CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

3/2025

Editore Associazione "Progetto giustizia penale", c/o Università degli Studi di Milano,
Dipartimento di Scienze Giuridiche "C. Beccaria" - Via Festa del Perdono, 7 - 20122 MILANO - c.f. 97792250157
ANNO 2025 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

I contributi da sottoporre alla Rivista possono essere inviati al seguente indirizzo mail: editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Contents

Contents

Contents

Diritti fondamentali e nuove sfide
Derechos fundamentales y nuevos desafíos
Fundamental Rights and Emerging Challenges

Quis custodiet ipsos custodes? La responsabilità delle piattaforme digitali per gli illeciti penali degli utenti

Modelli a confronto dal "*Good Samaritan*" al *Digital Services Act*

¿Quién vigila a los vigilantes? La responsabilidad de las plataformas digitales por los contenidos ilícitos de los usuarios

Comparación de modelos desde el "Buen Samaritano" hasta la Digital Services Act

Who's Watching the Watchers? The Liability of Digital Platforms for Users' Criminal Offenses

Comparing models from the "Good Samaritan" to the Digital Services Act

Paolo Beccari
Dottorando di ricerca in diritto penale nell'Università di Bologna
paolo.beccari3@unibo.it

Reati informatici e a mezzo internet, Libertà di espressione

Delitos informáticos, Libertad de expresión

Cybercrimes, Freedom of Expression

Abstracts

Il contributo analizza il ruolo e la responsabilità delle piattaforme digitali nella moderazione dei contenuti online, in un contesto spesso definito come una "*no law's land*". Dalla constatazione inziale di un'incerta attribuzione di responsabilità, soprattutto nel panorama italiano, emerge la tensione tra inerzia regolativa ed effetti lesivi derivanti dall'inazione delle piattaforme. Il saggio ricostruisce le origini normative del problema, esaminando il ruolo della *Section 23*0 del *Communications Decency Act* statunitense e della Direttiva E-commerce europea, soffermandosi poi sui modelli più recenti di law enforcement, dal modello tedesco della *NetzDG* al *Digital Services Act* dell'Unione europea, interrogandosi sull'ampia nozione di «*illegal content*» e sulle difficoltà di coniugare *legal standards* e *policy standards* di fronte agli illeciti penali online, nel necessario bilanciamento tra libertà di espressione, tutela degli interessi degli utenti e responsabilità degli intermediari.

El trabajo analiza el rol y la responsabilidad de las plataformas digitales en la moderación de contenidos en línea, en un contexto a menudo descrito como una "tierra sin ley". A partir de la constatación inicial de una atribución incierta de responsabilidad —especialmente en el panorama italiano—, emerge la tensión entre la inercia regulatoria y los efectos perjudiciales derivados de la inacción de las plataformas. El trabajo reconstruye los orígenes normativos del problema, examinando el papel de la Section 230 del *Communications Decency Act* estadounidense y de la Directiva de Comercio Electrónico europea, y se detiene luego en los modelos más recientes de aplicación de la ley, desde el modelo alemán de la NetzDG hasta el *Digital Services Act* de la Unión Europea. Asimismo, reflexiona sobre la amplia noción de "contenido ilegal" y las dificultades de armonizar los estándares jurídicos y los estándares de política interna frente a los ilícitos penales en línea, en el necesario equilibrio entre la libertad de expresión, la protección de los intereses de los usuarios y la responsabilidad de los intermediarios.

The paper examines the role and responsibility of digital platforms in moderating online content, in a context often described as a "no law's land." Starting from the initial observation of an uncertain allocation of responsibility—particularly in the Italian landscape—the analysis highlights the tension between regulatory inertia and the harmful effects stemming from platform inaction. The essay retraces the regulatory origins of the issue, examining the role of Section 230 of the U.S. Communications Decency Act and the European E-commerce Directive, and then focuses on more recent models of law enforcement, from the German NetzDG to the European Union's Digital Services Act. It explores the broad notion of "illegal content" and the challenges of reconciling legal standards and policy standards when addressing online criminal offenses, within the necessary balance between freedom of expression, user protection, and intermediary liability.

Sommario

1. Premessa. *No law's land*. Il ruolo delle piattaforme digitali nell'epoca del *Web*.

Post-truth era, l'età della "verità secondaria", della verità in secondo piano[1]. Altrimenti, secondo una traduzione decisamente più libera e qui giocata sull'anglicismo: l'epoca della "verità in un *post*", della "verità in tasca", potenzialmente priva di ogni fondamento di obiettività.

In questo duplice significato potrebbe compendiarsi la «rivoluzione»[2] determinata dall'avvento del Web, che ha visto l'utente divenire, da mero fruitore di contenuti, loro creatore e primo diffusore. L'idea della piena democratizzazione della conoscenza attraverso la rete, inaugurata alle soglie degli anni Novanta nel solco di un'algida navigazione dei contenuti[3], si è successivamente fondata, cioè, sulla progressiva e costante interazione *online* tra soggetti[4], sospingendo il veicolo del sapere tra i canoni dell'istantaneità e della disintermediazione. E tale veicolo – ben più della stessa rete – è divenuto proprio l'utente del Web, assegnatario di una nuova primazia: custodita, da un lato, nella possibilità di esprimersi in modo istantaneo, affidando il proprio pensiero alla rete con un semplice "*clic*" per discutere dei temi più vari con una platea potenzialmente indeterminata; dall'altro, nella facoltà di intervenire in via diretta, senza alcuna necessità di strutture e figure rappresentative delle proprie istanze.

A ben guardare, la primavera della post-verità risiede proprio nella significativa irrilevanza (se non nella sostanziale assenza) di corpi intermedi e dei tradizionali attori istituzionali della società, il cui annullamento può tuttavia rappresentare, come un'innovazione di portata rivoluzionaria, così anche il segno evidente di una «crisi epistemica»[5]. Non rileva più, infatti, *ciò* che viene detto né *da chi* viene detto, ma la possibilità immediata per *chiunque* di discuterne: così ogni cosa è posta in discussione e privata di fondamento[6]. Nell'interazione costante, priva di ostacoli e disancorata dalla verità, centrale è il tema della tutela delle libertà individuali, di difficile ancoraggio e tutela nella dimensione virtuale[7]. Quest'ultima diviene infatti un «Far

[1] La cui origine risale – secondo gli Oxford Dictionaries – al gennaio 1992, quando esso venne impiegato dal drammaturgo Steve Tesich in un articolo per la rivista statunitense *The Nation*, con riferimento all'avversione per le "verità scomode" («*uncomfortable truths*») sviluppata dagli americani a partire dalla vicenda "Watergate" nel 1972, sotto la presidenza di Richard Nixon, in seguito proseguita con la copertura offerta dalla società statunitense allo scandalo "*Iran-Contra affair*" durante il mandato di Ronald Reagan e, ancor più tardi, durante la prima guerra del Golfo. Un'epoca, dunque, di inaugurazione essenzialmente "popolare" secondo Tesich: «[*i*]*n a very fundamental way we, as a free people, have freely decided that we want to live in some post-truth world*» (cfr. S. Tesich, *"A Government of Lies"*, in *The Nation*, 6-13 gennaio 1992, 12-14). Per un impiego più recente del *post-truth era*, si veda Keyes (2004). Il termine *post-truth* è infine "riemerso" nel corso del 2016, nell'ambito delle *fake news* diffuse nell'ambito della c.d. "Brexit" e della campagna elettorale per le elezioni presidenziali statunitensi, infiltrate dalla propaganda russa e infine vinte dal candidato repubblicano Donald Trump. In argomento, in ambito italiano, per tutti, Guerini (2020).

[2] Sul termine, Floridi (2014), *passim*. In Italia, in ambito penalistico, Picotti (2023), p. 34, per cui, rispetto al fenomeno tecnologico, «[s]i deve parlare di "rivoluzione" proprio perché esso investe ogni sfera della vita e degli interessi delle persone e della collettività». Ancora, in riferimento al contesto italiano, ma in ambito costituzionalistico, Pollicino (2014), p. 453, che la definisce «prorompente».

[3] Emblematica della prima versione del Web, lanciata dall'informatico inglese Tim Berners-Lee nel 1991. Sul tema, cfr. lo stesso Berners-Lee (1999).

[4] Si tratta della seconda versione del Web ("Web 2.0"), definita nei primi anni Duemila dall'editore Tim O'Reilly nell'articolo "*What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*", in *O'Reilly*, 30 settembre 2005.

[5] È l'idea di Gershberg e Illing (2022), p. 19, per i quali «[*w*]*e certainly face an epistemic crisis as journalism and other institutions of knowledge – from schools and government agencies to respected scientific bodies – are dismissed and overwhelmed by the volume of communication that flourishes in digital culture*». Può dirsi, recuperando la logica della democratizzazione della conoscenza, che l'assenza di intermediazione determina la netta prevalenza dell'aspetto democratico – o, meglio, "anarchico" – su quello epistemico. Sul punto, cfr. Crouch (2004), p. 46, secondo cui l'avvento delle *media corporations* ha comportato «*reductions of choice and the debasement of political language and communication which are important components of the poor health of democracy*». Sul carattere "epistemico" della rete cfr. anche Floridi (1997).

[6] Con risvolti inevitabilmente problematici. È nell'efficace espressione delle «"dettature" o "dittature" di incompetenti» in netta contrapposizione alla valorizzazione delle competenze specialistiche, coniata intorno ai temi del "fine vita" da Canestrari (2021), p. 56.

[7] Cfr. Rodotà (2010), p. 339.

Web»[8], imprigionato – secondo una logica quasi *hobbesiana* – nei rapporti di forza tra utenti, la cui discussione è sovente attraversata da profili di illiceità penale (dal classico insulto alla più elaborata e artificiosa creazione di false ricostruzioni o di autentiche campagne d'odio a danno di singoli o gruppi di individui), ben lungi dall'idea originaria di «domare le masse ululanti» e di «costruire un mondo più socievole»[9].

E benché possa dirsi felice l'intuizione di trasporre le libertà sulla rete, coniandosi di fatto una vera e propria cittadinanza digitale[10], non si è finora assicurata alle stesse, al di là di una generica affermazione di principio, una protezione adeguata[11].

Neppure la *net neutrality* – presupposto all'estrinsecazione delle libertà *online*, e soprattutto della libertà di espressione[12] – ha garantito sufficiente tutela alla "proiezione virtuale" degli individui. Spesso, anzi, la neutralità della rete è divenuta centrale nel giustificare ogni assenza di responsabilità in capo ai prestatori di servizi della società dell'informazione[13]: suggellandosi, così, non soltanto il necessario binomio tra neutralità (dei prestatori) e libertà (degli utenti), ma anche tra neutralità e *irresponsabilità* di tali prestatori[14].

Nulla quaestio, se si considera che la disciplina originaria del mercato digitale in ambito comunitario aveva certificato le funzioni essenzialmente passive di tali soggetti, persone fisiche o giuridiche che fossero, incasellandoli nelle funzioni di mero trasporto, memorizzazione temporanea e *hosting* di siti Internet[15]. Eppure, sempre più marcatamente, essi sono divenuti detentori di significativo potere e discrezionalità, assommando nel proprio ruolo una serie di funzioni simbolo del loro interventismo: dall'estrazione all'elaborazione di dati (la c.d. profilazione), alla loro modifica fino alla comunicazione di quei dati agli utenti interessati; ma non soltanto.

In breve, la figura di un *host Provider* attivo si è progressivamente stagliata nel linguaggio della dottrina, anche penalistica[16], e delle Corti[17]; e benché possa dirsi ancora incerto il confine dell'ampia gamma di funzioni ascrivibili ai prestatori ospitanti l'attività di utenti (come l'imposizione all'utente di aggiornare la piattaforma, il controllo dei contenuti pubblicati *online* da costui, il diritto di interrompere in modo temporaneo o permanente il servizio erogato all'utente, inibendogli l'accesso alla piattaforma), è ormai certo, invece, che il loro ruolo «appare sempre più distante dalla conformazione normativa che per prima la direttiva 2000/31 aveva delineato, presupponendo una neutralità operativa in funzione di un'ipotetica equidistanza tra fornitori di contenuti e utenti»[18].

Mutatis mutandis, l'esigenza di dirimere i conflitti e tutelare le libertà nella dimensione virtuale permane. Tuttavia, il ruolo sempre più incisivo delle piattaforme digitali – termine ormai passato per antonomasia dal designare il servizio all'indicare il fornitore (e anche qui spesso

[8] È il titolo dell'opera di Grandi (2017).

[9] Cfr. Leslie, "*How to have better arguments online*", su *The Guardian*, 16 febbraio 2021: «[*i*]*n 2010, Time magazine made Mark Zuckerberg its person of the year. It described Facebook's mission as being to "tame the howling mob and turn the lonely, antisocial world of random chance into a friendly world". During the first decade of mass internet use, this was a popular theory: the more that people were able to communicate with others, the more friendly and understanding they would become, the result being a more peaceable and harmonious world*».

[10] Sul tema, cfr. Rodotà (2012), pp. 384 ss. Si rinvia anche a E. Celeste *et al.*, (2022).

[11] Numerose iniziative – per via "informale" o istituzionale – sono state adottate a livello internazionale e italiano. Tra le altre, si pensi, ad esempio, alla *Charter of Human Rights and Principles for the Internet* promossa e pubblicata nel 2011 dall'organizzazione *Internet Rights and Principles Dynamic Coalition* oppure alla *Dichiarazione dei diritti in Internet*, presentata in Italia alla Camera dei deputati nel 2015 dalla Commissione per i diritti e i doveri relativi ad Internet, presieduta da Stefano Rodotà, documento avente l'obiettivo di riconoscere nell'orbita del Web numerosi diritti e libertà costituzionali, suggellati all'art. 4 dal principio di neutralità della rete.

[12] Inquadrabile quale *condicio sine qua non* dell'ormai universalmente riconosciuto "diritto all'accesso" a Internet, la c.d. *net neutrality* (lett.: "neutralità della rete") è principio prima informatico e poi giuridico. Si veda l'art. 3 (3) del Reg. (UE) 2015/2120: «[i] fornitori di servizi di accesso a Internet, nel fornire tali servizi, trattano tutto il traffico allo stesso modo senza discriminazioni, restrizioni o interferenze, e a prescindere dalla fonte e dalla destinazione, dai contenuti cui si è avuto accesso o che sono stati diffusi, dalle applicazioni o dai servizi utilizzati o forniti, o dalle apparecchiature terminali utilizzate».

[13] È il termine utilizzato dall'art. 2 della Direttiva 2000/31/CE, c.d. *E-commerce*.

[14] Si veda Manetti (2014), p. 139, che sottolinea «l'imperante esaltazione della libertà della Rete, che pretendendo dai Provider assoluta neutralità si è saldata incrollabilmente con l'interesse di questi ultimi a non essere ritenuti responsabili per l'illiceità dei messaggi trasmessi».

[15] Si rimanda alle definizioni tracciate dagli artt. 12, 13 e 14 della Direttiva c.d. *E-commerce* (su cui, peraltro, *infra* § 4) e relative alle funzioni di «*mere conduit*», «*caching*» e «*hosting*».

[16] Ad es., Accinni (2017).

[17] Tra le prime pronunce di merito in Italia, si vedano Trib. Roma, 16 dicembre 2009 ("RTI c. YouTube"), Trib. Milano, 20 gennaio 2011 ("RTI c. ItaIaOnLine"), Trib. Milano, 19 maggio 2011 ("RTI c. Yahoo"), laddove il giudice civile ha condannato i fornitori di servizi di *hosting*, ritenendo integrati nei casi di specie i caratteri del c.d. "*hosting* attivo". In ambito europeo, di primario interesse è il *leading case* in materia di c.d. diritto all'oblio, "*Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos e Mario Costeja González*" (C-131/12) del 2014, nel cui contesto la Corte di Giustizia dell'Unione europea ha affermato, a determinate condizioni, la qualifica di titolare del trattamento di dati personali in capo al *provider* in ragione di una serie di operazioni tutt'altro che passive.

[18] L'osservazione è di Pollicino (2014), p. 454.

utilizzato in questo senso) – induce, a fronte di condotte socialmente e penalmente riprovevoli degli utenti da essi ospitati, a domandarsi l'opportunità del loro intervento, nella cui assenza o inefficacia può cogliersi uno spazio di eventuale responsabilità.

Nei vari ordinamenti, numerosi sono stati finora i modelli di regolamentazione approntati in tempi più o meno recenti, polarizzati sulle opposte esigenze di *participation* e *protection* degli utenti, e rivolti all'esigenza di *law enforcement* nello spazio digitale, facendo perno proprio sul ruolo degli *Internet Service Providers*. Tali paradigmi, nella cornice di una nuova "crisi della disintermediazione" e dunque di evidente *post-democracy*[19], costituiscono risposte ad esigenze di tutela che certamente coinvolgono in via diretta le piattaforme digitali. L'analisi intorno al ruolo di quest'ultime, peraltro, non può che muovere da alcune considerazioni preliminari sugli effetti degli illeciti commessi dagli utenti e sul disvalore di un intervento non tempestivo degli *Internet Service Providers*, all'origine di nuove forme di offesa alle vittime, spesso iscritte in fasce vulnerabili, dello spazio digitale.

2. Tra inerzia ed effetti lesivi. Quale responsabilità per le piattaforme? Lo "stallo" dell'arte in Italia.

Napoli, Italia, 2015

Tiziana Cantone, giovane ragazza originaria dell'hinterland napoletano, convive da poco tempo con il suo compagno, che la convince ad aver rapporti sessuali con lui e altri soggetti, e a filmarli. Nell'aprile di quell'anno, la donna accetta la proposta, con la condizione apparentemente "vantaggiosa" di poter scegliere gli altri soggetti con cui intrattenere atti sessuali, poi effettivamente compiuti e ripresi in video. Durante le riprese, nei cui titoli è leggibile il nome della ragazza e nelle cui immagini compare nitidamente il suo volto, si ode chiaramente quest'ultima appellare il proprio fidanzato «cornuto» ed esclamare con forte accento napoletano: «Stai facendo un video? Bravo!». In breve tempo, i video vengono diffusi su numerose chat e piattaforme, anche pornografiche, divenendo popolarissimi, soprattutto nel napoletano. L'espressione «Stai facendo un video? Bravo!» diviene subito virale, oggetto di numerose vignette e parodie sul Web (tra cui il video di una canzonetta italiana, che ottiene decine di milioni di visualizzazioni). Di fronte alla diffusione capillare e irrefrenabile delle proprie immagini a sfondo sessuale, la giovane decide di trasferirsi presso alcuni parenti in Emilia-Romagna e in Toscana, iniziando contestualmente una battaglia giudiziaria in sede civile al fine di chiederne la rimozione da alcune delle piattaforme più note (tra cui Facebook, Google, YouTube, del tutto inerti). Pur ottenendo la cancellazione dei video (peraltro, non da tutte le piattaforme interessate), alla donna viene negato dal giudice il risarcimento dei danni, seguendo invece la condanna alle spese giudiziarie: di qui, la delusione e il proposito di Tiziana Cantone di porre fine alla propria vita nel settembre 2016[20]*. Pochi mesi dopo il suicidio della giovane, nell'aprile 2017, viene archiviato dal GIP di Napoli il procedimento penale per diffamazione scaturito dalla querela contro i quattro iniziali diffusori dei video; lo stesso epilogo subirà il procedimento per istigazione al suicidio contro ignoti, archiviato nel dicembre 2017.*

Christchurch, Nuova Zelanda, 2019

Verso le ore 13:40 del 15 marzo, un ventottenne australiano di nome Brenton Harrison Tarrant, vicino ad ambienti neofascisti e islamofobi, indossando un casco dotato di telecamera e riproducendo in sottofondo alcune canzoni di stampo militare e nazionalista, avvia un video su Facebook[21]*, trasmettendo in diretta i primi 17 minuti del proprio attacco armato alla moschea di Al Noor, dove*

[19] Sul termine, per tutti, Crouch (2004).

[20] Così osserva, in quello che può esser considerato il primo scritto italiano sul tema, Caletti (2018), p. 66, ricostruendo la storia di Tiziana Cantone alla base della criminalizzazione specifica del fenomeno del c.d. "*revenge porn*" in Italia (poi avvenuta nel luglio 2019 con l'introduzione del nuovo art. 612-*ter* nel Codice penale); peraltro, lo stesso Autore non manca di interrogarsi sull'opportunità di regolare, contro le insidiose e più ampie forme di pornografia non consensuale, la responsabilità dei *providers* che ospitano contributi incriminati (*ivi*, pp. 91-92). Più di recente, Caletti (2021), pp. 117 ss. ("*Tiziana, Carolina and Giulia. Three (Non-)"Revenge Porn" Italian Stories*"). Per una breve, ma esaustiva cronaca della vicenda di Tiziana Cantone, cfr. Facci, "Storia di Tiziana Cantone", su *Il Post* (*online*), 15 settembre 2016. In ultimo, nel gennaio 2024, è stata esclusa dagli inquirenti e archiviata per assenza di prove l'ipotesi dell'omicidio della donna, insistentemente sostenuta dai familiari di lei. Sulla notizia, v. Rossano, "Tiziana Cantone, il caso è chiuso: archiviato anche l'ultimo filone d'inchiesta per omicidio", su *Corriere del Mezzogiorno*, 11 gennaio 2024.

[21] Sullo stesso *social network*, peraltro, il terrorista caricava contestualmente il *link* di accesso a un singolare manifesto, *The Great Replacement. Towards a new society*, fondato sull'idea di sostituzione etnica e di difesa dell'Occidente "bianco e cristiano", con il proposito di promuovere attacchi nei confronti di immigrati e di alcune personalità notorie. Su tale manifesto, cfr. le osservazioni di E. Thomas (2020), pp. 19 ss.

in quel momento si trovavano riunite per la preghiera musulmana del venerdì alcune centinaia di fedeli. Pochi minuti più tardi, spostatosi in auto con la diretta ancora in corso, apre il fuoco contro alcune persone situate all'esterno del vicino Centro Islamico di Linwood. A seguito dell'immediata segnalazione delle autorità locali, Facebook, soltanto nelle 24 ore successive agli attentati – nei quali trovano la morte oltre 50 persone in totale –, dichiara di aver rimosso ben 1,5 milioni di video, molti dei quali ancora in fase di caricamento. Di questi, tuttavia, circa 300mila versioni raggiungono i "newsfeed" di molti utenti prima di essere rimosse dalla piattaforma[22]*, complice la ripubblicazione del video da parte di altri utenti suprematisti, che ne effettuano peraltro il download. A nulla vale, alcuni mesi dopo, durante un discorso al Parlamento di Wellington, l'appello accorato dell'allora premier neozelandese Jacinda Ardern per evitare al terrorista ogni notorietà*[23]*: alla fine del 2022, il video è di nuovo pubblicato su Twitter – social network nel frattempo "passato di mano" da Jack Dorsey a Elon Musk e divenuto di stampo ancor più "liberale" – i cui algoritmi, però, non riconoscono il contenuto come illecito e ne consentono la propagazione*[24].

Washington DC, USA, 2021

La mattina del 6 gennaio si sta svolgendo al Congresso degli Stati Uniti d'America la certificazione dell'elezione del candidato democratico Joe Biden, in seguito alla vittoria nel voto presidenziale del precedente 3 novembre. A pochi passi, nel parco Ellipse di Washington D.C, una folla di sostenitori del Presidente uscente, Donald Trump, si raduna per ascoltare un comizio – la c.d. "Save America March" – "convocato" da quest'ultimo via Twitter. Molto attivo su tale social network e forte di una platea di oltre 87 milioni di followers, nelle settimane precedenti Donald Trump ha contestato a più riprese – in modo del tutto infondato e pretestuoso – la vittoria dell'avversario democratico, affermando a gran voce (o, meglio, twittando) l'illegittimità del voto e chiedendo ai propri collaboratori (incuso il Vicepresidente in carica Mike Pence, in quel momento intento a certificare l'esito del voto) di "ribaltare" i risultati elettorali, utilizzando un linguaggio fortemente denigratorio e pieno di falsità[25]*. E benché le accuse di Donald Trump abbiano alimentato un grave clima di crescente tensione, alla mattina del 6 gennaio i contenuti da lui postati sono liberamente accessibili su Twitter, in ossequio all'inscalfibile libertà di espressione consacrata nel primo emendamento della Costituzione statunitense. Al culmine della manifestazione, aizzata da ulteriori post pubblicati su altri social network simpatizzanti per Trump, la folla, indossando bandiere confederate, simboli nazisti e oggetti antisommossa, si dirige verso il Congresso, violandone il perimetro di sicurezza e irrompendo nel Palazzo, che viene devastato e saccheggiato*[26]*. Durante l'assalto, oltre agli ingenti danni inflitti al luogo simbolo della democrazia negli USA, perdono la vita un poliziotto e quattro manifestanti*[27]*. Pochi giorni dopo l'assalto, l'account Twitter di Donald Trump è "chiuso" dal gestore della piattaforma e viene riaperto solo il 20 novembre 2022, a seguito di un sondaggio degli utenti (con il 52% dei voti favorevoli) indetto dal nuovo proprietario, Elon Musk, che annuncia la riammissione di Trump citando il motto* «Vox Populi, Vox Dei».

Lo stigma di un'epoca di *post-truth* e di *post-democracy* può ben cogliersi nella mutata fisionomia delle stesse piattaforme, inesorabilmente al centro di un processo di forte trasformazione: dalla liberalizzazione del virtuale all'imprigionamento del reale – da reti (*networks*) a gabbie[28].

[22] Cfr. NZ Herald, "*Christchurch mosque shootings: Gunman livestreamed 17 minutes of shooting terror*", 15 marzo 2019, e Porro, "Come il video dell'attentato in Nuova Zelanda è dilagato sui social network", su *Wired.it*, 18 marzo 2019.

[23] «*He sought many things from his act of terror, but one was notoriety, and that is why you will never hear me mention his name. He is a terrorist, he is a criminal, he is an extremist, but he will – when I speak – be nameless. And to others, I implore you: speak the names of those who were lost rather than the name of the man who took them. He may have sought notoriety, but we in New Zealand will give him nothing*». Per la traduzione italiana, cfr. Ardern, ""Non dirò il suo nome". Il discorso di Jacinda Ardern", su *Il Foglio*, 20 marzo 2019.

[24] Sulla vicenda, Guelfi, "Twitter: ricaricati i video dell'attentato di Christchurch, ma il social non li riconosce", su *La Stampa*, 28 novembre 2022.

[25] Sugli epiteti denigratori con particolare riferimento al linguaggio di Donald Trump, cfr. Bianchi (2021), pp. 105 ss.

[26] Similmente originano e si svolgono, nell'estate 2024, le proteste violente di Southport, nel nord-ovest dell'Inghilterra, dove, a seguito dell'accoltellamento di alcuni bambini in una scuola da parte di un soggetto di carnagione scura non meglio identificato (anche per via della legge britannica che vieta alla polizia di rendere pubbliche le generalità in fase d'indagine), alcuni personaggi di estrema destra orchestravano una capillare campagna di false informazioni secondo le quali egli si chiamasse Ali Al-Shakati, fosse arrivato nel Regno Unito su un barcone e fosse stato ritenuto potenzialmente pericoloso dalle forze dell'ordine. In seguito, il Tribunale locale decideva di rivelarne l'identità per «ragioni di interesse pubblico», ovvero per contribuire a smentire tutte le notizie false che erano circolate al riguardo sulle piattaforme di *social network* – e mai rimosse. Sull'intera vicenda, v. Melley e Lawless, "*British police charge 17-year-old with murder over a stabbing attack that killed 3 children*", su *AP News*, 1° agosto 2024.

[27] Il caso è ripreso anche in apertura del contributo di Rinceanu (2021), pp. 333 ss.

[28] È precisamente la "parabola" di Mark Zuckerberg – già "uomo dell'anno" nel 2010 secondo la celebre rivista *Time* – che, il 31 gennaio 2024,

Un'eterogenesi dei fini operante su più livelli, almeno due. Da un lato, nel *perdurare* degli illeciti penali commessi *online*, che di rado si esauriscono nel compimento di una singola azione o più, ma sprigionano effetti dirompenti destinati a protrarsi in via potenzialmente illimitata nella realtà virtuale[29] – complici le "condivisioni", i "*likes*", i commenti operati da numerosi altri utenti. È il caso degli attentati di Christchurch, nel quale le semplici visualizzazioni degli utenti, destinatari del video "in diretta" della strage nei propri "*newsfeed*", e le successive condivisioni e ripubblicazioni, anche a distanza di anni – avvenute perciò ben oltre il termine della diretta video – hanno determinato una sorta di prolungamento della propaganda *online* del terrorista (svoltasi parallelamente alla strage nel quadro dei sanguinosi attentati di stampo islamofobo).

Dall'altro lato, quale automatica conseguenza del perdurare degli effetti nel *Cyberspace*, il loro *riverberarsi*, in moltissimi casi, nel mondo reale, ha arrecato agli individui tangibili danni psicologici e materiali attraverso lo sconvolgimento della loro vita quotidiana e delle loro abitudini[30]. Di fronte alla realizzazione di condotte illecite e penalmente rilevanti, viene a crearsi, cioè, una singolare commistione tra virtuale e reale, «un nuovo spazio sociale ibrido – l'«interrealtà» – che mescola il mondo digitale con quello fisico»[31] e che rende vano l'atto di spegnere il telefono o chiudere il computer. È qui paradigmatica la vicenda di Tiziana Cantone, alla disseminazione delle cui immagini sessualmente esplicite è seguita – prima – una radicale modifica delle proprie abitudini di vita[32] con il trasferimento presso alcuni parenti in altre città e – più tardi – il tragico epilogo del suicidio, nell'impossibilità di reggere l'onta e l'onda della ignobile colpevolizzazione della vittima[33] in seno a un'inarrestabile gogna mediatica[34]. In una parola, la mutata funzione sociale della piattaforma, intesa alla stregua di una "cassa di risonanza", amplifica la portata dei contenuti illeciti, spostando l'asse dalla *viralità* alla *pervasività* – di cui è emblema il citato "caso Trump": ciò che in altre parole si afferma con l'espressione inglese «*the Internet never forgets*»[35].

In termini penalistici, la questione appare, a prima vista, piuttosto complessa.

Si prenda ad esempio la classica diffamazione[36]. Un primo ordine di problemi attiene certamente alla fattispecie-base, ossia al contenuto illecito online dell'utente che, unito alla sua circolazione, sarebbe potenzialmente inquadrabile nello schema del reato di durata e in particolare in quello della fattispecie a consumazione prolungata[37]. Ancor di più, dovrebbe parlarsi di "*growing-offensivness crime*", di un reato a offensività crescente, dove la lesione inflitta al

è audito dal Congresso degli Stati Uniti, con l'accusa di non aver impedito la proliferazione sulle piattaforme della propria *Big Tech* "Meta" di contenuti pedopornografici, in danno della libertà sessuale e della privacy, dell'onore, della reputazione e della dignità di numerosi minori, di cui molti poi determinatisi al suicidio. A ben vedere, nel corso degli anni, *Meta* e altre aziende informatiche hanno mostrato una totale inerzia nel gestire le segnalazioni degli utenti, tanto che, pur non essendo direttamente responsabili della morte dei soggetti coinvolti, sono accusati da alcuni senatori di avere «le mani sporche di sangue». Sulla vicenda, si veda McKinnon e Tracy, "*You Have Blood on Your Hands': Senators Say Tech Platforms Hurt Children*", su *The Wall Street Journal*, 31 gennaio 2024. Sul pregiudizio al modello democratico nel suo complesso da parte delle piattaforme digitali si rinvia, per tutti, a Horder (2022). Deve, peraltro, menzionarsi il recente caso delle interferenze russe nel corso delle elezioni presidenziali del 2024 in Romania, per cui la Corte costituzionale rumena, con un'inedita decisione, ha annullato l'esito della prima tornata elettorale. Oltre ai 85.000 cyberattacchi ai sistemi elettorali, rivelati dall'*intelligence* rumena, e piattaforme di social media come *TikTok* e *Telegram* sono state sfruttate per operazioni di disinformazione su larga scala a sostegno del candidato ultranazionalista Călin Georgescu, attraverso contenuti generati dall'intelligenza artificiale, attività di "bot", fabbriche di "troll" o influencer a pagamento. Sul tema, cfr. Botan *et al.* (2025).

[29] È la definizione offerta da Panattoni (2020), p. 307, che individua dei tratti fondanti il *Cyberspace* «la durevole presenza e disponibilità cui è destinato il contenuto che si è deciso di caricare o condividere, resa possibile dalla mediazione dei processi di elaborazione, memorizzazione e trasmissione di dati a cui è sottoposta l'informazione e qualsiasi altro materiale caricato o diffuso».

[30] Sulle tipologie di danno riscontrabili dallo spazio digitale, Sjöholm (2022), pp. 76 ss.

[31] Così Riva (2018), p. 45. Similmente, Floridi (2016), p. 47, secondo cui «[i]l mondo digitale online trabocca nel mondo analogico offline, con il quale si sta mescolando». Sull'interdipendenza tra software e mondo fisico, v. anche Benanti (2024), pp. 146 ss., ove afferma che «[c]on tutti i risvolti metafisici che questo [il primo] comporta […] in fin dei conti cambia l'arredo del mondo».

[32] Con riferimento alla pornografia non consensuale (al di là del "caso Cantone"), gli effetti tangibili della disseminazione *online* di immagini a sfondo sessuale sono ben posti in luce da Caletti (2019), pp. 2056-57.

[33] Sul termine, Ryan (1971).

[34] Sul tema della gogna mediatica, storicamente, Defoe (1703). Nell'attuale panorama penalistico italiano, in particolare, Manes (2022), pp. 74 ss.; Piergallini (2022), pp. 709 ss. In argomento, cfr. anche Caletti (2024), pp. XV ss. Recentemente, in ambito italiano e in particolare bolognese, si segnala un preoccupante caso di "gogna mediatica" legato al sempre più frequente utilizzo del *social network* cinese *TikTok*, ove un giovane "influencer" si è tolto la vita in diretta video, dopo essere stato travolto da numerosi commenti con accuse false e infamanti in tema di pedofilia, presumibilmente ideate da due "influencers" concorrenti. Per una breve panoramica della vicenda, cfr. Tempera, "Suicida su TikTok, il padre di Vincent: "Nel suo cellulare chat sconcertanti"", su *Il Resto del Carlino*, 7 febbraio 2024. Ancor più di recente, si è disposta l'archiviazione per la prospettata fattispecie di istigazione al suicidio, con contestuale trasmissione degli atti alla procura di Bologna per una nuova indagine in punta di diffamazione a carico degli autori dei commenti infamanti.

[35] «La rete non dimentica». Cfr. Crockett (2016), p. 151.

[36] Sul tema, *ex multis*, cfr. Pezzella (2017) e Curreli (2017).

[37] Sul tema, Aimi (2017), 203 ss.

bene giuridico non raggiunge virtualmente mai il proprio culmine, ma aumenta insieme alla propagazione del contenuto illecito[38].

E anche rigettando l'idea di una diffamazione alla stregua di reato di durata[39] (con ogni conseguenza in capo all'*uploader* [40]) e accettando l'ormai consolidata fisionomia di tale delitto[41], è comunque sempre più evidente la rilevanza della permanenza in rete di un contenuto diffamatorio e, in generale, la seria minaccia che il *protrarsi* di ogni illecito online costituisce nei confronti di beni giuridici di primaria importanza, talvolta anche collettivi[42]. Così, «l'affermarsi di nuovi mezzi di lesione di vecchi beni giuridici»[43] e, con questi, di momenti di profonda intensificazione dell'offesa interpella il diritto penale e il ruolo dei gestori di piattaforme come garanti dello spazio digitale, sul cui disposto è sorto, però, un secondo ordine di problemi.

Il proposito di trovare «paradigmi idealtipici»[44] per la tutela dei beni in gioco e per una bilanciata responsabilizzazione degli *Internet Service Providers* si è scontrato infatti sin qui, da un lato, con la struttura di quegli stessi paradigmi e, dall'altro, con obblighi di natura sovranazionale.

Nel lungo dibattito sul tema in Italia, attraverso un approccio *ad excludendum*, si è dapprima rigettata l'idea di una responsabilità della piattaforma di natura concorsuale e, più precisamente, in termini di accessorietà minima[45]: non solo per l'assenza di coevità nella perpetrazione dell'illecito-*upload*, ma anche per quella dell'indispensabile sfumatura soggettiva del dolo di partecipazione[46]. In seguito, anche il terreno del reato omissivo proprio e improprio è sembrato piuttosto impervio, specialmente per l'inesistenza di puntuali obblighi di attivazione o di una generale clausola di impedimento invocabili di fronte ai casi di inerzia della piattaforma[47].

Sul punto, ancorché semplice – almeno linguisticamente – tradurre l'inerzia con l'omissione, si è fin da subito collocata nel novero degli *impossibilia* l'idea del gestore di piattaforma digitale capace di intervenire a fronte di ogni segnalazione di un (presunto) contenuto illecito[48], alla luce di una formula normativa nella quale l'esigibilità è pur sempre il «metro dell'obbligo»[49].

[38] Si tratta delle «evidenti ripercussioni sull'offensività delle condotte criminose che mettono a disposizione e quindi «diffondono» contenuti lesivi di diritti altrui» su cui v. B. Panattoni (2020), p. 308. Ancor più di recente, la Direttiva UE 2024/1385 del Parlamento europeo e del Consiglio del 14 maggio 2024 sulla lotta alla violenza contro le donne e alla violenza domestica espone con chiarezza simile concetto, affermando in premessa che l'utilizzo delle nuove tecnologie «comporta il rischio di un'amplificazione facile, rapida e diffusa di alcune forme di violenza online, con l'evidente rischio di provocare o aggravare danni profondi e a lungo termine per la vittima» (cfr. *Considerando* no. 18: «[*t*]*he use of ICT bears the risk of easy, fast and wide-spread amplification of certain forms of cyber violence with the clear risk of creating or enhancing profound and long-lasting harm to the victim*»).

[39] Sulla rilevanza del momento intercorrente tra la pubblicazione in rete e l'approfondimento dell'offesa, L. Picotti, *Diritto penale, tecnologie informatiche ed intelligenza artificiale*, cit., 89 ss.

[40] Per amor di chiarezza: conseguenze connesse all'offesa di beni determinata dalla (sola) perduranza e non, invece, a ulteriori eventi "aggravanti" il contenuto caricato online, come – a riprendere i casi citati in apertura di paragrafo – il suicidio di Tiziana Cantone e l'assalto al Congresso statunitense.

[41] Per cui, anche se «l'idea della permanenza del reato, unita alla mancanza di finitezza spazio-temporale della rete, è in grado di determinare un completo stravolgimento degli istituti collegati alla consumazione […] è preferibile l'interpretazione che fissa il disvalore del reato nella diffusione del contenuto lesivo e conseguentemente afferma la natura istantanea della violazione», come ben rileva Braschi (2020), p. 165. Allora, sulla qualificazione della perduranza, si vedano gli interessanti suggerimenti, di nuovo, di Panattoni (2020), pp. 313-14, che ritiene il protrarsi dell'illecito, in alternativa, postfatto non punibile oppure momento coincidente con gli effetti materiali del reato consumato.

[42] Il riferimento è alla denuncia di inizio 2024 del Sindaco di New York, Eric Adams, avverso le principali piattaforme statunitensi, ritenute «una tossina ambientale» fonte di «un pericolo per la salute pubblica» e soprattutto per la salute mentale dei giovanissimi. Cfr. Di Ronza, *New York dichiara i social media pericolo per la salute pubblica*, su *www.ansa.it*, 25 gennaio 2024.

[43] È l'espressione di Cadoppi (2022), p. 124.

[44] È la calzante nozione di Ingrassia (2012), pp. 15 ss. Su tali paradigmi, v. anche Nardi (2019), pp. 278 ss.

[45] Su cui, per tutti, Antolisei (2003), p. 551.

[46] *Ivi*, p. 567. Sul tema, con riferimento agli *Internet Service Providers*, cfr. De Natale (2010), p. 65.

[47] In giurisprudenza e in dottrina si è esclusa anche la configurabilità della speciale posizione di garanzia del direttore di periodico *ex* art. 57 c.p., principalmente per ragioni di analogia *in malam partem*. Cfr. Cass. Pen., sez. V., 16 luglio 2010 (dep. 1° ottobre 2010), n. 35511, con nota di Turchetti (2010). Sul punto, non sono mancati problematici indirizzi di segno contrario, come, ad es., Cass. Pen., sez. V, 23 ottobre 2018 (dep. 11 gennaio 2019), n. 1275, con nota di Mauri (2019). Nondimeno, anche qui, come si dirà *infra*, se è vero che, come rileva Polvani (1998), p. 225, «[…] la fattispecie si caratterizza sia per la presenza di una posizione di garanzia del soggetto agente sia per la previsione di un'altrui condotta di reato resa in qualche modo possibile dalla condotta colposa – omissiva o commissiva – del soggetto qualificato», è ben difficile immaginarsi una condotta colposa di natura attiva od omissiva in carico al *Provider*, che non avrebbe in ogni caso i poteri necessari per svolgere una selezione "in ingresso" dei contenuti (peraltro, da operare contestualmente per numerosissimi utenti) alla pari del direttore di stampa periodica.

[48] Deve infatti dirsi «problematico, per il gestore di rete conoscere previamente il carattere illecito del materiale immesso in rete e quindi poterne impedire l'immissione», come rilevano Manna e Di Florio (2019), p. 902. Ciò, naturalmente, dato l'enorme flusso di dati che transitano […] sui servers gestiti da ciascun Provider […] in conformità con la struttura aperta (od "anarchica" […]) di Internet, che non rappresenta un unitario sistema centralizzato, ma una possibilità di molteplici connessioni». Così Picotti (1999), p. 380.

[49] Cfr. Fornasari (1990), p. 318.

L'ostacolo materiale dell'assenza di poteri impeditivi è stato infine confermato, nell'ambito del diritto vivente, dalla pronuncia della Corte di cassazione nel noto caso "Google v. Vivi Down", unitamente all'inesistenza di qualsivoglia fondamento normativo nell'ordinamento italiano per una posizione di garanzia o per altri obblighi di attivazione in capo all'*Internet Service Provider*[50].

E infatti, benché certa giurisprudenza creativa abbia postulato l'omesso impedimento degli effetti di un reato in riferimento alla persistenza di un contenuto diffamatorio online[51] o perfino un autonomo reato di diffamazione in capo al gestore di piattaforma[52], l'ostacolo più grande non si è rivelato di natura particolare – in punta di poteri impeditivi od obblighi di attivazione –, bensì generale, per l'assenza di un paradigma di responsabilità applicabile al caso di specie. È stato, cioè, il silenzio sul punto della normativa italiana ed europea a tenere in stallo per lungo tempo il dibattito in Italia, polarizzato tra le formule consolidate del concorso e dell'omissione, ma del tutto inefficaci nella configurazione di profili di responsabilità penale.

3. Alle origini del "peccato originale": la *Section 230* statunitense e la Direttiva *E-commerce* dell'Unione europea.

Per comprendere le ragioni di un tale silenzio, occorre portarsi idealmente dall'altro lato dell'Oceano Atlantico, circa diciotto anni prima delle motivazioni della sentenza della Suprema Corte italiana sul caso "Google vs. Vivi Down". Se al tempo di quest'ultimo, Internet poteva già dirsi "maggiorenne", nel contesto statunitense di fine anni Novanta esso muoveva i suoi "primi passi".

Fu proprio questo a determinare il Congresso statunitense, agli inizi del 1996, all'approvazione di una norma di portata rivoluzionaria: con la *Section 230* del nuovo *Communications Decency Act*, il legislatore riconosceva ai fornitori di servizi informatici la sostanziale "immunità" dalla responsabilità di diffamazione per i contenuti di terzi, non solo per tutelarli da una giurisprudenza già alquanto intransigente[53], ma anche per difendere la libertà di espressione. Infatti, «il Congresso non voleva che le aziende facessero troppi controlli, esprimendo il desiderio che Internet raggiungesse il suo pieno potenziale di forum per una vera diversità di parola politica, opportunità unica per lo sviluppo culturale e per una miriade di vie per l'attività intellettuale»[54].

L'obiettivo, a dire il vero, era quello di prevenire la diffusione in rete di materiale pedopornografico, incentivando le piattaforme a intraprendere iniziative per la rimozione volontaria – e non forzata – dei contenuti di tal sorta. È significativo, a tal proposito, che il "paradigma di immunità" fosse *ab origine* inserito all'interno di un titolo rubricato «*Obscenity and Violence*» e che immaginasse un *Provider* non inerte, ma solerte e in buona fede. Per costui, il § (c) (1) della *Section 230* recuperava la suggestiva immagine evangelica del "Buon Samaritano" qualora operasse il blocco e la rimozione di materiali ritenuti potenzialmente offensivi, escludendone alla radice e in ogni caso, a fronte di un intervento, l'equiparazione all'autore di quei contenuti[55].

[50] Si tratta della celebre pronuncia di Cass. pen., sez. III, 17 dicembre 2013 (dep. 3 febbraio 2014), n. 5107, con nota di Ingrassia (2014): «[d]all'esame complessivo delle disposizioni riportate emerge che nessuna di esse prevede che vi sia in capo al *provider*, sia esso anche un *hosting provider*, un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito. Né sussiste in capo al provider alcun obbligo sanzionato penalmente di informare il soggetto che ha immesso i dati dell'esistenza e della necessità di fare applicazione della normativa relativa al trattamento dei dati stessi». Sulla sentenza, si veda anche Di Ciommo (2010), p. 832, laddove, nel ribadire che la sentenza dica l'ovvio, cita criticamente Shakespeare e il «molto rumore per nulla». Sul tema, in prospettiva più ampia, si vedano anche Apa e Pollicino (2013).

[51] Cfr. Cass. pen., sez. V, 14 luglio 2016 (dep. 27 dicembre 2016), n. 54949, con nota di Ingrassia (2017), p. 1623, ove l'A. rileva che, «[g]uardando ai manuali di diritto penale, non vi è traccia di riferimenti a una tale forma di manifestazione del reato». Già da tempo, del resto, la cronaca constatava il creazionismo giudiziario in tema, come eloquentemente riportato, ad es., nell'editoriale di Negri, "*Sui provider fa legge il giudice*", su *Il Sole 24 Ore*, 30 dicembre 2009.

[52] Così nella pronuncia di Cass. pen., sez. V, 8 novembre 2018 (dep. 20 marzo 2019), n. 12546, con nota di Pagella (2019).

[53] Ci si riferisce in particolare alla pronuncia del 1995 del Tribunale dello Stato di New York che, nella causa "*Stratton Oakmont, Inc. v. Prodigy Services Co.*", aveva ritenuto il *Provider*-convenuto responsabile di alcuni contenuti diffamatori pubblicati da terzi: secondo il giudice, nei provvedimenti assunti per "schermare" i commenti offensivi, Prodigy aveva dimesso infatti il proprio ruolo di mero distributore per ricoprire quello di editore, acquisendo la proprietà dei contenuti e divenendone perciò responsabile. Cfr. "*Stratton Oakmont, Inc. v. Prodigy Services Co.*" [*No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)]:* «[…] [*b*]*y actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and "bad taste", for example, PRODIGY is clearly making decisions as to content* [...]*, and such decisions constitute editorial control*».

[54] Graw Leary (2018), p. 561 [trad. libera di chi scrive].

[55] Cfr. *47 U.S. Code § 230* (c) (1): «*Protection for "Good Samaritan" Blocking and Screening of Offensive Material*» -- «*Treatment of*

In altre parole, nell'irresponsabilità del Provider – e in quelle ventisei parole[56] – trovava così la sua sintesi perfetta il contrasto al *child sex traffic* con la tutela della libertà di espressione. Ciò ha tuttavia spinto il *Provider* a comportarsi più come un "Ponzio Pilato" che come un buon Samaritano.

Così è stato anche per la progressiva dilatazione nel tempo dell'operatività delle garanzie di immunità e della discrezionalità dell'*Internet Service Provider*, equiparandosi ad esso anche il *Content Provider* – la piattaforma creatrice di contenuti[57] – e sancendosi l'irrilevanza della conoscenza effettiva degli effetti di un illecito in rete quale limite alla buona fede nella c.d. *content moderation*[58].

In questo modo, perfino le segnalazioni di possibili illeciti operate dagli utenti sono state di fatto "nullificate" da quell'immunità esorbitante varata nel 1996: si è detto correttamente che «la storia legislativa del *CDA* e la costruzione giudiziaria dello statuto indicano […] che i tribunali e i legislatori hanno dato maggior peso agli interessi dei post anonimi e degli *ISPs* che a quelli delle vittime»[59].

Sul punto, non ha purtroppo sortito effetto il meccanismo di c.d. *Notice and Take Down*, approntato a tutela del diritto d'autore con il c.d. *Digital Millennium Copyright Act*, appena un paio d'anni dopo la celebre *Section 230*: un meccanismo a tutela degli utenti che, pur ribadendo il «porto sicuro» («*safe harbor*») della irresponsabilità degli *Internet Service Providers*, ne condizionava l'esistenza alla predisposizione di un sistema di pronta notificazione e gestione degli illeciti in materia di copyright.

Qui, la conoscenza qualificata del fatto segnalato dall'utente al *Provider* avrebbe – almeno in linea di principio – chiamato in gioco, in caso di mancato intervento, la responsabilità di quest'ultimo[60].

Nei lacciuoli della novella, si è tuttavia cercato di restringere la portata dell'*actual knowledge* in capo alla piattaforma[61], distanziando i concetti di notifica e conoscenza qualificata, ed addossando piuttosto all'utente i più vari difetti formali nella presentazione della segnalazione[62], così relegando il *Provider* a mero arbitro di un algido "meccanismo di responsabilità" – le cui regole, ancora oggi, costui finisce per disconoscere.

Successivamente, e per lungo tempo, né il dilagare della pornografia non consensuale né l'onda del movimento "*MeToo*" hanno scalfito più di tanto l'idea di un *Provider* "*legibus solutus*". Solo in tempi più recenti si è tornato a far leva sulle eccezioni all'immunità del *Provider* originariamente disegnate della stessa *Section 230*, ma a più riprese aggirate dalle Corti statunitensi.

È significativo, in questo senso, il § (e) (1) della Sezione in parola, che ha costituito il fondamento di qualche recente pronuncia di segno contrario all'immunità assoluta[63], e dove si afferma che nessuna delle sue disposizioni «può essere interpretata in modo da compromettere l'applicazione […] di qualsiasi […] statuto penale federale»[64].

La legge penale federale, dunque, dovrebbe costituire un baluardo altrettanto insormontabile di fronte al dogma della libertà di espressione, che tuttavia rimane inscalfibile per Costituzione[65].

Publisher or Speaker. – No provider or user of any interactive computer shall be treated as the publisher or speaker of any information provided by another information content provider».

[56] In ripresa di Kosseff (2019).

[57] Per cui anche costui «dovrebbe trovare totale rifugio sotto una legge da "buon samaritano" senza il requisito di agire come un "buon samaritano"». Cfr. Sevanian (2014), p. 127 [trad. libera di chi scrive].

[58] Si rinvia a "*Zeran v. America Online, Inc., 129 F. 3d 327 - Court of Appeals, 4th Circuit 1997*", *§§ 332-333*: «[…] *notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services […] Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at selfregulation*».

[59] Così Spiccia (2013), p. 399: «[*t*]*he legislative history of the CDA and the judicial construction of the statute indicate, however, that courts and legislators have afforded greater weight to the anonymous posters and ISPs' interests than those of the victims*».

[60] Sul provvedimento, McNamara *et al.* (1999), pp. 5 ss., e Williamson (1999-2000), pp. 987 ss. In Italia, anche in rapporto alla normativa nazionale e a quella tedesca, si rimanda a Panattoni (2018), pp. 258 ss.

[61] Si rinvia, sul punto, al contributo di Zarins (2004), pp. 257 ss.

[62] Come avvenuto nel caso "*ALS Scan, Inc. v. RemarQ Communities, Inc.*" [239 F.3d 619 (2001)], di cui in Liddell ed Eshee (2002), p. 387.

[63] Ad esempio, nel caso "*Force v. Facebook, Inc.*" [*934 F.3d 53 (2d Cir. 2019)*], riportato nelle sue fasi da Baccin (2020).

[64] Cfr. *47 U.S. Code § 230* (e) (1): «*No Effect on Criminal Law.--Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute*». Significativa anche la successiva e più generale previsione di cui al § 230 (e) (3): «*State Law.--Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section*».

[65] Nel celebre Primo Emendamento: «*Congress shall make no law* […] *abridging the freedom of speech*». Perciò, molti hanno provato per lungo tempo a fare della diffusione di immagini esplicite un reato federale, come conferma Caletti (2019), p. 2051, come più tardi avvenuto con il c.d. *Take It Down Act*, qui citato nella nota seguente.

Eppure, tale dogma è tuttora discusso intorno alla responsabilità dei *Providers* e alla rete[66]. Si è sostenuto che la sua ampia interpretazione ha ricompreso sfumature antidemocratiche, ben lungi da ciò che esso mirava a proteggere e a promuovere[67]. Ciò non ha però impedito, negli ultimi decenni, che lo "statuto di immunità" d'oltreoceano abbia attecchito anche in Europa.

Benché quest'ultima e gli Stati Uniti si trovino storicamente su due estremi opposti nello specchio della protezione del discorso[68], nella configurazione del suo mercato digitale alle soglie del nuovo millennio l'allora Comunità europea aveva approvato una Direttiva fondata su esenzioni da responsabilità per i *Providers*, in ragione delle loro funzioni passive legate alle figure paradigmatiche dell'*access*, *cache* e *host Provider*.

Nella cornice della Direttiva E-commerce (2000/31/CE), ciò avrebbe dovuto costituire, a rigor di termini, un'eccezione a un generale paradigma di responsabilità[69].

E invece la normativa italiana di recepimento della Direttiva (d.lgs. 70/2003) ha evidentemente ribaltato la prospettiva, prevedendo in via generale un'esenzione da responsabilità del *Provider* per contenuti illeciti[70], temperata esclusivamente dai casi di intervento o coinvolgimento del *Provider* nell'illecito o di mancata informativa all'autorità giudiziaria o di vigilanza.

Di fronte a tali casi, fondati sull'«intento di evitare che, in casi di particolare gravità, il danno possa produrre i suoi effetti per un arco temporale prolungato»[71], il *Provider* risulta(va) (solo) «*civilmente* responsabile» del contenuto dei propri servizi, incorrendo in una forma atipica di responsabilità extra-contrattuale per il danno prodotto[72]. E del resto, come noto, *"ubi voluit dixit, ubi noluit tacuit*": sul versante penalistico, sin dall'inizio, il legislatore italiano ha evitato *in toto* una presa di posizione.

Così, senza un chiaro perimetro di responsabilità, in mancanza di puntuali obblighi di attivazione e tutela e nella (comprensibile) estraneità dell'*host Provider* attivo rispetto alla disciplina europea sul commercio elettronico e della sua normativa di attuazione italiana[73], quest'ultima è ben presto risultata del tutto "*outdated*": per nulla al passo con le sfide dello spazio digitale e – per ciò che qui interessa – con le insidie da esso derivanti. E non per nulla, ancorché a distanza di un ventennio, la Direttiva che aveva inaugurato la disciplina del mercato elettronico in Europa con il nuovo millennio è stata infine superata da un Regolamento di ben altro tenore – il c.d. *Digital Services Act*, che interviene su quella Direttiva e ne modifica il quadro in modo significativo.

[66] Cfr. Moon (2019), p. 642: «[…] *the internet has flourished since its creation, transforming into a staple of today's society. Therefore, the motivations behind the first goal of the CDA have been fulfilled*». Si rinvia anche a Citron (2023). A riprova del "cedimento" del dogma dell'immunità assoluta degli *ISPs*, negli Stati Uniti è stato di recente approvato un provvedimento federale ribattezzato dall'opinione pubblica "*Take It Down Act*", a tutela delle vittime di distribuzione non consensuale di immagini intime, anche in ragione dell'ampio utilizzo di meccanismi di intelligenza artificiale nella produzione di c.d. "*deepfakes*". Tra le misure, si prevedono obblighi di rimozione molto stringenti per le piattaforme digitali. Cfr. il *Press release* pubblicato dall'*U.S. Senate Committee on Commerce, Science, & Transportation*, dal titolo *Sens. Cruz, Klobuchar, Reps. Salazar, Dean Continue Fight to Pass TAKE IT DOWN Act*.

[67] È l'idea alla base del recente libro di Franks (2024), per cui il fondamentale principio della libertà di espressione «[...] è stato in pratica utilizzato legalmente in modo più visibile ed efficace per promuovere potenti interessi antidemocratici: misoginia, razzismo, zelo religioso e interesse personale delle imprese, in altre parole, discorsi sconsiderati» («[...] *in practice it has been legally deployed most visibly and effectively to promote powerful antidemocratic interests: misogyny, racism, religious zealotry, and corporate self-interest, in other words, reckless speech*» [trad. di chi scrive]).

[68] Cfr. Moon (2019), p. 643: «[*c*]*urrently, U.S. and European internet regulatory schemes are on two separate ends of the spectrum for speech protection*». Per un'ampia comparazione sul tema tra i due ordinamenti, si rinvia a Wilman (2020). In argomento, v. anche Hörnle (2021).

[69] Per il legislatore comunitario, cioè, l'irresponsabilità del *Provider* avrebbe costituito una deroga, come da considerando (42) della Direttiva 2000/31/CE (E-commerce): «[l]e deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Sulla Direttiva, Antonucci (2001).

[70] Cfr. Aceto di Capriglia (2018), p. 16: «[g]li artt. 14, 15 e 16 del decreto n. 70 del 2003, contemplano le diverse forme di responsabilità degli operatori *Internet*, enunciando una sostanziale deresponsabilizzazione dell'*Internet Service provider*. La normativa delinea un sistema volto a definire quando il prestatore di servizi non risponde delle attività illecite commesse dall'utente, invece che un sistema improntato a stabilire quanto egli sia responsabile».

[71] Così Riccio (2002), p. 210.

[72] Si veda l'art. 17, comma 3 del d.lgs. 9 aprile 2003, n. 70. Sulla natura della responsabilità, di nuovo, Riccio (2002), pp. 45 ss. che, scartata la responsabilità da cose pericolose *ex* art. 2050 c.c. propende per un atipico «criterio di imputazione a carattere colposo». Sulla responsabilità civile degli *Internet Service Providers*, anche in rapporto agli USA, Benatti e Portonera (2024).

[73] Sull'estraneità dell'*host Provider* "attivo" al d.lgs. 79/2003, S. Braschi (2020), p. 167.

4. Dalla (non-)*liability* alla *compliance*: la rapida ascesa e discesa della *NetzDG* tedesca, tra "*chilling effect*" e "*overblocking*".

In realtà, a segnare un primo e autentico «salto in avanti»[74] in ambito europeo è stato il *Bundestag* tedesco, approvando nel giugno 2017 la controversa *Netzwerkdurchsetzungsgesetz* (*NetzDG*).

Ribattezzato nell'opinione pubblica "*Facebook-Gesetz*" (in inglese: *Facebook Act*), il provvedimento federale ha costituito una risposta energica dello Stato tedesco alle significative recrudescenze di odio e disinformazione online affacciatesi nel dibattito pubblico verso la fine del 2015, a seguito della scelta governativa di aumentare esponenzialmente l'accoglienza di rifugiati siriani[75].

In tale contesto, la richiesta del Governo alle principali piattaforme di rimuovere i contenuti online ha assunto, in prima battuta, le vesti di uno strumento di *soft law*: su iniziativa del Ministero Federale della Giustizia e della Tutela dei consumatori, si istituiva una *task force* composta da *Internet Service Providers* e organizzazioni della società civile, guidati dal comune obiettivo di cancellare ogni spazio ai contenuti di odio e disinformazione online[76].

In effetti, il progetto alla base della *task force* esprimeva proprio l'idea per cui «[l]e piattaforme di social media [potessero] essere una forza trainante per creare consapevolezza sociale e promuovere un cambiamento positivo»[77]. Eppure, pur apprezzata in ambito europeo[78] (tanto da costituire il modello per un Codice di condotta contro l'odio online in seno all'Unione europea[79]), la grande concertazione pubblico-privata non sortiva fin dall'inizio gli effetti sperati.

Può dunque osservarsi come la *NetzDG* entri in scena in veste di *extrema ratio* successivamente a un tentativo di collaborazione con i "giganti del Web" giudicato fallimentare, ove la soluzione operata dal legislatore tedesco costituisce una sostanziale delega di responsabilità: da quella condivisa nella struttura pubblico-privata della *task force* si addiviene a una responsabilità in via esclusiva, che trasforma i *Providers* nei soli «organizzatori e curatori della comunicazione»[80] nello spazio digitale.

Il profilo di vera novità della Legge è però nell'articolazione del modello di responsabilità, incasellata ora in un ampio reticolato di obblighi molto stringenti per le piattaforme, la cui violazione comporta l'irrogazione di elevatissime sanzioni pecuniarie[81].

L'ambito di applicazione è limitato a quelle piattaforme di *social network* che operino nel territorio tedesco con scopo di profitto e che abbiano in esso almeno due milioni di utenti: vengono dunque in gioco un criterio "soggettivo" di natura qualitativa (piattaforme deputate al c.d. *social networking*, cioè alla interazione tra utenti) e uno di natura quantitativa, per cui si ritiene che soltanto gli *Internet Service Providers* numericamente "più forti" – anche in termini di bilancio – possano ottemperare agli obblighi del provvedimento[82].

[74] *Ivi*, 177.

[75] Cfr. il rapporto rilasciato nel 2018 dall'Organizzazione britannica per i diritti umani *Article 19*, dal titolo "*Germany: Responding to 'hate speech'*", nella cui introduzione si afferma: «*[i]t is estimated that in 2015, 60% (over 700,000) of asylum applications in the EU were filed in Germany. The German public's initial welcoming attitude towards refuges and asylum seekers in the summer of 2015 was short-lived. It was replaced with irrational fear in the population, populist rhetoric, and even instances of hatred and physical violence against asylum seekers and refugees. In 2017, this led to the Alternative for Germany (AfD), a far-right political party, gaining strength and seats in most regional parliaments*». Il documento riprende i dati sui richiedenti asilo dell'Ufficio statistico dell'Unione europea (Eurostat), le quali mostrano come proprio nel 2015 si sia raggiunto il picco massimo, pari a 1.282.690 domande d'asilo, di cui 1.216.860 presentate per la prima volta.

[76] Il progetto scaturiva da una lettera inviata dall'allora Ministro federale Heiko Maas a *Facebook*, al quale si chiedeva pubblicamente di fermare l'odio razziale dilagante sulla propria piattaforma. Per il testo di tale missiva, si rinvia a Huber e Hasters, "*Facebook: "Kein Ort für Rassismus"*", su *Der Tagesspiegel*, 27 agosto 2015.

[77] Ossia «*gemeinsam von der Überzeugung geleitet, dass Hassbotschaften in sozialen Medien keinen Platz*» [trad it. libera di chi scrive]. Cfr. il testo in lingua tedesca del documento dal titolo *Gemeinsam gegen Hassbotschaften Ergebnispapier der Task Force "Umgang mit rechtswidrigen Hassbotschaften im Internet" vorgeschlagene Wege zur Bekämpfung von Hassinhalten im Netz*, approvato il 15 dicembre 2015 dal *Bundesministerium der Justiz und für Verbraucherschutz*.

[78] Si veda il discorso "*United Against Hate Speech on the Web: Where do we stand?*" proferito a Berlino il 26 settembre 2016 da Věra Jourová, l'allora Commissario europeo per la giustizia, la tutela dei consumatori e l'uguaglianza di genere, che mostra «*appreciation for Minister Maas and the leadership role Germany has taken in tackling hatred online*» e definisce la *task force* a tale scopo istituita dallo Stato tedesco come «*a precursor as well as an example*».

[79] È il *Code of Conduct on countering illegal hate speech online* siglato il 31 maggio 2016 tra la Commissione europea e le quattro principali *Big Tech Companies* attive in ambito europeo (Facebook, Microsoft, Twitter, YouTube).

[80] «*Organisatoren und Kuratoren von Kommunikation*»: l'espressione è di Wagner G. (2020), p. 331.

[81] In Italia ne parlano Nardi (2019), pp. 22 ss.; Braschi (2020), pp. 168 ss.; Rinceanu (2021), pp. 333 ss.; Fiorinelli (2022), pp. 17 ss.

[82] Rileva dunque Reuter (2018) che, all'entrata in vigore della Legge, poco meno di una decina di *Providers* in Germania è soggetta agli obblighi della *NetzDG* (*Facebook*, *YouTube*, *Instagram*, *Twitter*, *Google+*, *Pinterest* e *Soundcloud*).

Accanto a tali criteri, la Legge tedesca delinea il proprio ambito di operatività in base a un ulteriore criterio "oggettivo": oggetto degli obblighi sono, cioè, quei contenuti illeciti («*rechtswidrige Inhalte*») elencati all'art. 1, comma 3 del provvedimento. Per assicurare una lettura nel solco della tipicità, il Legislatore tedesco non offre alcuna definizione generale di *hate speech* e *fake news*, ma opera un "*recursus ad Codicem*" e rinvia alle disposizioni dello *Strafgesetzbuch* relative, tra gli altri, ai delitti di incitamento a commettere reati e all'odio, di ingiuria e diffamazione di confessioni religiose e di singoli individui, di istituzione di associazioni a carattere criminale, terroristico o eversivo nei riguardi dello Stato, di pedopornografia, di falsificazione di dati e altre prove.

Nello schema della *NetzDG*, tali fattispecie sono anzitutto al centro di obblighi di rendicontazione semestrale, ispirate a regole di trasparenza verso gli utenti[83] e volte a offrire alle autorità competenti una panoramica delle statistiche e delle informazioni necessarie per la corretta implementazione della Legge[84]. Soprattutto, quelle fattispecie penali divengono il parametro per una procedura di "*content moderation*" ove, a fronte della segnalazione dell'utente, si prevede che il *Provider* rimuova o blocchi l'accesso ai contenuti manifestamente illeciti («*offensitlische rechtswidrige Inhalte*») entro ventiquattr'ore dalla ricezione della segnalazione, salvo sia stato concordato un termine più lungo con l'autorità giudiziaria competente. Un ulteriore termine di sette giorni è invece disposto dalla Legge per tutti gli altri contenuti che, semplicemente (e non manifestamente) illeciti, richiedano ulteriori valutazioni.

Nonostante i profili di indubbia novità e interesse, entrambe le categorie di obblighi – di trasparenza e di autoregolamentazione della piattaforma – hanno attirato numerose critiche.

Da un lato, i *reports* semestrali sono apparsi subito lacunosi, rivelando l'indiscusso primato dei *policy standards* sui *legal standards*. Solitamente, infatti, si sono privilegiate le linee guida delle piattaforme rispetto alle norme penali richiamate dalla *NetzDG*: in quanto valide universalmente[85], le prime consentono di bloccare o rimuovere un contenuto "una volta per tutte", senza la necessità di ripetere l'operazione in ogni Paese sulla base di nuove e analoghe segnalazioni di altri utenti[86].

Non c'è allora da stupirsi se, ad esempio, il report di *YouTube* dal titolo "*Removals under the Network Enforcement Law*" riporti – nell'ultima versione disponibile, da gennaio a giugno 2023[87] – notevoli discrepanze tra i contenuti "*removed globally*" in forza delle linee guida di *Google* e quelli "*removed locally*", ai sensi della *NetzDG*.

Il vero *punctum dolens* della Legge tedesca rimane tuttavia nella sua procedura di gestione delle segnalazioni. Non sono infatti mancate, dall'altro lato, critiche per l'enorme pregiudizio a numerose libertà di rango costituzionale[88], oltre che per la violazione di obblighi di natura sovranazionale[89], per cui si è detto che la «burocrazia privata» dei *Providers* sopperisce alle lacune dello Stato tedesco nel monitoraggio della rete, sostituendo a un modello accusatorio un modello inquisitorio[90].

In particolare, si è lamentato che tale impianto abbia sortito un effetto "agghiacciante" (c.d. "*chilling effect*") sulle opinioni e sulle interazioni degli utenti, dissuasi *ab origine* da dichiarazioni critiche per la paura di essere stigmatizzati e, in seguito, assoggettati a procedimenti

[83] Löber e Rossnagel (2019), p. 71: «[*m*]*it der gesetzlichen Berichtspflicht nach § 2 NetzDG soll "die gebotene Transparenz für die breite Öffentlichkeit" hergestellt werden*».
[84] Wagner B. *et al.* (2020), p. 262.
[85] Costituendo «un insieme di regole, valide in tutto il mondo e destinate ad avere la massima applicazione ed efficacia possibile», come affermano Löber e Rossnagel (2019), p. 72 («[*a*]*lleiniger Entscheidungsmaßstab ist das eigene, weltweit gültige Regelwerk, das größtmögliche Anwendung und Wirkung entfalten soll*» [trad. it. di chi scrive]).
[86] Così Heldt (2019), p. 37: «[*c*]*onsidering that content might be illegal in several countries, deleting it according to community guidelines might be more effective than taking it down for just one single country, with the possibility of repeating this action in another country further down the line*».
[87] Essendo entrato in vigore ad agosto 2023 lo "*ius superveniens*" del *Digital Services Act* dell'Unione europea, applicabile direttamente anche in Germania. Il report è, però, tuttora disponibile alla pagina web di Google intitolata *Removals under the Network Enforcement Law* (*https://transparencyreport.google.com/netzdg/youtube?hl=en*).
[88] Per un'ampia disamina, Claussen (2018).
[89] Ad esempio, sulla violazione del principio di territorialità della Direttiva E-commerce e delle sue deroghe, Spindler (2017); sulla violazione del divieto di obblighi di monitoraggio preventivo, Holznagel (2018)
[90] Così Wagner G. (2020), p. 330. Paradigmatico è stato il caso della parlamentare di *Alternative für Deutschland* Beatrix von Storch che, a poche ore dall'entrata in vigore della *NetzDG*, dopo essersi "scagliata" verbalmente su *Twitter* contro la polizia di Colonia, colpevole – secondo la von Storch – di aver "twittato" gli auguri di Capodanno in molte lingue, compreso l'arabo, si è vista bollare il commento come *hate speech*, poi subito rimosso dalla piattaforma insieme al suo *personal account*. Nei giorni successivi, tale limitazione della libertà di espressione ha sollevato numerose polemiche nei riguardi del Governo tedesco, anche a seguito della notizia per cui la von Storch e un altro parlamentare di *AfD* erano stati posti sotto indagine per incitamento all'odio dalla stessa polizia di Colonia.

penali[91], con inevitabile compromissione della libertà di manifestazione delle proprie opinioni in modo accessibile a tutti, scolpita all'art. 5, co. 1 della *Grundgesetz*.

E non è stato risparmiato, secondo i più critici, neppure il co. 2 dell'art. 5 *GG*, che toglie icasticamente ogni spazio alla censura nella Repubblica tedesca: la previsione di elevatissime sanzioni pecuniarie[92] per l'inottemperanza agli obblighi della *NetzDG* ha prodotto un eccesso di attivismo nel blocco e nella rimozione di contenuti (c.d. "*overblocking*") da parte dei *Providers*, garantito dalla mancanza di strumenti sanzionatori per la cancellazione di contributi leciti, che invece richiederebbero una pronta reintegrazione a fronte della dimostrata inoffensività. È noto, infatti, che – nel quadro della *NetzDG* – «solo "troppa poca cancellazione" (di contributi illeciti) è minacciata di sanzioni, mentre "troppa cancellazione" (di contributi leciti) rimane priva di sanzioni»[93].

Un simile squilibrio tra l'intervento su (presunti) contenuti illeciti e la (mancata) reintegrazione di contenuti leciti è sintomatico della preferenza accordata alla *compliance* delle piattaforme con gli obblighi della Legge tedesca a scapito del ruolo degli utenti e di una logica preventiva fondata sulla cooperazione tra *stakeholders* e *shareholders* del Web, che rimane invece un punto irrisolto.

Irrisolto sembrerebbe, in realtà, perfino lo stesso modello di responsabilità fondato dalla *NetzDG* in capo ai *Providers*: se le sanzioni milionarie sono da taluni qualificate come penali[94], da talaltri sono ritenute amministrative[95] – *species*, quest'ultima, sulla quale potrebbero comunque intervenire gli ormai consolidati criteri "Engel" a suggellarne una volta per tutte la natura *sostanzialmente* penale[96]. Peraltro, tale soluzione sembrerebbe avallata dalla previsione di un'esplicita posizione di vigilanza riscontrabile nell'obbligo di monitoraggio mensile affidato dall'art. 3 della Legge al *management* del *social network*[97], che più facilmente ricondurrebbe la questione nell'orbita del reato omissivo.

In altre parole, il *Bundestag* avrebbe realizzato nei fatti ciò che, nel dibattito italiano, si è soltanto postulato per via pretoria: un obbligo di intervento successivo alla pubblicazione del contenuto (da parte dell'utente) e alla conoscenza qualificata della sua illiceità penale (da parte del *Provider*). Diversamente dalla normativa italiana di recepimento della Direttiva *E-commerce*, esclusivamente incentrata su profili di responsabilità civile, la *Telemediengesetz* del 2007 in Germania avrebbe costituito, infatti, nel proprio silenzio, una «regolamentazione trasversale intergiurisdizionale»[98], in grado di tenere aperta la porta a modelli di responsabilità penale come quello in oggetto.

La conferma di una simile disciplina – e, più in generale, di un tal ruolo del diritto penale nello spazio digitale – si è rivelata, da più parti, altamente problematica per gli effetti perversi sul dibattito online che si sono in precedenza menzionati.

Va dato atto all'ordinamento tedesco di aver operato significativi interventi sul testo legislativo della *NetzDG*[99], nell'auspicato tentativo di bilanciare la soluzione originaria con il

[91] In questi termini, Liesching (2018), p. 28. Sul tema, cfr. il report di Perch (2021).

[92] Nei confronti del responsabile della violazione, l'art. 4 della *NetzDG* prevede ammende fino a cinquecentomila euro, per i casi meno gravi, e fino a cinque milioni di euro, per i casi più gravi. Le stesse somme possono essere inoltre decuplicate nei confronti dell'ente, cioè della *Big Tech Company*.

[93] Così Hong (2018): «[*n*]*ur das "Zuwenig-Löschen" (von rechtswidrigen Beiträgen) wird mit Sanktionen bedroht, das "Zuviel-Löschen" (von rechtmäßigen Beiträgen) bleibt dagegen sanktionslos*» [trad. it. di chi scrive].

[94] In Germania, ad es., è la posizione di Hoven (2018), p. 99: «[*m*]*it dem Netzwerkduchgesetzungsgesetz (NetzDG) vom September 2017 […] dürfte die Aussicht, persönlich für illegale Inhalte strafrechtlich zur Verantwortung gezogen zu werden, den Druck auf Betreiber von Internetplattformen noch deutlich erhöhen*»; in Italia, Galli (2019), p. 38, che si esprime in termini di obbligo di cancellazione «assistito da sanzione penale».

[95] In Germania, Claussen (2018), p. 119: «[…] *the NetzDG states the violations of the reporting duties or the procedures regarding complaints about unlawful content as an administrative offence, according to Art. 4*»; in Italia, Nardi (2019), p. 281: «[i]l mancato rispetto della disciplina comporta l'applicazione di una sanzione amministrativa pecuniaria».

[96] Data, come noto, dai tre criteri fissati dalla Corte EDU, *Engel e altri c. Paesi Bassi* (8 giugno 1976, serie A n. 22), § 82, operanti anche disgiuntamente: 1) la qualificazione del diritto interno; 2) la natura dell'infrazione; 3) la severità della pena. Nel caso della *NetzDG*, la severità della sanzione e il richiamo alle fattispecie dello *Strafgesetzbuch* suggerirebbero una forma di responsabilità sostanzialmente penale in capo alla piattaforma. In tema, Mazzacuva F. (2017), spec. 95 ss.

[97] Per cui è previsto che i responsabili della piattaforma debbano monitorarla attraverso controlli mensili («*muss durch monatliche Kontrollen überwatch werden*»), secondo la nota posizione da *Überwachergaranten* tipicamente fondante il reato omissivo. Il garante di vigilanza ha, come noto, il compito di «*Eindämmen einer konkreten Gefahrenquelle*», del contenimento di una specifica fonte di pericolo. Così, per tutti, Kaufmann (1959), p. 283.

[98] In questi termini, Hoven (2018), p. 98. Sulla compatibilità tra obblighi della Direttiva *E-commerce* e posizioni di garanzia, Schröder (2006), p. 673: «[*w*]*enn die EG-Verordnung die Pflichtigen beschreibt und die einzelnen Handlungspflichten im Sinne von Handlungsgeboten formuliert, kann auch bei der Prüfung eines Unterlassungsdelikts auf die Heranziehung dieser Regelungsmaterie nicht mehr verzichtet werden*».

[99] Ci si riferisce anzitutto al «Progetto di legge sulla lotta all'estremismo di destra e ai crimini d'odio» (RegE 19/17741: «*Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität*»), presentato dopo l'attentato alla sinagoga di Halle nell'ottobre 2019 e, in

maggior intervento della macchina statale nella "*content moderation*", se non altro in forma di garanzie e meccanismi di tutela di fronte alle arbitrarie decisioni del *Provider*. Tanto non è bastato: nel 2021 *Google* ha intrapreso un ricorso al Tribunale amministrativo di Colonia avverso le disposizioni della *NetzDG*, in base all'asserita violazione della *privacy* dei propri utenti[100], confermando invero l'insostenibilità di quel «campo minato per i *social networks*»[101]. Il 1° marzo 2022 il Tribunale amministrativo ha accolto la richiesta di tutela d'urgenza presentata da Google, ritenendo che le disposizioni del NetzDG da loro contestate violassero la Direttiva *E-commerce*, con particolare riguardo al principio del Paese d'origine (art. 3). Di conseguenza, i giudici amministrativi hanno dichiarato la temporanea inapplicabilità di tali norme fino a una nuova decisione definitiva nel merito, di fatto affermando il contrasto tra la Legge tedesca sui *social networks* e il diritto dell'Unione europea[102].

Il modello tedesco, però, non è rimasto del tutto *vox clamantis*, riuscendo a ispirare altre discipline legislative in ambito europeo – a cominciare da quelle francese[103] e austriaca[104], come altre di stampo ben più illiberale[105] – fino a costituire un esempio per la nuova regolamentazione europea.

5. Vent'anni dopo l'*E-commerce*: l'Unione europea alla prova del *Digital Services Act*. Gli "incerti confini" della nozione di «illegal content».

Si è osservato che non vi è prova più evidente dell'influenza della *NetzDG* rispetto all'approvazione del *Digital Services Act* dell'Unione europea[106], nuovo Regolamento che sembrerebbe capitalizzare alcune criticità della Legge tedesca. Sarebbe, però, riduttivo e inopportuno definirlo esclusivamente una prosecuzione dell'opera iniziata dal Legislatore di Berlino. La proposta del *Digital Services Act*, piuttosto, si iscrive nel più ampio e nobile intento di gettare le basi dell'avvenire digitale dell'Unione («*shaping Europe's digital future*», secondo il sito della Commissione europea[107]) mediante un insieme di disposizioni volte alla tutela dei dati personali e dei diritti fondamentali, al controllo della navigazione dei minori sul Web, al con-

seguito a ulteriori critiche, all'ancor più organica proposta di modifica della *NeztDG* (RegE 19/18792: «*Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes*»), infine approvata dal *Bundestag* il 18 giugno 2020.

[100] Sulla vicenda, cfr. l'articolo di Busvine, "*Google takes legal action over Germany's expanded hate-speech law*", in *www.reuters.com*, 27 giugno 2021.

[101] Come definiscono la *NetzDG* Spiegel e Heymann (2020), pp. 344 ss.

[102] Cfr. *Verwaltungsgericht Köln*, decisione del 1° marzo 2022 n. 6 L 1277/21, relativa al provvedimento cautelare in materia di tutela d'urgenza nei confronti delle disposizioni della *NetzDG* contestate da *Google Ireland Ltd*. Analogamente, cfr. la decisione del medesimo Tribunale del 1° marzo 2022 n. 6 L 1354/21 a favore di *Meta Platforms Ireland Ltd*.

[103] Il riferimento è alla «*Loi no 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*», subito ribattezzata "*Loi Avia*" dalla prima firmataria, la deputata di *LaREM* Lætitia Avia. Il testo, come riportato nella relazione introduttiva, mirava ambiziosamente a «ripristinare lo stato di diritto su Internet, e ricordare che le disposizioni di legge hanno la precedenza sulle generali condizioni d'uso di ogni operatore». A seguito di alcune modifiche suggerite dal *Conseil d'État* e mosse, in ispecie, dal rischio di incompatibilità con la Direttiva comunitaria sul commercio elettronico, nuovi emendamenti hanno condotto all'adozione di un articolato testo definitivo che, tuttavia, in fase di promulgazione ha dovuto affrontare una dirompente pronuncia del *Conseil constitutionnel*. Quest'ultimo, interpellato dal ricorso di ben sessanta senatori, ha sancito l'illegittimità costituzionale di gran parte della novella, smantellando l'impianto predisposto dal legislatore francese e mutilando numerosi degli originari diciannove articoli.

[104] Si tratta della Legge federale n. 2020/0544/A, intitolata «Legge federale relativa alle misure di protezione degli utenti delle piattaforme di comunicazione» o «*Kommunikationsplattformen-Gesetz* (*KoPl-G*)», basata sull'assunto – dato ai *media* dall'allora Ministra federale della Giustizia, l'On. Alma Zadic – per cui «Internet non è uno spazio avulso dalla legge». Benché maggiormente bilanciata rispetto alla *NetzDG* e alla *Loi Avia*, anche la *KoPl-G* ha subito attirato critiche da parte dell'OSCE e di altre organizzazioni per i diritti umani, fondate sulle preoccupazioni relative alla compressione della libertà di espressione in rete.

[105] In particolare, la Legge della Repubblica di Turchia n. 7253/2020 («Legge sulla regolamentazione delle pubblicazioni realizzate nell'ambito di Internet e sulla lotta ai reati commessi mediante queste pubblicazioni») approvata il 29 luglio 2020 (e subito definita "legge-bavaglio") e le "*Anti-Fake News Laws*" della Federazione Russa, promulgate il 18 marzo 2019. Ancorché emanate nell'alveo del Consiglio d'Europa, e pur manifestamente ispirate alla *NetzDG* tedesca, le due normative costituiscono, rispetto a quest'ultima, una ben più grave minaccia alla libertà di espressione, viste le modalità di gestione del dissenso all'interno dei due Paesi. È ciò che diviene poi ben più evidente nell'ordinamento cinese, che affianca al modello economicamente orientato degli Stati Uniti e a quello giuridicamente orientato dell'UE un ulteriore modello "statocentrico" dello spazio virtuale, nel quale le piattaforme digitali divengono la longa manus del controllo del potere pubblico sugli individui. Così Bradford (2023), pp. 69 ss.

[106] La «*no greater evidence of NetzDG's influence than recent enactment of the EU's DSA*» è evidenziata da Rinceanu e Stephenson (2023), p. 74.

[107] L'obiettivo si inserisce nell'ambito della IX Legislatura del Parlamento europeo (2019-2024): nel suo alveo rientra proprio la proposta di *Digital Services Act*. Si veda il link *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en*.

trasto alla disinformazione e alle altre minacce online, in una complessiva cornice di pluralità democratica, competitività economica, sostenibilità ambientale e alfabetizzazione digitale – in una parola, per un'Unione europea *leader* globale nello «sviluppo di *standards* digitali da promuovere a livello internazionale».

In realtà, uno dei maggiori obiettivi appare indubbiamente quello di domare i "giganti del Web"[108]. Il nuovo robusto e articolato quadro normativo sui servizi digitali[109] – fatto di 156 *considerando* e 93 articoli – si rivolge primariamente a questi ultimi, attraverso obblighi puntuali di individuazione di punti di contatto per le autorità (Art. 11 DSA) e per gli utenti (Art. 12 DSA), di nomina di legali rappresentanti in ogni Stato membro (Art. 13 DSA), di implementazione di termini e condizioni con l'indicazione di policies, procedure, provvedimenti e strumenti utilizzati nella "*content moderation*" (Art. 14 DSA), di rendicontazione per la trasparenza (Art. 15 DSA), di segnalazione e azione (Art. 16 DSA: c.d. "*notice and take-down*"), di motivazione delle decisioni agli utenti (Art. 17 DSA), di notifica delle infrazioni alle autorità (Art. 18 DSA), di predisposizione di un sistema interno di gestione dei reclami (Art. 20 DSA), di informativa sulla possibilità di risoluzione extragiudiziale delle controversie (Art. 21 DSA), di provvedimenti e protezione contro gli abusi (art. 23).

La base di partenza è costituita dalla Direttiva *E-commerce*, su cui il *Digital Services Act* si innesta, nell'intento di integrarla e non superarla[110] (nel suo titolo, il Regolamento è «relativo a un mercato unico dei servizi digitali e […] modifica la direttiva 2000/31/CE»), pur con i necessari aggiustamenti in considerazione dell'evoluzione del mercato digitale.

Tra i tratti fondanti la Direttiva del 2000, sono richiamate dal *Digital Services Act* le funzioni di *mere conduit*, *caching* e *hosting* (Artt. 4, 5 e 6 DSA)[111], cui di nuovo si accosta il divieto di obblighi di generale monitoraggio preventivo (Art. 8 DSA), in ossequio alla *net neutrality*.

La vera novità del Regolamento è rappresentata dal suo art. 7, che traspone nel contesto dell'Unione europea la figura del "*Good Samaritan*" statunitense, prevedendo la possibilità di esenzioni da responsabilità per i *Providers* che «in buona fede e in modo diligente» abbiano intrapreso iniziative o misure per ottemperare al diritto dell'Unione o a quello nazionale.

Non è difficile riconoscere qui una *contaminatio* ancor più evidente di quella che, a suo tempo, aveva dimostrato la Direttiva *E-commerce* nei confronti della disciplina adottata dal Congresso.

Al tempo stesso, il *Digital Services Act* parrebbe influenzato dalle eccezioni al requisito dell'*actual knowledge* previste dalla normativa statunitense in tema di *copyright*. Accanto alla positivizzazione della figura del *Provider* attivo di cui all'art. 7 (benché quale buon Samaritano), l'art. 16 del nuovo Regolamento prevede infatti che gli *hosting Providers* ai quali siano pervenute notificazioni acquistino conoscenza effettiva dell'illegalità dei contenuti in questione, sempre che questi permettano a una piattaforma diligente di riconoscerne la rilevanza senza approfondite valutazioni giuridiche[112]. E tali notificazioni obbligano peraltro il *Provider*, ai sensi del successivo art. 18, a informare sul contenuto in esame le autorità di polizia e giudiziarie dello Stato membro coinvolto.

Bagliori del modello tedesco, come si è anticipato, possono invece riscontrarsi nell'ampio articolato di obblighi previsti dal *Digital Services Act* in tema di trasparenza[113], tra cui figurano *in primis* l'obbligo di effettuare una valutazione preventiva dei rischi connessi all'utilizzo della piattaforma (Art. 34) e di proporre soluzioni per la loro mitigazione (Art. 35 DSA), l'obbligo di *reports* semestrali (Art. 42 DSA), l'obbligo di consentire l'accesso ai dati (c.d. *disclosure*) ad autorità e ricercatori (Art. 40 DSA)[114].

Deve osservarsi come, nella crasi tra l'esperienza d'oltreoceano e quella del vecchio Continente, la logica del nuovo Regolamento sia quella di «stabilire un principio, ma poi riempirlo di

[108] Eifert *et al.* (2021), pp. 987 ss. Interessante la prospettiva fondante il menzionato processo di trasformazione: dal "domare le masse ululanti" ("*taming the howling mobs*") al domare i *gatekeepers* del Web ("*taming the giants*"). Sul tema della responsabilità degli intermediari digitali nel nuovo Regolamento europeo, *ex multis*, Braschi (2023).

[109] Tra i più noti commentari sull'argomento, cfr. Wilman *et al.* (2024); Novovic (2024); Raue e Hofmann (2024).

[110] «[*B*]*y building on it, not over it*», come affermano Turillazzi *et al.* (2023), p. 104.

[111] Sul punto, rileva bene Vicinanza (2025), p. 10, che esse sono «sostanzialmente sovrapponibili agli articoli 12, 13, 14 e 15 della direttiva sul Commercio Elettronico».

[112] È l'art. 6, § 3 DSA a disporre che «le segnalazioni di cui al presente articolo permettono di acquisire una conoscenza o consapevolezza effettiva ai fini dell'articolo 6 in relazione alle specifiche informazioni in questione qualora consentano a un prestatore diligente di servizi di memorizzazione di informazioni di individuare l'illegalità della pertinente attività o informazione senza un esame giuridico dettagliato».

[113] Su tali obblighi e in un'ottica di *compliance*, cfr. D'Agostino (2023); Birritteri (2023).

[114] Sul punto, Turillazzi *et al.* (2023), p. 95, che affermano: «[t]*he DSA stands by the fact that providers of intermediary services must disclose, in their Terms of Service (ToS), any policies, procedures, measures, and tools used for content mod eration (i.e. algorithmic decision-making)*».

eccezioni»[115], muovendosi secondo un approccio "asimmetrico" e, per certi versi, incongruente.

Non sfugge, per esempio, il contrasto tra la ricordata assenza di obblighi di monitoraggio *ex ante* (Art. 8 DSA) e la possibilità per i *Providers* di impedire una violazione («*to prevent an infringment*») su richiesta dell'autorità, così *de facto* svolgendo controlli preventivi[116].

Nondimeno, le varie tipologie di piattaforme considerate dal *Digital Services Act* – dalle *Very Large Online Platforms* (*VLOPs*) alle *micro* e *small enterprises* – rivelano, nelle differenze di trattamento, «un apparato sanzionatorio severo, ma nebuloso nella sua configurazione»[117].

Le difficoltà applicative si devono, peraltro, anche al ruolo preponderante dei Coordinatori dei servizi digitali (Art. 49 ss. DSA), i cui poteri costituiscono il presidio dell'attività ispettiva e sanzionatoria a livello nazionale, contribuendo, però, a far ravvisare nel Regolamento europeo «un approccio "statocentrico", anziché "eurocentrico"»[118], lontano dalla logica dell'armonizzazione.

Ancorché *trait d'union* tra la Commissione europea e le altre autorità nazionali, tali Coordinatori godono infatti di grande discrezionalità nell'applicazione delle sanzioni, le cui regole di irrogazione sono stabilite dai singoli Stati membri (Art. 52 DSA)[119], in misura certamente considerevole – fino al 6% del fatturato globale annuo riferito all'esercizio precedente, per le violazioni più gravi, e fino all'1% del fatturato globale annuo riferito all'esercizio precedente, per le violazioni "minori"[120].

Le maggiori incertezze appaiono, tuttavia, sul piano definitorio.

Il vero punto nodale è infatti racchiuso nell'ampia e vacua nozione di contenuto illecito (*rectius*: illegale). Il Regolamento europeo – al suo Art. 3, lett. h – stabilisce che è tale «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»[121].

Non si comprende bene, cioè, a che cosa sarebbe rivolto l'ampio articolato di obblighi approntato dal legislatore europeo: quale sia, in una parola, l'oggetto della *compliance* delle piattaforme, che è rimesso a qualche remota fonte dell'Unione e, soprattutto, al diritto interno agli Stati membri.

Peraltro, anche la definizione di ciò che è lecito (*rectius*: legale) viene lasciata completamente nelle mani di questi ultimi. Tra le premesse al Regolamento, infatti, il *Considerando* n. 39 prevede la possibilità, 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».

Nella difficoltà di tracciare il perimetro tra lecito e illecito, e fornire così un sostrato di tassatività-determinatezza al *Digital Services Act*, non sono mancati i commentatori che hanno proposto un combinato disposto tra le disposizioni del Regolamento e l'ancor più recente

[115] Così sottolinea Zeno-Zencovich (2023), p. 13: «[*t*]*he first technique adopted is that of establishing a principle, but subsequently empty ing it through an exception*».

[116] Lo rilevano Turillazzi *et al.* (2023), p. 101, che soggiungono come tali incongruenze rendano potenzialmente controversa l'implementazione del Regolamento e consentano notevoli difformità tra gli Stati membri («[*i*]*nconsistencies in some articles of the DSA may result in a contradictory application of the novel regulation and further fragmentation amongst MSs*»).

[117] Così, con riferimento al DSA, Sarzana di Sant'Ippolito (2023), p. 400.

[118] *Ivi*, 403. E ciò, benché i Coordinatori siano a loro volta "coordinati" dall'*European Board for Digital Services*, ai sensi degli Artt. 61 ss. DSA.

[119] Il quale prevede che «[g]li Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione del presente regolamento da parte dei fornitori di servizi intermediari che rientrano nella loro competenza e adottano tutte le misure necessarie per assicurarne l'applicazione in conformità dell'articolo 51». Perciò Turillazzi *et al.* (2023), p. 101, evidenziano che la responsabilità primaria per l'applicazione del DSA spetta ancora agli Stati membri, piuttosto che all'Unione europea, con ulteriori incongruenze e frammentazioni a livello nazionale. Da evidenziare, inoltre, che in Italia il d.l. 15 settembre 2023, n. 123 (c.d. "Caivano"), convertito con modificazioni dalla L. 13 novembre 2023, n. 159, ha indicato al suo art. 16 quale Coordinatore dei Servizi Digitali l'Autorità per le garanzie nelle comunicazioni.

[120] Nei casi di "*very large online platforms*" (*VLOPs*) e "*very large search engines*" (*VLSEs*) la potestà sanzionatoria è della stessa Commissione *ex* Art. 74 DSA. Sul riparto di competenze tra livello nazionale e sovranazionale, v. Sabia (2023).

[121] Sul punto, ancora, Turillazzi *et al.* (2023), p. 94, che notano la grande incertezza definitioria. Molto critico anche Zeno-Zencovich (2023), p. 13, che, 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. Lo specchio dell'incertezza normativa è dato, peraltro, dai meccanismi di *risk assessment* e di *risk mitigation* (Artt. 34 e 35 DSA) richiesti alle piattaforme attraverso i loro algoritmi, le cui decisioni, tuttavia, secondo l'A. (p. 14) si risolvono in uno «screening che ha cancellato da Internet Madonne che allattano, putti, dipinti e sculture di Venere, città e persone il cui nome rientrava nel vocabolario primitivo politicamente scorretto di Facebook».

Direttiva sulla lotta alla violenza di genere e domestica, in una interessante prospettiva di "intersezionalità" europea[122].

Intanto, è forse ancora presto per attestare il «*Brussels effect*» del *Digital Services Act*, nel contributo alla *governance* dei servizi digitali al di fuori dell'Unione[123] (pur non mancando certo l'interesse di numerosi Paesi in via di adesione a quest'ultima).

Ciò che è evidente, ad oggi, è che esso rappresenta «un punto di partenza piuttosto che di arrivo»[124] (o, se si preferisce, piuttosto che un "porto sicuro") e che la sua struttura potrà essere ulteriormente implementata, proprio a cominciare dalle sue zone d'ombra e dalle sue più basilari definizioni.

6. "*A matter of words*". La conoscibilità dell'illecito penale tra *legal standards* e *policy standards*. Sintesi e prospettive.

Da responsabili *per niente* a responsabili *per tutto*. In questa nemesi potrebbe compendiarsi il lungo cammino – ultraventennale – dalla sostanziale immunità degli *Internet Service Providers* al loro ruolo di primo piano nel contrasto ai contenuti illeciti *online*: dalla *liability* alla *compliance* con inediti reticolati di obblighi, dal "*Good Samaritan*" statunitense al *Digital Services Act* dell'Unione europea.

Molteplici sono, naturalmente, le questioni sottese e sollevate da questo marcato "*overturning*": la legittimazione dell'autorità privata della piattaforma nel determinare che cosa è illecito e che cosa non lo è[125], il ruolo sempre più capillare del diritto sovranazionale europeo nello stabilire nuovi obblighi di criminalizzazione[126], l'utilizzo di algoritmi – e gli interrogativi sulla loro responsabilità "mediata" – nella *detection* di contenuti illeciti[127].

Quella principale rimane, però, l'insostenibilità di un ruolo esclusivamente punitivo in capo alle piattaforme digitali, per le evidenti ricadute che ciò comporta sulla libertà di espressione degli utenti.

Se il *Digital Services Act* porta il merito di aver implementato meccanismi di *checks and balances* (attraverso la previsione di c.d. *disclosure policies* e meccanismi di ricorso), esso non ha tuttavia colto nel segno all'atto di definire chiaramente l'oggetto della *compliance* degli *Internet Service Providers*, cioè il fondamento dei loro stessi obblighi.

In punto di tassatività-determinatezza, è allora da preferire la soluzione del legislatore tedesco e il richiamo espresso della *NetzDG* del 2017 alle norme dello *Strafgesetzbuch*.

E se la scelta di un *numerus clausus* poteva dirsi inadeguata a descrivere una categoria in continua evoluzione come quella degli illeciti online, essa ha pur rappresentato, al contempo, un'indicazione tassativa per ogni *Provider* nell'azione tempestiva dinanzi a contenuti illeciti e nella propria periodica rendicontazione – in una parola, un'indicazione chiara sul *quid* della

[122] Per esempio, Allen (2023). Il richiamo è alla recente Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio del 14 maggio 2024 sulla lotta alla violenza contro le donne e alla violenza domestica, che, già nelle proprie premesse, riconosce che varie forme di violenza di genere sono intrinsecamente collegate al diffuso utilizzo delle nuove tecnologie (ICT), ben in grado di amplificare l'offensività dei tradizionali "*gender-based crimes*" e di mutare la stessa fisionomia di tali fattispecie (così, ad es., il *Considerando* n. 17). Vista la necessità di definizioni condivise («*harmonized definitions*»), il legislatore europeo ha fornito direttamente i caratteri fondanti alcuni fenomeni, come la condivisione non consensuale di materiale intimo o manipolato (art. 5), lo stalking online (art. 6), le molestie online (art. 7), l'istigazione alla violenza o all'odio online (Art. 8) determinata, tra gli altri, da motivi di genere. Da un lato, l'ampiezza delle definizioni offerte dalla Direttiva permette di considerare alcuni fenomeni di più recente emersione sul Web, come il c.d. voyeurismo digitale, l'utilizzo di intelligenze artificiali nella produzione di contenuti sessualmente espliciti (c.d. *deepfakes*), l'abuso sessuale a mezzo immagini istantanee (c.d. *cyberflashing*) e ogni altra nuova forma di diffusione non consensuale di contenuti intimi (si pensi, ad es., all'uso sempre crescente di messaggi vocali in tema di abusi o di c.d. *reels* nonché alla facilità con cui è possibile editare tali contenuti). Dall'altro, è però sostanzialmente nullo il margine di discrezionalità degli Stati membri intorno alla criminalizzazione dei fenomeni delineati dal legislatore sovranazionale, che introduce così una serie di obblighi positivi di criminalizzazione. La corretta implementazione di questi ultimi nelle varie legislazioni penali a livello nazionale non può che richiedere *standards* uniformi su alcuni aspetti determinanti, tra cui, in particolare, il ruolo del consenso alla produzione/diffusione dei contenuti online: aspetto che, pur menzionato espressamente dalla Direttiva, curiosamente non viene comunque analiticamente definito e su cui, dunque, permane non poca incertezza. Sulla Direttiva, tra i primi commenti degni di nota, si rinvia a Braschi (2024).

[123] Sul tema, Husovec e Urban (2024).

[124] Così Keller (2023), 237, che lo ritiene esattamente «*a starting point, rather than an end point*».

[125] Sul tema, *ex multis*, Martinelli (2018). Sul punto, sarebbe auspicabile un maggior affiancamento dell'autorità pubblica statale alla figura del *Provider*, «nella prospettiva della destrutturazione/ricostruzione del rapporto tra sfera pubblica e sfera privata», come ben affermava S. Rodotà (2012), p. 426.

[126] Per tutti, Mitsilegas (2009).

[127] Può condividersi l'assunto di S. Rodotà (2012), p. 403, per cui «il ricorso all'algoritmo non può divenire una forma di deresponsabilizzazione dei soggetti che lo adoperano». Similmente e più di recente, in tema di intelligenza artificiale, cfr. Kissinger *et al.* (2023), 88.

content moderation.

Non soltanto il *Digital Services Act* si dimostra lontano dalla logica dell'armonizzazione, rinviando la decisione su ciò che è illecito (e su ciò che è lecito) agli Stati membri; i problemi di una definizione tanto liquida sorgono anche in punto di conoscibilità dei potenziali illeciti online, su due livelli: quello dell'utente, che commetterebbe un illecito online e ne subirebbe le conseguenze senza saperlo e, *in secundis*, quello del *Provider*, che non avrebbe *in toto* gli strumenti per comprendere, in un contesto legislativo complesso come quello dell'Unione europea, che cosa "gestire" e che cosa no.

La moderazione dei contenuti affronta dunque una crisi sul piano della trasparenza/prevenzione, nei confronti degli gli utenti (che al momento della prima registrazione dovrebbero essere ben informati dalle linee guida delle piattaforme su cosa possono o non possono postare), e sull'ulteriore piano della gestione/segnalazione alle autorità, da parte degli ISP (che dovrebbero poter basare le proprie *policies* e i propri meccanismi di segnalazione/ricorso su illeciti predeterminati e non potenzialmente nuovi ogni volta).

Si assiste così al fenomeno inverso, alla prevalenza dei (*private*) "*community standards*" sui (*public*) "*legal standards*", dove questi ultimi tacciono e i primi si trovano a doverne colmare le lacune, molto spesso in modo eccessivamente arbitrario e restrittivo[128]. In quest'ottica, i problemi sollevati dalla *NetzDG* rimangono un'eredità pesante e un monito vivo per il legislatore europeo che, certamente animato dalle migliori intenzioni, ha fatto tuttavia il passo più lungo della gamba, fondando la propria riflessione sulla responsabilità lontano dalla tipicità, che è però fondamento e limite della prima.

Potrebbe qui soccorrere uno sguardo attento alla più recente regolamentazione del Regno Unito, il c.d. *Online Safety Act*, nella cui impostazione di "*safety by design*" rispetto alle problematiche dello spazio digitale – cioè, nell'idea fondante di «ridurre la tendenza di un certo prodotto o servizio a creare o esacerbare tali problemi»[129] – può ravvisarsi il merito dell'efficacia della novella.

Come si è osservato nella dottrina inglese, infatti, «nonostante la legge si concentri apparentemente sui sistemi e sui processi dei fornitori di servizi, la realtà è che la portata e l'applicazione dei doveri variano a seconda del tipo di contenuto e dei servizi. In particolare, gli obblighi variano a seconda dal tipo specifico di contenuto, che a sua volta dipende dall'applicazione di una serie di reati»[130].

Tale normativa, concentrandosi anzitutto sui contenuti di pornografia minorile e non consensuale, è decisamente articolata e specifica in tal senso. Benché infatti delinei in apertura un'ampia e generica nozione di contenuto illecito, inteso quale «*content that amounts to a relevant offence*»[131], essa si premura in seguito di individuare ben otto sezioni relative a tipologie di contenuti pornografici: dal più allarmante «*Child sexual exploitation and abuse material* (*CSEAM*)», classificato come «*priority illegal content*» fino alle "meno problematiche" «*Obscene (but not extreme) publications*», ritenute dalla Legge «*non-designated illegal content*»[132].

Certo, neppure l'*Online Safety Act* – ancora in fase di implementazione – si ritiene immune da vizi e da ricadute problematiche sulla libertà di espressione[133]; esso appare però maggiormente fermo e bilanciato nel prevedere un nuovo «*duty of care approach*»[134] di fronte alle

[128] È il caso, ad esempio, delle *policies* sui contenuti relativi alle immagini di nudo e atti sessuali di adulti offerte da *Meta*, che – in modo decisamente più articolato rispetto alla nozione legislativa di "sessualmente esplicito" – non consentono «immagini, e immagini digitali, di nudo di adulti, se raffigurano: genitali visibili (anche se coperti da peli pubici) tranne se contrassegnati da un avviso di contenuti visibili in un contesto medico o sanitario (ad es. parto e momenti successivi al parto, chirurgia di conferma del genere, esami per il cancro o altre malattie); ani visibili e/o primi piani di fondoschiena completamente nudi tranne se contrassegnati da un avviso di contenuti visibili in un contesto medico o sanitario o se modificati su un personaggio pubblico; capezzoli femminili in vista, ad eccezione di contesti di allattamento al seno, mastectomia, medico, sanitario o atti di protesta».

[129] «*The objective of "safety by design" is – like product safety – to reduce the tendency of a given feature or service to create or exacerbate such issues*»: così Woods (2024). Ciò è riscontrato anche dalle linee-guida del D*epartment for Science, Innovation and Technology* e del *Department for Digital, Culture, Media & Sport* del Governo britannico del 29 giugno 2021, dal titolo *Principles of safer online platform design* (*https://www.gov.uk/guidance/principles-of-safer-online-platform-design*), secondo le quali «*the process of designing an online platform to reduce the risk of harm to those who use it. Safety by design is preventative. It considers user safety throughout the development of a service, rather than in response to harms that have occurred*».

[130] «*Despite the Act ostensibly focusing on service providers' systems and processes, the reality is that the scope and application of duties vary based on the content type, as well as between services. In particular, obligations vary depending on the specific type of content which itself depends on the application of a range of criminal offences*». Così McGlynn *et al.* (2023), p. 14.

[131] Cfr. la *Section* 59(2) dell'*Online Safety Act 2023*.

[132] Per una panoramica di queste categorie, cfr. McGlynn *et al.* (2023), pp. 16 ss.

[133] Alcune preoccupazioni sono sollevate, ad. es., da Gerbrandt (2025).

[134] In questi termini, Gorwa (2024), p. 49.

numerose interazioni che ancora oggi attraversano i *social media*, tutt'altro che prossimi a una parabola discendente[135].

Dal modello inglese potrebbe cogliersi, in particolare, la suggestione di far coincidere il più possibile *standards* normativi e *standards* delle piattaforme, oltre a criteri di priorità nella valutazione degli illeciti penali online in base alla loro severità e potenziale pervasività, restituendo loro maggior determinatezza e conoscibilità. Muovendo dalla più chiara delimitazione dei fenomeni lesivi e dalla riformulazione degli *standards* di tutela ove necessario[136], nella maggior compenetrazione tra norme (penali) pubbliche e linee guida private mediante appositi codici di condotta indirizzati agli *Internet Service Providers*, potrebbero offrirsi maggiori e puntuali indicazioni all'utente al momento della sua registrazione o della segnalazione di presunti contenuti illeciti (attraverso appositi *banners* o *link* di approfondimento obbligatorio della possibile offesa subìta), così restringendo notevolmente l'alveo di una censura *de facto* arbitrariamente operata dalle piattaforme e sovrapponendolo a una rimozione *de iure* orientata secondo canoni predisposti dal legislatore[137].

Una simile implementazione e un tale miglior coordinamento delle linee guida potrebbe certamente interessare l'ordinamento dell'Unione europea, ancora alle prese con la piena attuazione del suo *Digital Services Act*, che in tale prospettiva potrebbe essere integrato da specificazioni sulla natura di ciò che costituisce contenuto illecito online, per esempio attraverso un protocollo addizionale o espliciti riferimenti, nel testo del Regolamento, ad altre fonti dell'Unione europea.

Anche in ambito europeo, quindi, di fronte alla richiamata «crisi epistemica» dello spazio digitale, la soluzione parrebbe quella di tornare al "design delle parole", più propriamente alla *littera legis* in materia penale[138]: all'idea fondamentale per cui il linguaggio chiaro e comprensibile impresso nelle norme e, di riflesso, nelle linee-guida delle piattaforme possa, per l'utente e per gli *Internet Service Providers*, arginare «resistenze creative» o, più semplicemente, «fraintendimenti di successo» dovuti all'assenza di trasparenza, prevenzione e chiarezza[139], favorendo un'equilibrata moderazione dei contenuti online nella forma di una *compliance* "integrata" tra utenti, piattaforme e legislatori[140].

Bibliografia

Accinni, Giovanni Paolo (2017): "Profili di responsabilità penale dell'hosting provider "attivo"", *Archivio penale,* 2, pp. 1-21

Aceto di Capriglia, Salvatore (2018): "Gli illeciti *on line* e le nuove frontiere della responsabilità civile nell'era digitale", *federalismi.it,* 6, pp. 1-25

Aimi, Alberto (2017): *Le fattispecie di durata. Contributo alla teoria dell'unità o pluralità del reato*, Torino, Giappichelli, 2017

Allen, Asha (2023): "An Intersectional Lens on Online Gender-Based Violence and the DSA", in Hoboken van, Joris, Quintais, João Pedro, Appelman, Naomi, Fahy, Ronan, Buri, Ilaria, e Straub, Marlene (editors), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, (Berlin, Verfassungsbooks), pp. 121-133

[135] Cfr. Bogost, "*The Age of Social Media Is Ending. It never should have begun*", in *The Atlantic*, 10 novembre 2022.
[136] Si pensi, ad esempio, alle problematiche emergenti dalla nozione di *hate speech*, su cui ancora non vi è una definizione univoca a livello europeo; allo stesso modo, alla nozione di consenso nei reati sessuali, accertabile solo "in negativo".
[137] Cfr. Monti (2019), pp. 36 ss., ove l'A. distingue tra una censura *de facto*, operata spontaneamente dalle piattaforme digitali, e una censura *de iure* che a sua volta si articola in funzionale quando segue un intervento giudiziale ovvero sostanziale.
[138] Sul tema, in Italia, è certamente questo lo sforzo di K. Summerer *et al.* (2025), laddove si cercano di individuare i tratti fondanti le più ricorrenti categorie di illeciti penali online, per riempire di significato l'ampia nozione di contenuto illecito offerta dal *Digital Services Act*.
[139] È il concetto ripreso da Hildebrandt (2017), p. 308: «[*h*]*uman language facilitates shared meaning and 'common sense', as well as the ability to disrupt such meaning by means of creative resistance or simply by generating successful misunderstandings that—in turn—lead to subtle or not so subtle shifts in meaning*».
[140] Sul ruolo integrato degli utenti, cfr. Kissinger *et al.* (2023), 95*:* «[i]n un certo senso, l'individuo diventa parte di un sistema in cui l'intelligenza umana e quella artificiale collaborano per guidare un intero gruppo di persone attraverso le strade da esse prescelte». Sul tema degli "interventi positivi" nell'alveo dei contenuti sessualmente espliciti online, cfr. inoltre Flynn *et al.* (2024).

Antolisei, Francesco (2003): *Manuale di Diritto penale. Parte Generale* (a cura di L. Conti, Milano, Giuffrè)

Antonucci, Antonia (2001): "eEurope: la costruzione del quadro normativo", in Ead. (editor), *E-Commerce. La Direttiva 2000/31/CE e il quadro normativo della rete* (Milano, Giuffrè), pp. 1-25.

Apa, Ernesto, e Pollicino, Oreste (2013): *Modeling the liability of internet service providers: Google vs. Vivi down. A constitutional perspective* (Milano, Egea)

Baccin, Alice (2020): *Responsabilità penale dell'*Internet Service Provider *e concorso degli algoritmi negli illeciti* online: il caso *Force v. Facebook*, *Sistema penale*, 5, pp. 75-102.

Benanti, Paolo (2024): *Il crollo di Babele. Che fare dopo la fine del sogno di Internet?* (Milano, Edizioni San Paolo)

Benatti, Francesca, Portonera, Giuseppe (2024): "La responsabilità di diritto civile degli Internet Service Providers. Spunti dalla comparazione con la giurisprudenza statunitense", *Nuova Giurisprudenza Civile e Commerciale*, 2, pp. 476-485

Berners-Lee, Tim (1999): *Weaving the Web. The* Past, Present *and* Future *of the* World Wide Web *by its* Inventor (New York, Harper)

Bianchi, Claudia (2021): *Hate speech. Il lato oscuro del linguaggio* (Roma-Bari, Laterza)

Birritteri, Emanuele (2023): "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", *Media Laws – Rivista di diritto dei media*, 2, pp. 52-87.

Botan, Madalina, Stefuerac, Remus, Stancea, Andreea (2025): "Electoral dynamics in the age of disinformation: Understanding Romanian voter support for nationalist populist parties in the 2024 election", *New Perspectives*, 33, 2, pp. 103-121.

Bradford, Anu (2023): *Digital Empires: The Global Battle to Regulate Technology*, Oxford-New York, Oxford University Press)

Braschi, Sofia (2020): "*Social media* e responsabilità penale dell'*Internet Service Provider*", *MediaLaws – Rivista di diritto dei media*, 3, pp. 157-177

Braschi, Sofia (2023): "Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli *Internet Service Provider*?", *Diritto Penale e Processo*, 3, pp. 367-377

Braschi, Sofia (2024): "La nuova direttiva sulla lotta alla violenza contro le donne e alla violenza domestica e le sue ricadute nell'ordinamento nazionale", *Diritto penale e processo*, 10, pp. 1367-1379

Cadoppi, Alberto (2022): *Il "reato penale". Teorie e strategie di riduzione della criminalizzazione* (Napoli, Edizioni Scientifiche Italiane)

Caletti, Gian Marco (2018): ""*Revenge porn*" e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane", *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 67-100.

Caletti, Gian Marco (2019): "Libertà e riservatezza sessuale all'epoca di Internet", in *Rivista italiana di diritto e procedura penale*, 4, pp. 2045-2090.

Caletti, Gian Marco (2021), "Can Affirmative Consent Save "Revenge Porn" Laws? Lessons from the Italian Criminalization of Non-Consensual Pornography", *Virginia Journal of Law & Technology*, 25, 3, pp. 117-174.

Caletti, Gian Marco (2024): Habeas corpus digitale. *Lo statuto penale dell'immagine corporea tra privatezza e riservatezza* (Torino, Giappichelli)

Canestrari, Stefano (2021): *Ferite dell'anima e corpi prigionieri. Suicidio e aiuto al suicidio nella prospettiva di un diritto liberale e solidale* (Bologna, Bononia University Press)

Celeste, Edoardo, Heldt, Amélie, Keller, Clara Iglesias (2022): *Constitutionalising Social Media* (Oxford, Hart Publishing)

Citron, Danielle Keats (2023): "How to Fix Section 230", *Boston University Law Review*, 103, pp. 713-761

Claussen, Victor (2018): "Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation", *MediaLaws – Rivista di diritto dei media*, 3, pp. 110-136

Crockett, May (2016): *"The Internet (Never) Forgets"*, *SMU Science and Technology Law Review*, 19, pp. 151-182

Crouch, Colin (2004): *Post Democracy* (Cambridge, Polity Press)

Curreli, Carlo (2017): "La controversa responsabilità del gestore di un sito web, in caso di diffamazione commessa da terzi", *Responsabilità civile e previdenza*, 5, pp. 1648-1659

D'Agostino, Luca (2023): "Disinformazione e obblighi di compliance degli operatori del mercato digitale alla luce del nuovo *Digital Services Act*", *Media Laws – Rivista di Diritto dei Media*, 2, pp. 16-51

De Natale, Domenico (2010): "La responsabilità dei servizi di informazione in Internet", in Ruggieri, Francesca, Picotti, Lorenzo (editors), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali* (Torino, Giappichelli), pp. 50-66

Di Ciommo, Francesco (2010): "Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line. A proposito della sentenza Google/Vivi Down", *Diritto dell'informazione e dell'informatica*, 6, pp. 829-857

Eifert, Martin, Metzger, Alex, Schweitzer, Heike, Wagner, Gerhard (2021): "Taming the giants: the DMA/DSA package", *Common Market Law Review*, 58, 4, pp. 987-1028

Fiorinelli, Gaia (2022), "L'attuale ruolo del provider nella società digitale: modelli di responsabilità penale", *La legislazione penale*, pp. 1-34

Floridi, Luciano (1997): *Internet. An Epistemological Essay* (Milano, Il Saggiatore)

Floridi, Luciano (2017): *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (trad. it. a cura di M. Durante, Milano, Raffaello Cortina Editore)

Floridi, Luciano, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022 (trad. it. a cura di M. Durante)

A. Flynn-A.J. Scott-E. Cama (2024): "An Empirical Research Study on Barriers, Facilitators, and Strategies to Promote Bystander Intervention in Intimate Image Abuse Contexts", in Caletti, Gian Marco, Summerer, Kolis (editors), *Criminalizing Intimate Image Abuse: A Comparative Perspective* (Oxford-New York, Oxford University Press), pp. 376-399

Fornasari, Gabriele (1990), *Il principio di inesigibilità nel diritto penale* (Padova, CEDAM)

Franks, Mary Anne (2024): *Fearless Speech* (New York, Bold Type Books)

Galli, Martina (2019): "Soltanto parole? Discorsi d'odio e intervento penale", in Petrilli, Raffaella (editor), *Hate speech. L'odio nel discorso pubblico. Politica, media, società* (Roma, Round Robin), pp. 23-40

Gerbrandt, Ricki-Lee (2025): "Threatening & protecting press publishers and journalism in the UK's regulation of social media platforms", *Journal of Media Law*, 17, 1, pp. 68-102

Gershberg, Zac, e Illing, Sean (2022): *The Paradox of Democracy. Free Speech, Open Media, and Perilous Persuasion* (Chicago, University of Chicago Press)

Gorwa, Robert (2024): *The Politics of Platform Regulation. How Governments Shape Online Content Moderation* (Oxford-New York Oxford University Press)

Grandi, Matteo (2017): *Far Web. Odio, bufale, bullismo. Il lato oscuro dei social* (Milano, Rizzoli)

Graw Leary, Mary (2018): "The Indecency and Injustice of the Communications Decency Act", *Harvard Journal of Law and Public Policy*, 41, 2, pp. 554-622.

Guerini, Tommaso (2020): Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali* (Torino, Giappichelli)

Heldt, Amélie P. (2019): "Reading between the lines and the numbers: an analysis of the first NetzDG reports", in Schulz, Wolfgang, Ketterman, Matthias C., Heldt, Amélie P., *Probleme und Pontenziale des NetzDG. Ein Reader bit fünf HBI-Experstisen* (Hamburg, Hans-Bredow-Instituts), pp. 30-44

Hildebrandt, Mireille (2017): "Saved by Design? The Case of Legal Protection by Design", *NanoEthics*, 11, pp. 307-311

Holznagel, Bernd (2017): "Das Compliance-System des Entwurfs des Netzwerkdurchsetzungsgesetzes", *Zeitschrift für Urheber- un Medienrecht*, 8-9, pp. 615-624.

Hong, Mathias (2018): "*Das NetzDG und die Vermutung für die Freiheit der Rede*", *www.verfassungsblog.de*

Horder, Jeremy (2022): *Criminal Fraud and Election Disinformation*, Oxford-New York, Oxford University Press

J. Hörnle, Julia (2021): *Internet Jurisdiction Law and Practice* (Oxford-New York, Oxford University Press)

Hoven, Elisa (2018): "*Die strafrechtliche Verantwortlichkeit der Betreiber von Social-Media-Plattformen*", *Zeitschrift für Wirtschaftsstrafrecht und Haltung in Unternehmen*, 4, pp. 97-106.

Husovec, Martin, Urban, Jennifer (2024): "Will the DSA have the Brussels Effect?", in Quintais, João Pedro (editor), *From the DMCA to the DSA. A Transatlantic Dialogue on Online Platform Regulation and Copyright* (Berlin, Verfassungsbooks), pp. 73-84.

Ingrassia, Alex (2012): "Il ruolo dell'ISP nel Ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano", in Lupària, Luca (a cura di), *Internet provider e giustizia penale: modelli di responsabilità e forme di collaborazione processuale* (Milano, Giuffrè), pp. 15-65

Ingrassia, Alex (2014): "La sentenza della Cassazione sul caso Google", *Diritto penale contemporaneo*

Ingrassia, Alex (2017): "Responsabilità penale degli internet service provider: attualità e prospettive", *Diritto Penale e Processo*, 12, pp. 1621-1628

Kaufmann, Armin (1959): *Die Dogmatik der Unterlassungsdelikte* (Göttingen, Klaus Schwarz)

Keller, Daphne (2023): "The European Union's New DSA and the Rest of the World", in Hoboken van, Joris, Quintais, João Pedro, Appelman, Naomi, Fahy, Ronan, Buri, Ilaria, Straub, Marlene (editors), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications* (Berlin, Verfassungsbooks), pp. 227-241

Keyes, Ralph (2004): *The post-truth era: dishonesty and deception in contemporary life* (New York, St. Martin's Press, New York)

Kissinger, Henry, Schmidt, Eric, Huttenlocher, Daniel (2023): *L'era dell'intelligenza artificiale. Il futuro dell'identità umana* (trad. it. a cura di A. Piccato, Milano, Mondadori)

Kosseff, Jeff (2019): *The Twenty-Six Words That Created the Internet* (New York, Cornell University Press)

Liddell, Pearson Jr., Eshee, William Jr. (2002): "Substantial Notice under the Digital Millennium Copyright Act", *Texas Wesleyan Law Review*, 8, 2, pp. 379-391

Liesching, Marc (2020): "Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG. Überblick über die wesentlichen Kritikpunkte", *Multimedia und Recht*, 1, pp. 26-30

Löber, Lena, Rossnagel, Alexander (2019): "Das Netzwerkdurchsetzungsgesetz in der Umsetzung", *Multimedia und Recht*, 2, pp. 71-76.

Manes, Vittorio (2022): *Giustizia mediatica. Gli effetti perversi sui diritti fondamentali e sul giusto processo* (Bologna, il Mulino)

M. Manetti, Michela (2014): "Libertà di pensiero e anonimato in Rete, Diritto dell'informazione e dell'informatica", 2, pp. 139-152

Manna, Adelmo, Di Florio, Mattia (2019): "Riservatezza e diritto alla privacy: in particolare, la responsabilità *per omissionem* dell'*internet service provider*", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (editors), *Cybercrime* (Milano Wolters Kluwer) pp. 961-1000

Martinelli, Silvia (2018): "L'autorità privata del provider", in Sirena, Pietro, Zoppini, Andrea (editors), *I poteri privati e il diritto della regolazione* (Roma, Roma-Tre Press), pp. 555-568

Mauri, Roberta Eleonora (2019): "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*

Mazzacuva, Francesco (2017): *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico* (Torino, Giappichelli)

McGlynn, Clare, Woods, Lorna, Antoniou, Alexandros (2023): "Pornography, the Online Safety Act 2023 and the need for further reform", *Journal of Media Law*, 15, 2, pp. 211-239

McNamara, Elizabeth, Blum Jeffrey H., Gough, Denise (1999): "Online Service Provider Liability Under the Digital Millennium Copyright Act", *The Internet & Communications Law*, 17, *Comm. Law*, pp. 5-8.

Mitsilegas, Valsamis (2009): "The third wave of third pillar law. Which direction for EU criminal justice?", *European Law Review*, 34, 4, pp. 523-560

Monti, Matteo (2019): "Privatizzazione della censura e *Internet platforms*: la libertà d'espressione e i nuovi censori dell'agorà digitale", *Rivista italiana di informatica e diritto*, 1, pp. 35-51

Moon, Laura (2019): "A New Role for Social Network Providers: NetzDG and the Communications Decency Act", *Transnational Law & Contemporary Problems*, 28, 1, pp. 623-646

Nardi, Valérie (2019): "I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider?", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 268-288

Novovic, Milos (2024): *The EU Digital Services Act (DSA): A Commentary* (Alphen Aan Den Rijn Wolters Kluwer International)

Pagella, Cecilia (2019): "La Cassazione sulla responsabilità del blogger per contenuti diffamatori (commenti) pubblicati da terzi", *Diritto penale contemporaneo*

Panattoni, Beatrice (2018): "Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di *Notice and Take Down*", *Diritto penale contemporaneo*, 5, pp. 249-263

Panattoni, Beatrice (2020): *I riflessi penali del perdurare nel tempo dei contenuti illeciti*, *Sistema penale*, 5, pp. 308-324

Perch, Laurent (2021): "The concept of chilling effect. Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU" *(*Open Society Foundation [report])

Pezzella, Vincenzo (2017): "Diffamazione sui social network: il gestore del sito deve rimuovere i contenuti?", in *Web & Tech*

Picotti, Lorenzo (1999): "Fondamento e limiti della responsabilità penale dei Service-providers in Internet", *Diritto penale e processo*, 3, pp. 379-386

Picotti, Lorenzo (2023): "Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (editors), *Cybercrime* (Milano, Wolters Kluwer), pp. 32-105

Piergallini, Carlo, *Il "penale" senza "diritto"?*, in Piergallini, Carlo, Mannozzi, Grazia, Sotis, Carlo, Perini, Chiara, Scoletta, Marco, e Consulich Federico (a cura di), *Studi in onore di Carlo Enrico Paliero*, Giuffrè Francis Lefebvre, Milano, 2022, 709-732.

Pollicino, Oreste (2014): "Tutela del Pluralismo nell'era digitale, ruolo e responsabilità degli Internet Service Provider", *Percorsi costituzionali*, 1, pp. 453-464

Polvani, Michele (1998): *La diffamazione a mezzo stampa* (Padova, CEDAM)

Raue, Benjamin, Hofmann, Franz (2024): *Digital Services Act. Article-by-Article Commentary* (London, Bloomsbury Publishing)

Reuter, Markus (2018): *NetzDG: Sieben Unternehmen haben Kontaktstellen benannt*, *www.netzpolitik.org*

Riccio, Giovanni Maria (2002): *La responsabilità civile degli* internet providers (Torino, Giappichelli)

Rinceanu, Johanna (2021): "Verso una forma di polizia privata nello spazio digitale? L'inedito ruolo dei provider nella disciplina tedesca dei social network", in M. Catenacci, Mauro, D'Ascola, Vincenzo Nico, Rampioni, Roberto (editors), *Studi in onore di Antonio Fiorella*, vol. I (Roma, RomaTre Press), pp. 333-360

Rinceanu, Johanna, e Stephenson, Randall (2023): "Digital Iatrogenesis. Towards an Integrative Model of Internet Regulation", in *eucrim*, 1, pp. 73-82

Riva, Giuseppe (2018): *Fake news. Vivere e sopravvivere in un mondo di post-verità* (Bologna, il Mulino)

Rodotà, Stefano (2010): "Una costituzione per Internet?", *Politica del diritto*, 3, pp. 337-352

Rodotà, Stefano (2012): *Il diritto di avere diritti* (Roma-Bari, Laterza)

Ryan, William (1971): *Blaming the victim* (New York, Pantheon Books)

Sabia, Rossella (2023): "L'enforcement pubblico del Digital Services Act tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni", *Media Laws – Rivista di Diritto dei Media*, 2, pp. 88-113

Sarzana di Sant'Ippolito, Fulvio. *Le sanzioni nel* Digital Markets Act, in Bolognini, Lucia, Pelino, Enrico, e Scialdone, Marco (a cura di), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Giuffrè, Milano, 2023, 385-405.

Schröder, Christian (2006): "Zur Europäisierung der Fahrlässigkeits- und Unterlassungsdelikte", *Neue Zeiftschrift für Strafrecht*, 12, pp. 669-673

Sevanian, Andrew M. (2014): "Section 230 of the Communications Decency Act: A "Good Samaritan" Law Without the Requirement of Acting as a "Good Samaritan"", in *UCLA Entertainment Law Review*, 21, 1, pp. 121-146

Sjöholm, Maria (2022): *International Human Rights Law and Protection Against Gender-Based-Harm on the Internet*, (Berlin, Springer)

Spiccia, Patricia (2013): "The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given", *Valparaiso University Law Review*, 48, 1, pp. 369-416

Spiegel, Johanna, Heymann, Britta (2020): "Ein Minenfeld für Anbieter sozialer Netzwerke. Zwischen NetzDG, Verfassungsrecht und Vertragsfreiheit", *Kommunikation & Recht*, 5, pp. 344-350

Spindler, Gerald (2017): "*Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz- europarechtswidrig?*", *Zeitschrift für Urheber- und Medienrecht*, 6, pp. 473-507

Summerer, Kolis, Matteudakis, Matteo Leonida, Caletti (2025): *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea* (Pisa, ETS Edizioni)

Thomas, Elise (2020): "Manifestos, mimetic mobilisation and the chan boards in the Christchurch shootings", in I. Kfir e J. Coyne (a cura di), *Counterterrorism Yearbook 2020* (Australian Strategic Policy Institute), pp. 19-22

Turchetti, Sara (2010): "L'art. 57 c.p. non è applicabile al direttore del periodico online", in *Diritto penale contemporaneo*

Turillazzi, Aina, Taddeo, Mariarosaria, Floridi, Luciano, Casolari, Federico (2023): "The Digital Services Act: an analysis of its ethical, legal, and social implications", *Law, Innovation and Technology*, 15, 1, pp. 83-106

Vicinanza, Anna (2025), "La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso Telegram al Digital Services Act", *Quaderni AISDUE*, 1, pp. 1-18

Wagner, Ben, Rozgonyi, Krisztina, Sekwenz, Marie-Therese, Cobbe, Jennifer, Singh, Jatinder (2020): "Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act", *FAT* '20 (Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency)*, pp. 261-271

Wagner, Gerhard (2020): "Haftung von Plattformen für Rechtsverletzungen (Teil 1)", *Gewerblicher Rechtsschutz und Urheberrecht*, 4, pp. 329-337

Williamson, Justin (1999): "Online Service Provider Copyright Liability: Is the Digital Millennium Copyright Act the Answer?", *Kentucky Law Journal*, 88, pp. 987-1017.

Wilman, Folkert (2020): *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Celtenham Edward Elgar Publishing)

Wilman, Folkert, Kaleda, Saulius Lukas, Loewenthal, Paul-John (2024): *The EU Digital Services Act. A commentary* (Oxford-New York Oxford University Press)

Woods, Lorna (2024): "Safety by Design", *Online Safety Act Network*

Zarins, Emily (2004): "Notice versus Knowledge under the Digital Millennium Copyright Act's Safe Harbors", *California Law Review*, 92, 1, pp. 257-298

Zeno-Zencovich, Vincenzo (2023): "The EU regulation of speech. A critical view", *Media Laws – Rivista di diritto dei media*, 1, pp. 11-18

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu