims in England and Wales: victims' views on sentencing and the opportunity for restorative justice?*, in «Howard Journal of Crime and Justice», 54/2 (2015), pp. 193 ss.

[9] T.L.A.S. Robalo, R.B.B. Abdul Rahim, *Cyber Victimisation, Restorative Justice and Victim-Offender Panels*, cit., pp. 61 ss. Cfr. altresì J. Braithwaite, *Crime, shame and reintegration*, Cambridge University Press, Cambridge, 1989, *passim.*

Anche nell'ipotesi in cui l'autore o la vittima non esprimano il loro consenso alla partecipazione, nonché nell'ipotesi, non del tutto implausibile, in cui l'autore della condotta non sia stato identificato, la flessibilità che caratterizza la giustizia riparativa è tuttavia in grado di offrire qualche opportunità.

I processi di giustizia riparativa con vittime e/o autori del reato surrogati e addirittura le soluzioni più complesse che coinvolgono in uno stesso programma diverse vittime di reati simili che incontrano autori di reati simili (*Victim-Offender Panels*) costituiscono opzioni comunque praticabili[10].

2. *Esperienze applicative*

Se vogliamo riflettere sul modo in cui la giustizia riparativa può operare in concreto in questo contesto, può esser utile fare riferimento a qualche esperienza descritta nella letteratura internazionale.

Un programma di giustizia riparativa, per esempio, si è svolto nel Minnesota attraverso l'impiego di una *restorative conference* in un'ipotesi di pedopornografia.

Nel 2011, infatti, in una scuola media della contea di Wright, alcuni studenti, tra gli 11 e i 14 anni, avevano condiviso per via telematica con altri colleghi immagini sessualmente esplicite di una loro compagna dopo averle sottratte dal cellulare del suo ragazzo. In base alla disciplina nazionale questi ragazzi avrebbero potuto essere chiamati a rispondere del reato di detenzione e diffusione di materiale pedopornografico[11].

In seguito ad un'intesa raggiunta tra l'istituzione scolastica coinvolta, il procuratore della contea e l'ufficio dello sceriffo, il caso venne tuttavia inviato al *Wright County Restorative Justice Agent*, che avviò un programma di gruppo, organizzando una *conference* con quasi quaranta invitati tra studenti, genitori, il procuratore della contea, lo sceriffo, i responsabili della scuola e gli insegnanti.

La fase della raccolta del consenso fu, come sempre, assai delicata. Le maggiori resistenze alla partecipazione furono espresse da alcuni genitori convinti aprioristicamente che i loro figli fossero del tutto estranei ai fatti.

Il programma ebbe comunque esito positivo.

Il racconto della ragazza, in particolare, permise a tutti di comprendere nel dettaglio la portata offensiva della vicenda. Ella ebbe modo di spiegare che aveva desiderato solo condividere una foto intima con il ragazzo, mentre quell'immagine era entrata – senza il suo consenso – nella disponibilità di un numero non precisato di destinatari, producendo effetti devastanti sulla sua vita.

[10] C. McGlynn, *Seeking Justice for Image-based Sexual Abuse.Examining the Possibilities of Restorative and Transformative Justice Approaches*, in G.M. Caletti, K. Summerer (a cura di), *Criminalizing Intimate Image Abuse. A Comparative Perspective*, Oxford University Press, Oxford, 2024, pp. 343 ss.; T.L.A.S. Robalo, R.B.B. Abdul Rahim, *Cyber Victimisation, Restorative Justice and Victim-Offender Panels*, cit., pp. 61 ss.

[11] L'esperienza è descritta da N. Riestenberg, *Restorative group conferencing and sexting: repairing harm in Wright County*, 2014, in https://cyberbullying.org/restorative-group-conferencing-and-sexting, *passim.*

L'accordo raggiunto a chiusura del programma coinvolse a vario titolo tutti i partecipanti: gli studenti si scusarono, redassero una relazione scritta sui rischi connessi all'invio e alla ricezione di materiale pornografico minorile e si impegnarono per il futuro a segnalare immediatamente ai responsabili dell'istituzione scolastica eventuali casi di circolazione di immagini a contenuto sessualmente esplicito o altre informazioni a riguardo; i genitori si assunsero il compito di monitorare più da vicino l'uso del cellulare e di internet da parte dei figli; le istituzioni pubbliche e la scuola, infine, si impegnarono a dar corso a specifici progetti informativi per i genitori e per gli studenti concernenti il fenomeno del *sexting* e ad attività di sensibilizzazione per un uso consapevole della rete.

Un altro programma interessante, invece, ha coinvolto soltanto due adulti e si è svolto in Finlandia, nel 2018[12].

Il 18 agosto 2017, a Turku, città del sudovest della Finlandia, diverse persone vennero accoltellate nella Piazza del Mercato da un giovane di origine straniera. L'ondata di razzismo che si diffuse nella popolazione finlandese a seguito di questa vicenda indusse il giornalista Sami Koivisto a pubblicare un articolo di sostegno ai migranti, ai richiedenti asilo e alla comunità musulmana in generale che avevano subito pesanti discriminazioni dopo l'attacco.

Pochi giorni dopo l'articolo, però, la famiglia del giornalista fu minacciata di morte in un *forum* online dove venne pubblicata anche un'immagine a fumetti in cui l'omicidio veniva celebrato con caffè e torta.

La polizia, una volta identificato l'autore della condotta penalmente rilevante, prima di dar corso al procedimento penale, decise tuttavia di proporre al giornalista un programma di giustizia riparativa – condotto dagli agenti stessi – che, in ipotesi di esito positivo, avrebbe potuto condurre ad una definizione del procedimento in sede non giudiziale. Quasi un anno dopo la pubblicazione della minaccia, Koivisto aveva così l'opportunità di incontrare la persona che si era resa responsabile del fatto e, sebbene inizialmente riluttante, decise di accettare.

Nel novembre 2018 ebbe luogo l'incontro, durante il quale Koivisto ebbe la possibilità di descrivere l'impatto che il discorso d'odio aveva avuto sul suo lavoro, sulla sua famiglia e sulla sua vita quotidiana. Come egli ebbe modo di spiegare, la semplice narrazione del suo punto di vista lo aveva fatto sentire subito più libero ed "*empowered*".

L'uomo che lo aveva minacciato, dopo averlo ascoltato, si scusò e cerco di spiegargli le proprie ragioni. Dichiarò che pur comprendendo che ciò che era stato fatto non poteva essere cancellato, egli era profondamente dispiaciuto e disgustato per quanto aveva fatto; aggiunse altresì che non si sarebbe mai ritrovato in una situazione simile e non avrebbe mai scritto un messaggio come quello se non avesse partecipato ad un *forum* di discussione online.

[12] Cfr. S. Koivisto, *"The scariest thing was he's just a regular Finnish guy"*, 2019, in https://yle.fi/aihe/artikkeli/2019/11/06/face-to-face-with-a-man-who-wished-an-asylum-seeker-would-kill-my-family-the.

Il punto più interessante del racconto del giornalista è quello in cui egli si dice sorpreso che la persona seduta davanti a lui fosse solo un ragazzo finlandese "normale" con bambini piccoli a casa. Accade spesso, infatti, che la percezione della vittima in merito all'autore del reato – e anche allo stesso fatto illecito – cambi dopo un programma di giustizia riparativa e ciò è ancora più frequente se i reati sono commessi con strumenti tecnologici, senza che i protagonisti si siano mai visti prima. L'incontro con "il volto dell'altro" può aiutare la persona offesa a ridisegnare le false immagini che si siano formate in lei, unilateralmente.

Anche questa mediazione si concluse positivamente.

I partecipanti raggiunsero un accordo avente ad oggetto la scrittura a quattro mani di un articolo sui discorsi di odio, sul loro impatto economico, sul loro effetto sulla salute della nazione e sui rischi che essi fanno correre al mantenimento dell'armonia sociale.

3. *Le risposte riparative all'illecito online nella disciplina organica della* restorative justice

Se gli strumenti riconducibili alla giustizia riparativa possono intercettare plurime istanze che – a maggior ragione pensando a questo tipo di criminalità – non trovano accoglimento nella giustizia tradizionale, dobbiamo comunque chiederci se sia preferibile che essi rispondano ad una logica di autonomia/alternatività o di complementarità rispetto alla giustizia punitiva.

Uno sguardo anche superficiale al dibattito internazionale sulla nozione di giustizia riparativa ci rivela punti di vista ben poco convergenti, espressi da concezioni ancorate alla prevalenza della dimensione dell'incontro su quella della riparazione, o viceversa[13].

In una diversa prospettiva si coglie una contrapposizione teorica forte tra un'opzione purista ed un'opzione massimalista di *restorative justice*[14]. In quella "purista" di McCold, ad esempio, tale nuovo modello di giustizia deve essere concepito come integralmente alternativo ed estraneo a quello tradizionale, evitando di mutuarne metodi, prassi e concetti, rifiutando ogni forma di coazione e valorizzando il consenso, la volontarietà e l'informalità[15]. In quella "massimalista" di Walgrave, invece, la *restorative*

[13] Marshall si riferisce alla *restorative justice* come ad un "approccio *problem-solving*" al reato, o, più precisamente, ad un processo in cui tutte le parti interessate da un particolare reato si incontrano per decidere insieme come affrontare le conseguenze dell'offesa e le sue ripercussioni nel futuro (T.F. MARSHALL, *Restorative Justice. An Overview*, Home Office, London, 1999, p. 5). Al contrario, la dimensione della riparazione è valorizzata da autori come G. BAZEMORE, L. WALGRAVE, *Restorative Juvenile Justice: in Search of Fundamentals and an Outline for Systemic Reform*, in ID. (ed. by), *Restorative Juvenile Justice: Repairing the Arm of Youth Crime*, Criminal Justice Press, Monsey, 1999, p. 48, che propongono la seguente definizione di giustizia riparativa: «*every action that is primarily oriented towards doing justice by repairing the harm that is caused by crime*».

[14] Per un approfondimento cfr. F. REGGIO, *Giustizia dialogica*, Angeli, Milano, 2010, pp. 109 ss.

[15] P. MCCOLD, *Toward a Holistic Vision of Restorative Juvenile Justice: A Reply to the Maximalist Model*, in «Contemporary Justice Review» (2000), pp. 357 ss.

justice è solo «un'opzione nel fare giustizia, a seguito della commissione di un reato, che è primariamente orientata alla riparazione del danno individuale, relazionale e sociale causato da quel fatto criminoso»[16]. Il ricorso a percorsi e a soluzioni consensuali (mediazione, *restorative conferencing*, *sentencing circles*) è da preferire, ma non si esclude l'applicazione della sanzione penale o, addirittura, di forme di imposizione della riparazione, quando necessario.

Entrambe le prospettive sono abbracciabili, ma perché la seconda possa essere presa in considerazione è pur sempre necessario, in via preliminare, che il sistema della giustizia tradizionale possa concretamente ed efficacemente operare rispetto a quel fatto di reato. Quando si ha a che fare con l'illecito online, invece, gli ostacoli tecnici e giuridici – anche solo per quanto attiene alla legge applicabile e alla giurisdizione, in ipotesi di reati "a dimensione "transfrontaliera" – sono tali da non consentire di dare nulla per scontato.

Affrontando, quindi, – innanzitutto – le ipotesi più semplici, in cui gli ostacoli appena menzionati siano superabili e il sistema giudiziario nazionale possa intervenire efficacemente, un esempio molto chiaro di incontro tra la giustizia riparativa e quella punitiva – nel segno della complementarità – è offerto proprio dall'ordinamento italiano, grazie alla disciplina organica della giustizia riparativa, che è stata introdotta con il d.lgs. 10 ottobre 2022, n. 150 e che non prevede nessuna esclusione per queste forme di criminalità, essendo i programmi accessibili «senza preclusioni in relazione alla fattispecie di reato o alla sua gravità» (art. 44 c. 1), nonché «in ogni stato e grado del procedimento penale, nella fase esecutiva della pena e della misura di sicurezza, dopo l'esecuzione delle stesse e all'esito di una sentenza di non luogo a procedere o di non doversi procedere, per difetto delle condizione di procedibilità […] o per intervenuta causa estintiva del reato» (art. 44 c. 2).

Due specifici aspetti ci sembrano tuttavia meritevoli di essere evidenziati, se si vuole garantire un accesso sicuro ed efficiente a questi strumenti da parte di soggetti che esprimano un genuino consenso alla partecipazione.

Innanzitutto, non si possono sottovalutare i rischi di vittimizzazione secondaria ai quali la vittima è esposta anche nell'ambito dei programmi di *restorative justice*. La giustizia informale non è certo esente da rischi per la persona offesa, soprattutto quando si innesta su relazioni connotate dalla violenza, anche se perpetrata con strumenti tecnologici, e in particolare in caso di violenza domestica o di "violenza nelle relazioni strette", a prescindere dal genere, definita nel 18° "considerando" della Direttiva 2012/29/UE del Parlamento Europeo e del Consiglio del 25 ottobre 2012, che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato, come «commessa da una persona che è l'attuale o l'*ex* coniuge o partner della vittima

[16] L. Walgrave, *Restorative Justice, Self-interest and Responsible Citizenship*, Willan Publishing, Cullompton (Devon), Portland (Oregon), 2008, p. 21, dove, integrando la definizione di Bazemore and Walgrave, già citata, si legge: «*an option for doing justice after the occurrence of an offence that is primarily oriented towards repairing the individual, relational and social harm, caused by that offence*».

ovvero da un altro membro della sua famiglia, a prescindere dal fatto che l'autore del reato conviva o abbia convissuto con la vittima».

Possiamo pensare così, per esempio, a casi di cyberstalking che coinvolgono partners dove i soggetti abusanti che abbiano utilizzato tecnologie dell'informazione e della comunicazione per commettere il reato potrebbero strumentalizzare deliberatamente i programmi di giustizia riparativa solo per acquistare un controllo ancora più penetrante sulla vittima.

Più che pensare ad un'occasione di incontro – anche a distanza – tra le parti, in queste circostanze potrebbe essere necessario adottare degli ordini di protezione per tutelare la persona offesa; gli ordini potrebbero comprendere il divieto per l'indagato di accedere a determinate località, di avvicinarsi alla vittima o alle persone a carico a una distanza inferiore a quella prescritta o di contattarla, anche attraverso interfacce online[17].

La disciplina organica della giustizia riparativa, del resto, si mostra cauta sul punto, nel momento in cui richiede un duplice, imprescindibile, vaglio di fattibilità dei programmi. L'art. 129-*bis* c.p.p., innanzitutto, prevede che l'invio ai Centri degli interessati sia disposto dall'autorità giudiziaria, qualora reputi che lo svolgimento di un programma di giustizia riparativa possa essere utile alla risoluzione delle questioni derivanti dal fatto per cui si procede e non comporti un pericolo concreto per gli interessati e per l'accertamento dei fatti. È quindi necessario che l'autorità giudiziaria, soprattutto di fronte a forme di criminalità come queste, si ponga il problema della sicurezza delle vittime e apra le porte ai programmi solo se non ci sono rischi concreti per loro.

Superato questo primo vaglio – che potrebbe mancare solo in ipotesi di accesso precedente alla presentazione della querela – interviene un secondo momento di valutazione gestito dai mediatori esperti, due per ogni procedura (art. 53 d.lgs. 150/2022) ed auspicabilmente formati in modo adeguato, che si articola in alcuni passaggi obbligati, ma che si conclude proprio con il giudizio definitivo sulla fattibilità del programma che segue allo svolgimento degli incontri preliminari (art. 54, c. 1, d.lgs. 150/2022).

Altro profilo di ancora più spiccata specificità è quello concernente le modalità attraverso le quali il programma potrebbe essere gestito in presenza di illeciti online.

Se, da un lato, l'incontro dovrebbe avvenire di regola in presenza, nel mondo "reale", per consentire ai protagonisti di guardarsi finalmente in faccia e di dialogare liberamente – ricorrendo anche al linguaggio non verbale –, dall'altro lato non si possono sottovalutare i costi, non solo economici, che in alcune occasioni si devono sostenere per rendere possibile l'incontro tra persone che sono residenti in luoghi distanti tra loro, ma che la rete ha "avvicinato"; costi che, in concreto, potrebbero impedire del tutto lo svolgimento dei programmi. Proprio nei casi da ultimo citati, allora, i mediatori dovrebbero poter proporre anche incontri da remoto, con lo scopo di favorire un percorso che altrimenti non potrebbe neppure iniziare.

[17] Cfr. sul punto il Considerando 45 della Direttiva 2024/1385 "sulla lotta alla violenza contro le donne e alla violenza domestica".

Nel d.lgs. 150/2022 non è stata inserita una disciplina della *restorative justice* in forma telematica. Si parla soltanto di «spazi e luoghi adeguati allo svolgimento dei programmi e idonei ad assicurare riservatezza e indipendenza» (art. 55 d.lgs. 150/2022), ma si dà quasi per scontato che gli spazi e i luoghi siano "fisici".

Nell'ambito della disciplina della mediazione civile, invece, la mediazione telematica ha rappresentato già da tempo una via praticabile, se disciplinata dal regolamento dell'organismo di mediazione, prima di divenire ampiamente accessibile durante il periodo di emergenza epidemiologica, a partire dal d.l. 17 marzo 2020 n. 18, e di fare un significativo salto di qualità con l'art. 8 *bis* d.lgs. 4 marzo 2010 n. 28, introdotto dal d.lgs. 10 ottobre 2022 n. 149, e con l'art. 8 *ter* d.lgs. 28/2010, che disciplina la mediazione da remoto, introdotto dal d.lgs. 27 dicembre 2024 n. 216. Oggi possiamo affermare che alle parti è riconosciuto un vero e proprio diritto di partecipare all'incontro con collegamento audiovisivo da remoto.

L'esperienza incoraggiante maturata in materia civile potrebbe favorire lo sviluppo di una maggior fiducia negli strumenti tecnologici, anche per quanto riguarda la *restorative justice*. Se nella disciplina organica in vigore non si ravvisano ostacoli insuperabili allo svolgimento di incontri da remoto – nei casi in cui il "luogo" e lo "spazio" adeguato sia proprio quello virtuale – sarebbe comunque auspicabile che si addivenisse al più presto ad una specifica disciplina in materia. È indispensabile che si prevedano degli accorgimenti utili a garantire la riservatezza del percorso, mentre non è certo opportuno che si arrivi a riconoscere alle parti un diritto alla mediazione a distanza analogo a quello che può essere esercitato nell'ambito della mediazione civile. Per quanto riguarda la *restorative justice*, infatti, è sempre preferibile che sia il mediatore a valutare se ci sono i presupposti per ammettere il ricorso agli strumenti tecnologici, tenuto conto delle informazioni raccolte negli incontri preliminari e del consenso espresso dalle parti.

Un'apertura in questa direzione pare imposta anche dagli strumenti normativi sovranazionali. La Direttiva 2024/1385 "sulla lotta alla violenza contro le donne e alla violenza domestica", nel Considerando 30, per esempio, si sofferma sull'opportunità di sporgere denuncia online o tramite altre tecnologie dell'informazione e della comunicazione accessibili e sicure «per denunciare la violenza contro le donne o la violenza domestica, almeno per quanto riguarda i reati informatici di condivisione non consensuale di materiale intimo o manipolato, lo *stalking* online, le molestie online, l'istigazione alla violenza o all'odio online, definiti nella presente direttiva. La vittima dovrebbe poter caricare materiale relativo alla denuncia, ad esempio *screenshot* che attestino la presunta condotta violenta». L'art. 14 della Direttiva impone agli Stati membri di garantire alle vittime questa possibilità.

Se per alcune forme di reati commessi mediante le tecnologie sopra descritte l'accesso alla giustizia tradizionale deve poter avvenire anche attraverso strumenti informatici, una giustizia inclusiva come quella riparativa non può precludere del tutto questa alternativa, in presenza di ragioni serie.

4. *La giustizia riparativa come modello autonomo/alternativo: il ruolo dei fornitori delle piattaforme online*

Se immaginiamo, invece, una giustizia riparativa che, anche solo per necessità, si ponga come alternativa – o che sia comunque autonoma – rispetto a quella punitiva, decisivo ci sembra il ruolo promozionale che innanzitutto potrebbe essere svolto direttamente dai fornitori delle piattaforme online[18]. Come anticipato, quest'opzione merita di essere considerata con speciale attenzione di fronte a queste forme di criminalità, vista la frequente incapacità della giustizia punitiva di intervenire in modo efficace.

I fornitori delle piattaforme, a prescindere dalle questioni classiche che possono porsi in tema di giurisdizione o di legge applicabile, e a prescindere dagli obblighi esecutivi, di segnalazione o di mitigazione dei rischi a loro carico, derivanti dall'impatto della tecnologia sui diritti fondamentali, che già discendono dal Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE, il c.d. *Digital Services Act*, sono chiamati a partecipare alla *governance*, intesa come coordinamento tra soggetti privati e pubblici coinvolti nella gestione della rete, mediante iniziative di autoregolamentazione e di coregolamentazione, ai fini del contrasto alla diffusione di contenuti illegali online, per la tutela degli utenti. Queste iniziative sono stimolate proprio dalla natura trasnazionale, delocalizzata e in perenne evoluzione del mezzo della rete stessa, che mette in discussione l'assoluta centralità dello Stato[19].

Proprio nel quadro di tali regolamentazioni dovrebbe essere disciplinato e garantito anche l'accesso alla giustizia riparativa.

Il *Digital Services Act* già prevede – ad altri fini – che i fornitori di piattaforme online offrano un sistema interno di gestione dei reclami contro le decisioni da loro prese all'atto del ricevimento di una segnalazione in merito all'illegalità di contenuti pubblicati o alla loro incompatibilità con le condizioni generali (art. 20).

I destinatari del servizio, compresi le persone o gli enti che hanno presentato segnalazioni, hanno poi diritto di scegliere un organismo di risoluzione extragiudiziale delle controversie certificato ai fini della definizione conciliativa delle liti inerenti a tali decisioni, compresi i reclami che non è stato possibile risolvere mediante il sistema

[18] Nel Considerando 13 del *Digital Services Act* si precisa che «le piattaforme online, quali le reti sociali o le piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali, dovrebbero essere definite come prestatori di servizi di memorizzazione di informazioni che non solo memorizzano informazioni fornite dai destinatari del servizio su richiesta di questi ultimi, ma diffondono anche tali informazioni al pubblico, su richiesta dei destinatari del servizio». All'art. 3 lett. i) viene offerta la definizione di piattaforma online: «un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento».

[19] S. Pasta, *Razzismi 2.0. Analisi socio-educativa dell'odio online*, cit., pp. 144 s.

interno di gestione. I fornitori di piattaforme online provvedono affinché le informazioni in merito alla possibilità di avere accesso a una risoluzione extragiudiziale delle controversie siano facilmente accessibili sulla loro interfaccia.

Così, sulla falsariga di questo modello, si potrebbe implementare un sistema del tutto autonomo – ancorché non necessariamente alternativo (in termini di *aut aut*) alla giustizia tradizionale – di giustizia riparativa, che coinvolga autori e vittime (in accezione individuale o diffusa, seppur con qualche maggiore difficoltà operativa in questo secondo caso) e che sia gestito da organismi specializzati, distinti da quelli chiamati ad occuparsi della relazione tra il fornitore della piattaforma e il destinatario del servizio, *ivi* incluso il segnalante.

Fermi gli obblighi di rimozione di contenuti illeciti e, se necessario, di segnalazione alle autorità giudiziarie, dovrebbero essere proprio le piattaforme a mettere a disposizione gratuitamente degli organismi – formati da professionisti mediatori – che siano "riconosciuti" attraverso un sistema di certificazione, che faccia capo al coordinatore dei servizi digitali dello Stato membro in cui è stabilito l'organismo stesso, sulla scorta di quanto indicato dal *Digital Services Act* per i già citati enti di risoluzione extragiudiziale delle controversie *ivi* contemplate (art. 21 c. 3). L'accesso ai programmi di giustizia riparativa dovrebbe di regola avvenire tempestivamente – superando gli ostacoli legati alla territorialità degli interventi più classici e alla stessa nozione, in concreto non sempre condivisa dagli interessati, di illecito online – su richiesta delle vittime, che avrebbero comunque il diritto di continuare a rivolgersi altresì alla giustizia tradizionale, con i limiti che questa presenta. Non è tuttavia da escludersi anche un accesso su istanza dell'*offender*.

Il programma, sempre con il consenso dei partecipanti, potrebbe essere attivato anche in ipotesi di conflitto tra i partecipanti in merito al livello di tollerabilità di un certo contenuto offensivo ospitato dalle piattaforme.

In questo orizzonte la giustizia riparativa potrebbe assumere una valenza davvero autonoma e, in tal senso, rivoluzionaria, anche per i casi in cui una condanna giudiziale sarebbe difficile da ottenere[20].

La prospettiva ci sembra incoraggiante, sebbene alcuni ostacoli siano innegabili. Non vi è dubbio, infatti, che il consenso degli interessati, stella polare della *restorative justice*, non può non condizionare l'accesso ai programmi e ne rappresenta un limite fisiologico, che, al contrario, la risposta penale, per il suo carattere coercitivo, non incontra.

Anche solo considerando questa caratteristica ineliminabile del modello, quindi, è molto difficile dire se per questa via la *restorative justice* potrà contribuire nel tempo a trainare la logica punitiva verso una logica più riparativa e più attenta alle esigenze delle vittime, nel rigoroso rispetto dei principi europei e internazionali in materia. Il tasso elevato di ineffettività della giustizia punitiva nel contesto dei reati commessi per

[20] A. Zizzola, *Restorative Justice Responses to Cyber Harm Cyberbullying, Cyberstalking and Online Abuse/ Harassment*, cit., *passim.*

via telematica non può tuttavia che sollecitare un serio investimento anche in questa direzione, con la messa a disposizione di strumenti riparativi accessibili a tutti coloro che siano interessati ad utilizzarli e accompagnati dalle precauzioni necessarie per assicurare la sicurezza delle parti.

ELENCO E QUALIFICHE DEGLI AUTORI

Olimpia Barresi, Assegnista di ricerca in diritto penale nell'Università di Bologna.

Malaika Bianchi, Professoressa associata di diritto penale nell'Università di Parma.

Emanuele Birritteri, Ricercatore in diritto penale nell'Università di Roma Unitelma Sapienza.

Matilde Botto, Assegnista di ricerca in diritto penale nell'Università di Bologna.

Sofia Braschi, Ricercatrice in diritto penale nell'Università di Pavia.

Corrado Caruso, Professore ordinario di diritto costituzionale nell'Università di Bologna.

Anna Costantini, Ricercatrice in diritto penale nell'Università di Torino.

Federico Ferri, Ricercatore in diritto dell'Unione europea nell'Università di Bologna.

Roberto Flor, Professore associato di diritto penale nell'Università di Verona.

Alessandra Galluccio, Professoressa associata di diritto penale nell'Università Statale di Milano.

Antonella Massaro, Professoressa associata di diritto penale nell'Università Roma Tre.

Elena Mattevi, Ricercatrice in diritto penale nell'Università di Trento.

Beatrice Panattoni, Assegnista di ricerca in diritto penale nell'Università di Verona.

Caterina Paonessa, Professoressa associata di diritto penale nell'Università di Firenze.

Andrea Perin, Professore associato di diritto penale nell'Università di Brescia.

Monica Tortorelli, Ricercatrice in diritto penale nell'Università del Molise.

Marco Venturoli, Professore associato di diritto penale nell'Università di Ferrara.

Arianna Visconti, Professoressa associata di diritto penale nell'Università Cattolica del Sacro Cuore.

L'elenco completo delle pubblicazioni
è consultabile sul sito

www.edizioniets.com

alla pagina

http://www.edizioniets.com/view-Collana.asp?Col=Jura. Temi e problemi del diritto

Pubblicazioni recenti

STUDI

discipline penalistiche

- Kolis Summerer, Matteo L. Mattheudakis, Gian Marco Caletti (a cura di), *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea*, 2025
- Gianfranco Martiello, *La tutela penale dell'agente pubblico dalle aggressioni del privato: una indagine di parte speciale*, 2025
- Gherardo Minicucci, *La plurisoggettività nell'agire colposo. Una rilettura in chiave normativa*, 2025
- Caterina Paonessa, *Giudizi prognostici e diritto penale. Luoghi, funzioni, garanzie*, 2024
- Rosa Palavera, *Sul dolo. Promuovere, discernere, recuperare volizioni nel sistema penale*, 2020
- Caterina Iagnemma, Error in deliberando*. Scelte e gestioni fallaci della condotta nell'illecito colposo*, 2020
- Gianfranco Martiello, *I limiti penali dell'uso della forza pubblica: una indagine di parte generale*, 2019
- Rosa Palavera, *Scienza e senso comune nel diritto penale. Il ricorso problematico a massime di esperienza circa la ricostruzione della fattispecie tipica*, 2017
- Guido Casaroli, Fausto Giunta, Roberto Guerrini, Alessandro Melchionda (a cura di), *La tutela penale della sicurezza del lavoro. Luci ed ombre del diritto vivente*, 2015
- Kolis Summerer, *Causalità ed evitabilità. Formula della* condicio sine qua non *e rilevanza dei decorsi causali ipotetici nel diritto penale*, 2013
- Giulio De Simone, *Persone giuridiche e responsabilità da reato. Profili storici, dogmatici e comparatistici*, 2012
- Giulio Paoli, *Fare l'avvocato (con l'arringa nel processo Majorana e scritti vari)*, a cura di Mario Pisani, 2011
- Cristina de Maglie, *I reati culturalmente motivati. Ideologie e modelli penali*, 2010
- Gabrio Forti, Maurizio Catino, Francesco D'Alessandro, Claudia Mazzucato, Gianluca Varraso (a cura di), *Il problema della medicina difensiva. Una proposta di riforma in materia di responsabilità penale nell'ambito dell'attività sanitaria e gestione del contenzioso legato al rischio clinico*, 2010
- Caterina Paonessa, *Gli obblighi di tutela penale. La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari*, 2009
- Stefano Canestrari, Fausto Giunta, Roberto Guerrini, Tullio Padovani (a cura di), *Medicina e diritto penale*, 2009
- Costanza Bernasconi, *Il reato ambientale. Tipicità, offensività, antigiuridicità, colpevolezza*, 2008

Edizioni ETS
Palazzo Roncioni - Lungarno Mediceo, 16, I-56127 Pisa
info@edizioniets.com - www.edizioniets.com
Finito di stampare nel mese di dicembre 2025