CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

4/2021

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 2021 - 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).

La disinformazione tra politica e diritto.
Dimensione istituzionale, strategie preventive e dinamiche punitive

La desinformación entre la política y el derecho.
Dimensión institucional, estrategias preventivas y dinámicas represivas

Disinformation Between Politics and Law.
Institutional Dimension, Preventive Strategies and Punitive Trends

Il presente contributo, qui pubblicato all'interno di una sezione speciale, costituisce la sezione giuridica della ricerca dal titolo "Come individuare e contrastare operazioni coordinate di disinformazione in Italia. Casi di studio e indicazioni di policy per istituzioni pubbliche e private", condotta nell'A.A. 2020/2021 da ricercatori dell'Università Luiss Guido Carli, della Harvard Kennedy School e della School of Information dell'Università del Michigan. La ricerca è stata realizzata con un contributo dell'Unità di Analisi, Programmazione e Documentazione Storica del Ministero italiano degli Affari Esteri e della Cooperazione Internazionale (MAECI), ai sensi dell'art. 23-bis del d.p.r. n. 18 del 5 gennaio 1967. Le riflessioni contenute in questa ricerca riflettono esclusivamente la visione degli autori e non sono necessariamente rappresentative dell'opinione del MAECI e delle altre istituzioni di ricerca coinvolte. Si ringraziano l'Unità di Analisi, Programmazione e Documentazione Storica del MAECI e gli altri Direttori della ricerca (Irene Pasquetto, Gianni Riotta e Costanza Sciubba Caniglia) per avere consentito la pubblicazione degli scritti in questa sede.

La disinformazione tra politica e diritto
La desinformación entre la política y el derecho
Disinformation Between Politics and Law

La disinformazione tra politica e diritto
La desinformación entre la política y el derecho
Disinformation Between Politics and Law

La disinformazione tra politica e diritto
La desinformación entre la política y el derecho
Disinformation Between Politics and Law

Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di *compliance*

La desinformación y la responsabilidad de las plataformas. Obligaciones y formas de compliance

Disinformation and Platforms Liability. Obligations and Compliance Requirements

Luca D'Agostino
Assegnista di ricerca in Diritto penale presso l'Università Luiss "Guido Carli"
ldagostino@luiss.it

Libertà di espressione, Reati informatici, Diritto UE, Diritto penale comparato

Libertad de expression, Delitos informáticos, Derecho UE, Diritto penale comparato

Freedom of Expression, Cybercrimes, EU Law, Comparative criminal law

Abstracts

L'esperienza maturata negli ultimi anni dimostra come le piattaforme online possano essere strumentalizzate per la diffusione di notizie false su vasta scala, in un contesto non sufficientemente regolamentato sotto il profilo degli obblighi a carico dei *provider*. Oggi gli intermediari del web (quali siti di *newsmaking*, portali di divulgazione, social network) costituiscono i maggiori canali di distribuzione delle informazioni, da cui emerge chiaramente la centralità del ruolo del *provider* nel contrasto al fenomeno della disinformazione.

Il presente lavoro si occupa anzitutto di descrivere il complesso degli obblighi che gravano sui fornitori di servizi, con particolare riguardo al controllo sui contenuti immessi online dagli utenti e alla rimozione di contenuti illeciti. Il quadro normativo – che a livello sovranazionale risulta fermo alla Direttiva 2000/31/CE – pare ormai prossimo a un profondo cambiamento, reso necessario dalla incalzante evoluzione tecnologica e dalla esigenza di una maggiore responsabilizzazione delle piattaforme digitali. In tale prospettiva, riveste particolare importanza la proposta di riforma attualmente all'esame delle istituzioni dell'Unione, il c.d. *Digital Services Act*, che contiene alcune disposizioni volte specificamente contrastare il fenomeno della disinformazione.

Nella prospettiva di una futura riforma, lo studio passa in rassegna le scelte di regolazione compiute in altri ordinamenti nazionali, tra cui la Francia e la Germania, che di recente hanno introdotto determinati obblighi a carico dei gestori delle piattaforme. In un'ottica comparatistica sono tracciate anche similitudini e differenze tra il quadro normativo eurounitario e quello statunitense. La premessa teorica sarà il fondamento per l'elaborazione di alcune indicazioni di *policy* sul contrasto alle operazioni coordinate di disinformazione, che tengano conto non solo del vigente quadro normativo, ma anche dell'esigenza di una auto-responsabilizzazione degli operatori economici di fronte ai rischi legati alla diffusione di notizie false su larga scala.

La experiencia adquirida en los últimos años muestra cómo las plataformas online pueden ser explotadas para la difusión de noticias falsas a gran escala, en un contexto que no está suficientemente regulado en cuanto a las obligaciones de los *provider*. Hoy en día, los intermediarios de la web (como los sitios de noticias, los portales de difusión o *social network*) son los principales canales de distribución de información, lo que demuestra claramente el rol central del *provider* en la lucha contra el fenómeno de la desinformación.

Este artículo describirá en primer lugar el conjunto de obligaciones que pesan sobre los proveedores de servicios, con especial atención al control de los contenidos publicados online por los usuarios y a la eliminación de los

contenidos ilegales. El cuadro normativo - que a nivel supranacional sigue basándose en la Directiva 2000/31/CE - parece estar a punto de experimentar un profundo cambio, obligado por la imperiosa evolución tecnológica y por la necesidad de una mayor responsabilidad de las plataformas digitales. En esta perspectiva, es especialmente importante la propuesta de reforma que están examinando las instituciones de la UE, el llamado *Digital Services Act*, que contiene algunas disposiciones destinadas específicamente a combatir el fenómeno de la desinformación. Con vistas a una futura reforma, el estudio examina las opciones normativas adoptadas en otros ordenamientos jurídicos nacionales, como Francia y Alemania, que han introducido recientemente determinadas obligaciones para los operadores de plataformas. En una perspectiva comparativa, también se describen las similitudes y diferencias entre los sistemas normativos de la UE y de Estados Unidos. La premisa teórica será la base para la elaboración de algunas indicaciones políticas sobre el contraste a las operaciones coordinadas de desinformación, que tengan en cuenta no sólo el vigente cuadro normativo, sino también la necesidad de una autorresponsabilidad de los operadores económicos frente a los riesgos asociados a la difusión de noticias falsas a gran escala.

The experience of recent years shows how online platforms can be exploited to spread disinformation on a large scale, in a context that is not sufficiently regulated in terms of providers' obligations. Nowadays, web intermediaries (such as news-making sites, divulgation portals, social networks) are the main channels of information distribution, which clearly shows the central role of the provider in fighting the phenomenon of disinformation.
This paper will first describe the set of obligations imposed on service providers, with particular regard to the control of the contents posted online by users and the removal of illegal ones. The regulatory framework - which at supranational level is still based on the Directive 2000/31/EC - seems to be about to change radically, as a result of the rapid technological evolution and the need for greater accountability of digital platforms. From the said perspective, the reform proposal currently under scrutiny by the EU institutions, the so-called Digital Services Act, which contains some provisions aimed specifically at combating the phenomenon of disinformation, is particularly relevant.
With a view to a future reform, the paper reviews the regulatory options adopted in other national legal systems, including France and Germany, which have recently introduced certain obligations on platform operators. From a comparative perspective, similarities and differences between the EU and US regulatory frameworks are also addressed. This theoretical premise will be the basis for the development of some policy recommendations on the fight against coordinated disinformation operations, which take into account not only the current regulatory framework, but also the need for a self-accountability of economic operators addressing risks related to the dissemination of false information on a large scale.

Sommario

I. Hosting providers e gestori di piattaforme. Inquadramento del tema

I.1. *Premessa. La disinformazione e il ruolo del provider.*

Internet rappresenta oggi il principale canale di condivisione e diffusione delle informazioni, al punto da influenzare persino il dibattito democratico su temi di elevato impatto economico, politico e sociale[1]. Nelle pagine precedenti di questo studio, si è posto in evidenza come i *social media* siano un potente strumento di manipolazione dell'informazione[2], una fonte sempre più centrale di notizie e opinioni politiche e uno strumento di interazione e organizzazione politica[3].

Le nuove tecnologie hanno infatti reso più "democratica" la produzione dei contenuti (c.d. effetto *top-down*) ma, al tempo stesso, accentrato i canali di distribuzione delle informazioni nelle mani di piattaforme di grandi dimensioni (c.d. effetto *bottom-up*).

Ciò comporta il rischio, sottolineato dalla Commissione Europea, che le nuove tecnologie possano essere impiegate per diffondere disinformazione su vasta scala[4], in un contesto non sufficientemente regolamentato sotto il profilo degli obblighi a carico delle piattaforme.

In Italia il dibattito sul ruolo del *provider* nel contrasto alla disinformazione è stato segnato dalla presentazione in Senato di un disegno di legge[5] contenente disposizioni specifiche sull'attività delle piattaforme di pubblicazione e diffusione di notizie presso il pubblico[6].In particolare la proposta legislativa prevedeva a carico dei *provider* un dovere generale di controllo sulla diffusione di notizie non attendibili o non veritiere[7], da attuare anche mediante appositi strumenti di segnalazione da parte degli utenti, nonché l'obbligo – penalmente sanzionato – di immediata rimozione di tali notizie.

Poiché i maggiori canali di informazione sono gestiti direttamente dagli intermediari del web (quali siti di *newsmaking*, portali di divulgazione, social network), emerge chiaramente la centralità del ruolo del *provider* nel contrasto alle operazioni di disinformazione. Si farà riferimento in particolare alla figura dell'*hosting provider* c.d. attivo, che rappresenta la catego-

[1] Sul punto si richiamano le considerazioni espresse nella prima parte del documento (v. *supra,* Cap. I § I)

[2] Le piattaforme digitali assumono la veste di nuovi intermediari e, progressivamente, si sono sostituite ai giornalisti nel ruolo di "custodi" della comunicazione. Cfr. Rozgonyi (2018); Pitruzzella *et al.* (2017), pp. 2 ss.

[3] Si veda sul punto il citato studio di Vargas Valdez (2018).

[4] Per approfondimenti sugli studi condotti dalla Commissione v. *supra,* § Cap. I e *infra* § II.3 sulla proposta legislativa in materia di servizi digitali.

[5] Disegno di Legge AS-2688 presentato al Senato in data 7 febbraio 2017, recante «*Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica*» (c.d. DDL Gambaro). Sui profili sanzionatori contenuti nel disegno di legge si rinvia alla successiva disamina penalistica (v. i*nfra*, Cap. III § III.1.).

[6] L'art. 3 del DDL prevedeva che all'atto dell'apertura di una piattaforma informatica destinata alla pubblicazione o diffusione di informazione presso il pubblico, non soggetta agli obblighi della normativa sulla stampa, l'amministratore della piattaforma medesima dovesse, entro quindici giorni darne apposita comunicazione, tramite posta elettronica certificata, al Tribunale territorialmente competente, trasmettendo il nome e l'URL della piattaforma elettronica e le proprie generalità personali.

[7] L'art. 7 del DDL imponeva ai gestori delle piattaforme informatiche di effettuare un «*costante monitoraggio dei contenuti diffusi attraverso le stesse, con particolare riguardo ai contenuti verso i quali gli utenti manifestano un'attenzione diffusa e improvvisa, per valutarne l'attendibilità e la veridicità*».

ria certamente prevalente nella attuale configurazione del mercato dei servizi digitali e nella moderna *sharing economy* (**§ I.2**.). Nel delineare gli obblighi a carico di quest'ultimo, sono stati ipotizzati due distinti modelli responsabilità, facenti leva sul controllo preventivo sulle informazioni immesse in rete, ovvero sui doveri di attivazione *ex post* (**§ I.3**.).

Nel fornire indicazioni di *policy* per gli operatori del settore, si dovrà dapprima descrivere il complesso degli obblighi che attualmente gravano sui fornitori di servizi, con particolare riguardo al controllo sui contenuti immessi *online* dagli utenti e alla rimozione di contenuti illeciti.

Il quadro normativo in materia di servizi della società dell'informazione è stato armonizzato a livello comunitario con l'emanazione della Direttiva 31/2000/CE, la quale prevede forti limitazioni di responsabilità per il *provider* e sancisce l'assenza di un obbligo generale di sorveglianza sui contenuti immessi in rete dai destinatari del servizio (**§ II.1**.). Tale status ammette però alcune deroghe laddove il provider, essendo a conoscenza del contenuto illecito delle informazioni divulgate o trasmesse, operi come *host* attivo secondo la giurisprudenza dalla Corte di Giustizia (**§ II.2**.). La materia risulta ormai prossima a un profondo cambiamento, reso necessario dalla incalzante evoluzione tecnologica e dalla esigenza di una maggiore responsabilizzazione delle piattaforme digitali. In tale prospettiva, sarà esaminata la proposta di riforma attualmente all'esame delle istituzioni dell'Unione, il c.d. *Digital Services Act*, che contiene alcune disposizioni volte specificamente contrastare il fenomeno della disinformazione (**§ II.3**.).

Successivamente l'attenzione sarà rivolta alla normativa italiana sul commercio elettronico (**§ III.1**.) che, nel delineare gli obblighi a carico del fornitore di servizi, si pone in linea con la direttiva sui servizi della società dell'informazione, riconoscendo uno status di tendenziale irresponsabilità del provider per omesso controllo. Ne consegue che tra gli ambiti di responsabilità del provider per condotte di disinformazione poste in essere dagli utenti della piattaforma, l'ordinamento italiano ammette soltanto un rimprovero per omessa attivazione *ex post facto*, salvi i casi di concorso nel reato eventualmente commesso (**§ III.2**.).

Nella parte conclusiva l'analisi verterà sulle scelte di regolazione compiute in altri ordinamenti nazionali, tra cui la Francia e la Germania, che di recente hanno introdotto determinati obblighi a carico dei gestori delle piattaforme. Sempre in un'ottica comparatistica, saranno delineate le differenze tra il quadro giuridico comunitario e quello statunitense (**§ III.3**.).

La trattazione si chiude con l'elaborazione di alcune indicazione di *policy* sul contrasto alle operazioni di disinformazione, che tengano conto non solo del vigente quadro normativo, ma anche dell'esigenza di una auto-responsabilizzazione degli operatori del settore **(§ III.4**.) di fronte ai rischi di manipolazione dell'informazione.

Tali indicazioni si pongono in linea con l'intento della Commissione europea[8] di prevenire la diffusione di informazioni false in rete mediante la combinazione di strumenti di *hard law* e fonti di autoregolazione privata.

I.2. *La figura dell'*hosting provider *e le problematiche legate agli* user-generated contents

Come noto, l'*Internet Service Provider* svolge un ruolo essenziale per il funzionamento della rete, poiché garantisce agli utenti servizi di connessione, memorizzazione (*hosting* di siti web, messaggistica, *cloud*), e indicizzazione di contenuti (motori di ricerca, piattaforme di streaming, *social network*).

Il vigente quadro normativo individua tre tipologie di *provider* in base alla specifica attività svolta e, soprattutto alle tempistiche di *retention* dei dati trasmessi o prodotti dagli utenti[9].

Si individua anzitutto la figura del *mere conduit* (o *access*) *provider*, che svolge una attività di mero trasporto di dati mediante la gestione del flusso di informazioni intercorrente tra terzi

[8] L'attuale proposta di regolamento sui servizi digitali (DSA) introduce meccanismi premiali e incentivi per la piattaforma di grandi dimensioni che rispetti le regole di *soft law*, prevedendo che l'adesione a un codice di condotta debba essere considerata una misura di attenuazione dei rischi adeguata (*considerandum* n. 68). Per contro, il fatto che la piattaforma online rifiuti, senza adeguate spiegazioni, l'invito della Commissione a partecipare all'applicazione di un codice di condotta potrebbe essere preso in considerazione, se del caso, nel determinare se la piattaforma online abbia violato gli obblighi stabiliti dal DSA (*amplius*, § II.3).

[9] Sul regime di responsabilità previsto per le diverse tipologie di *provider* v. *amplius*, § II.1.

al fine di consentire l'accesso alla rete e alle risorse digitali. L'attività di "semplice trasporto" include la memorizzazione automatica, intermedia e transitoria delle informazioni, ma è comunque limitata alla trasmissione dell'informazione sulla rete di comunicazione, senza eccedere il tempo ragionevolmente necessario a tale scopo.

Diversamente, il *caching provider* presta un servizio di memorizzazione automatica, intermedia e temporanea delle informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta[10]. Trattasi dunque di un anello intermedio nella catena di distribuzione dell'informazione, che permette di migliorare le prestazioni e la fruizione dei contenuti digitali.

Il fornitore di servizi di *hosting* (anche detto *content provider*) svolge invece un'attività consistente nella archiviazione di dati in transito e di memorizzazione di informazioni, al fine di renderle reperibili a utenti remoti. I file multimediali archiviati sono accessibili al solo destinatario del servizio (si pensi alle piattaforme di *cloud* personale o alle caselle di posta elettronica), a una cerchia ristretta di utenti, ovvero alla generalità degli utenti della rete.

In quest'ultimo caso il *provider* si trova in una posizione piuttosto singolare fungendo da intermediario tra il singolo utente e l'intera collettività operante in rete. Difatti, egli assicura la *retention* del dato per un periodo di tempo indeterminato, senza perdere il controllo sull'informazione né il potere di disabilitare l'accesso ai dati trasmessi dal destinatario del servizio.

Per questo motivo, l'*hosting provider* è quello più di frequente chiamato a rispondere per gli illeciti commessi dagli utenti del servizio, specie laddove il fornitore indicizzi il contenuto dei file ospitati, accrescendone la visibilità e la possibilità di fruizione sulla rete.

Ricorrendo a una classificazione ormai ricorrente in dottrina[11] e in giurisprudenza[12], il fornitore di servizi di *hosting* si dice "passivo" allorché si limiti a mettere a disposizione lo spazio virtuale, senza compiere alcun intervento sui file caricati dall'utente; per contro, si parla di *host* attivo allorché il *provider* compia attività di indicizzazione, catalogazione e selezione dei file, esprimendo in tal modo un interesse per il contenuto degli stessi.

La distinzione assume rilevanza in virtù del particolare regime di limitazione della responsabilità previsto dalla normativa sul commercio elettronico, secondo cui l'*hosting provider* non è responsabile delle informazioni memorizzate a richiesta dell'utente, a condizione che: a) non sia effettivamente a conoscenza che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso[13].

Il regime sopra descritto si riferisce a una figura di provider meramente passivo, che riceve le informazioni senza in alcun modo intervenire su di esse; egli va esente da responsabilità in quanto semplice intermediario che offre all'utenza un protocollo di comunicazione e uno spazio virtuale sui cui memorizzare i contenuti. Al contrario, l'*hoster* "attivo" elabora il patrimonio informativo che si trova sulla piattaforma[14], spesso mediante strumenti automatizzati che permettano di estrarre valore dalla massa di dati, a fini di lucro.

Date tali premesse, appare chiaro come la figura dell'*hosting provider* quale mero ricettore

[10] In informatica la *cache* è un livello di *storage* dei dati ad alta velocità che memorizza un sottoinsieme di dati, in genere di natura temporanea, per rispondere alle richieste più rapidamente di quanto non sarebbe possibile accedendo ogni volta al percorso principale in cui si trovano i dati. Il *caching* permette di riutilizzare in modo efficiente dati già recuperati o elaborati.

[11] Ampia la letteratura sul tema. Tra i contribuiti più recenti v. Resta (2004), pp. 1715 ss.; Ingrassia (2012), pp. 15 ss; Bugiolacchi (2015), pp. 1261 ss.; Accinni (2017), pp. 1 ss.; Bocchini (2017), pp. 632 ss.; Panattoni (2018), pp. 249 ss.; Nardi (2019), pp. 17 ss.

[12] Corte di Giustizia UE, 23 marzo 2010, C-236/08, C-237/09, C-238/08, *Google Inc. c. Louis Vuitton e altri*; 12 luglio 2011, C-324/09, *L'Oréal SA and others v. eBay*. Per un quadro sulla giurisprudenza della Corte di Giustizia sul tema della responsabilità del *provider* si veda il documento pubblicato da EUIPO, *IPR Enforcement case-law collection. The liability and obligations of intermediary service providers in the European Union*, agosto 2019, in euipo.europa.eu. Nei repertori nazionali *ex plurimis* si veda, per la giurisprudenza civile, App. Milano, 7 gennaio 2015, n. 29; Trib. Napoli Nord, 3 novembre 2016 n. 9799 in *Giurisprudenza Italiana*, 2017, 3, 629 ss.; Trib. Torino, 7 aprile 2017, n. 1928, in *Danno e responsabilità*, 2018, 1, 87 ss.; Trib. Roma, 15 febbraio 2019, n. 3512, in sites.les.univr.it; Cass. Civ. Sez. I, 19 marzo 2019, n.7708, in *Il Diritto industriale*, 2019, 4, 364 ss.; per la giurisprudenza penale, Trib. Milano, 12 aprile 2010, n. 1972 in *Corriere del merito*, 2010, 960 ss..; Cass. Pen., Sez. III, 29 settembre 2009, n. 49437, in *Cassazione Penale*, 2011, 1093; Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946 in *Foro Italiano*, 2017, 251 ss.

[13] Art. 14 Direttiva 31/2000/CE; art. 16 D. Lgs. 70/2003.

[14] Si richiama al riguardo la nota definizione data dal Tribunale di Milano, secondo cui l'hosting provider attivo sarebbe: «*il prestatore dei servizi della società dell'informazione il quale svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito*» (Trib. Milano, Sez. Impresa, 9 settembre 2011, n. 10893, in *Il Diritto industriale*, 2011, 6, 565 ss.).

passivo di informazioni sia un modello oramai recessivo, salvo rari casi[15]. Nella moderna *data driven economy* i fornitori di servizi assumono un ruolo sempre più attivo, che si sostanzia nel costante intervento sui contenuti pubblicati dagli utenti allo scopo di accrescerne la visibilità, incrementarne le potenzialità di interazione e di diffusione.

Se si considera l'attività delle piattaforme di più grandi dimensioni – che maggiormente sono interessate da operazioni di disinformazione su larga scala – si potrà notare come la sostenibilità economica del business si basa sul reimpiego a fini lucrativi delle informazioni ottenute mediante l'analisi dei dati e la profilazione degli utenti. Un modello che si discosta sensibilmente da quello del provider "neutrale".

Il mutamento del ruolo del *provider* comporta un cambio di prospettiva sul piano della responsabilità[16], sollevando l'interrogativo se sussista a suo carico un qualche obbligo di controllo sui contenuti pubblicati da terzi. In caso di risposta affermativa, si dovrà chiarire a che titolo i fornitori di servizi possano essere chiamati a rispondere qualora abbiano agevolato la diffusione del materiale illecito, ovvero abbiano omesso di attivarsi per disabilitarne l'accesso o impedirne la visibilità sulla piattaforma.

Tenuto conto delle finalità del presente studio, l'analisi avrà ad oggetto in particolare la responsabilità delle piattaforme per la diffusione di *user-generated contents* dalla duplice prospettiva del controllo preventivo e degli obblighi successivi di rimozione del materiale illecito.

I.3. *I paradigmi del controllo preventivo e dell'attivazione* ex post facto

Il difficile bilanciamento tra garanzie di libertà di espressione ed esigenze di controllo è una *vexata questio* che, dalla prospettiva penalistica, si compendia nella opportunità di considerare il fornitore di servizi come il titolare di una posizione di garanzia volta ad impedire la commissione di reati sulla piattaforma virtuale (art. 40, cpv, c.p.), ovvero come un soggetto gravato da un mero obbligo di attivazione successivo alla commissione di un illecito.

Quale che sia il ruolo riconosciuto al *provider*, va comunque precisato che resta fuori dal campo di indagine l'ipotesi in cui questi concorra con l'utente nella realizzazione del fatto (responsabilità per concorso commissivo) oppure commetta *manu propria* un reato (responsabilità monosoggettiva)[17]. Quindi l'attenzione sarà rivolta a due distinti paradigmi ascrittivi della responsabilità: il primo per omesso impedimento del fatto-reato dell'utente; il secondo per violazione dell'obblighi di intervento e di rimozione dei contenuti illeciti presenti sulla piattaforma.

In dottrina, chi ritiene sussistente il solo obbligo di attivazione *ex post* sostiene che, se l'ordinamento pretendesse dai *provider* di attivarsi per impedire la commissione di reati, ciò varrebbe ad introdurre meccanismi di censura preventiva tali da minare alle fondamenta la libertà di Internet. Il legislatore dovrebbe pertanto astenersi dal dettare regole *ad hoc* per prevenire la commissione di reati, poiché tale eventualità non giustifica aprioristicamente la possibilità di adottare meccanismi di limitazione preventiva[18].

A questa lettura si contrappone quella che considera la presenza di controllori nel cyberspazio funzionale alla tutela dei diritti dei singoli e, di riflesso, della effettiva libertà della rete. Il legislatore non potrebbe dimostrarsi indifferente di fronte a un fattore di rischio così allarmante, dovendo piuttosto predisporre delle misure di carattere preventivo. Difatti, la progressiva informatizzazione dei processi produttivi, informativi e decisionali renderebbe ormai evidente la necessità di controlli e di centri di imputazione di obblighi di filtraggio o rimozione[19].

[15] Vi sono alcuni servizi della società dell'informazione che ancora oggi si conformano al modello dell'*host* passivo, si pensi ad esempio al *cloud storage* o all'affitto di *server* per *hosting* di siti web. Per contro, vi sono altri servizi che progressivamente migrano verso il modello dell'*host* attivo, quali ad esempio servizi di messaggistica istantanea o di posta elettronica.

[16] Baccin (2020), p. 76.

[17] Non può certamente dubitarsi che il gestore della piattaforma debba rispondere dei reati dallo stesso realizzati o commessi in concorso con gli utenti della piattaforma. A tal riguardo la dottrina ormai da tempo si è chiesta in cosa debba sostanziarsi il contributo atipico di partecipazione dell'ISP e se la responsabilità a titolo di concorso commissivo soggiaccia alle regole comuni ovvero debba essere ricondotta a uno statuto autonomo. In argomento, Picotti (1999), pp. 379 ss.; Seminara (1997), pp. 71 ss. Sulle responsabilità connesse ad operazioni di disinformazione e sul relativo inquadramento penalistico si rinvia alla successiva sezione di questo studio (v. *infra*, Cap. III § III.1.).

[18] La tesi si fonda sul rilievo di Internet come strumento di libera manifestazione del pensiero, in grado di riunire una comunità meritevole di tutela come 'formazione sociale' (artt. 2, 21 Cost.). Non vi sarebbe alcuna necessità di controllori o garanti, essendo sufficiente il presidio apprestato dalla legge per punire il singolo che abbia abusato della propria libertà. Sul punto v. Ingrassia (2012), cit., p. 19.

[19] Si argomenta che il ruolo del diritto penale non è soltanto quello di punire le condotte antigiuridiche e colpevoli, ma altresì quello di

La prima tesi, assolutamente prevalente in dottrina e in giurisprudenza, è quella che meglio descrive l'impostazione seguita dal legislatore europeo e nazionale nel disciplinare la materia[20]. Essa propone un più equo bilanciamento tra le contrapposte esigenze [21] facendo gravare sui *provider*, al ricorrere di determinate situazioni, obblighi di attivazione e di collaborazione con l'Autorità. Secondo questa impostazione spetta al legislatore disciplinare in modo preciso e puntuale le condizioni che legittimano la limitazione delle libertà in Internet, per evitare che la garanzia della sicurezza nella rete si trasformi in uno strumento generalizzato di censura.

La previsione di un dovere generalizzato di sorveglianza comprimerebbe in modo eccessivo non soltanto la libertà dei singoli utenti, ma anche del titolare del fornitore del servizio (o di altro soggetto qualificato), che sarebbe tenuto *ad impossibilia* a dotarsi di apparati e strumenti preventivi. Soltanto in tempi recenti una parte della giurisprudenza ha mostrato aperture verso il paradigma della responsabilità per omesso impedimento di reati, nel caso della diffamazione telematica[22]. Secondo tale indirizzo il gestore di un sito web che – pur essendo a conoscenza della presenza di contenuti offensivi – non si attivi per rimuoverli può rispondere di diffamazione *ex* artt. 595, 40 cpv c.p. per aver consapevolmente mantenuto on line il post offensivo. La soluzione ha incontrato le critiche della dottrina che, correttamente, denuncia lo stravolgimento dello schema commissivo della diffamazione (da reato istantaneo in reato permanente), nonché la trasformazione di un obbligo di rimozione *ex post* in un obbligo impeditivo a carattere necessariamente preventivo[23].

Il modello dell'attivazione *ex post* trova riscontro anche nella proposta di regolamento sui servizi digitali elaborata dalla Commissione europea, in cui si ribadisce l'assenza di un dovere di sorveglianza e si afferma che gli obblighi a carico dei provider sono volti a far fronte a situazioni determinate di pericolo[24].

Ciò posto, si pone il problema di definire a quali condizioni il *provider* dovrà attivarsi, e di stabilire quale siano le conseguenze penali e amministrative per l'inosservanza dell'obbligo imposto dalla legge.

II. Unione Europea

II.1. *Il vigente quadro normativo in materia di commercio elettronico e servizi digitali*

A livello eurounitario la Direttiva 2000/31/CE, adottata per armonizzare le legislazioni degli Stati membri all'interno del mercato unico, rappresenta il referente normativo principale in materia di servizi digitali e di commercio elettronico. Tenuto conto delle marcate differenze tra le varie legislazioni nazionali, la direttiva voleva tracciare una base comune applicabile ai servizi delle società dell'informazione e, dunque, a tutte le transazioni online, in cui le negoziazioni e la conclusione degli accordi avvengono senza la presenza fisica dei contraenti.

La direttiva costituiva l'asse portante del piano d'azione della Commissione che nel di-

prevenire la commissione di reati. Quando vi è una fonte di rischio che trovi causa in un rapporto qualificato tra un soggetto e l'attività da questi esercitata, l'attribuzione di una posizione di garanzia è funzionale a una tutela effettiva dell'interesse, giuridicamente rilevante, esposto a pericolo. La garanzia dei diritti nel cyberspazio può pertanto essere assicurata soltanto attraverso l'individuazione di soggetti chiamati a 'sorvegliare' l'operato degli utenti. In tal senso, ai controllori spetta l'obbligo di attivarsi per prevenire la commissione di reati, laddove ciò risulti tecnicamente e 'umanamente' possibile.

[20] Si veda in questa sezione *infra* § II.2 e § III. 1

[21] Nella moderna società, il pluralismo democratico passa *in primis* per la libera fruizione degli strumenti informatici e telematici, che consentono al cittadino un effettivo esercizio dei propri diritti (manifestazione del pensiero, istruzione, associazionismo politico e sindacale etc.). D'altro canto, sarebbe impossibile non considerare come dette libertà possano irrimediabilmente essere compromesse in uno spazio virtuale privo di regole e di tutori dell'ordine. Si rinvia sul punto alle considerazioni espresse in apertura di questo report (v. *supra*, Cap. I § I).

[22] Si richiama in particolare Cass. Pen., Sez. V, 8 novembre 2018, n. 12546 in *Diritto Penale Contemporaneo*, 17 maggio 2019, con nota di Pagella (2019).

[23] Sul tema, anche per ulteriori riferimenti e richiami bibliografici, v. Gullo (2019), p. 3920.

[24] *«I prestatori di servizi intermediari non dovrebbero essere soggetti a un obbligo di sorveglianza di carattere generale. Ciò non riguarda gli obblighi di sorveglianza in casi specifici e, in particolare, lascia impregiudicati gli ordini emessi dalle autorità nazionali secondo le rispettive legislazioni, conformemente alle condizioni stabilite nel presente regolamento. Nessuna disposizione del presente regolamento dovrebbe essere intesa come un'imposizione di un obbligo generale di sorveglianza o di accertamento attivo dei fatti, o come un obbligo generale per i prestatori di adottare misure proattive in relazione ai contenuti illegali»* (considerandum n. 28).

cembre 1999 aveva lanciato l'iniziativa e-Europe con lo scopo di "mettere l'Europa in rete"[25], previa disciplina degli aspetti giuridici applicabili ai servizi della società dell'informazione, in particolare al commercio elettronico, nel mercato interno[26].

Quanto all'ambito soggettivo di applicazione della normativa, i "servizi della società dell'informazione" indicano tutti quei servizi prestati normalmente dietro retribuzione, a distanza, per via elettronica, mediante apparecchiature elettroniche di elaborazione e di memorizzazione di dati, su richiesta individuale del destinatario dei servizi (art. 2, lett. a). Si definisce invece "prestatore" la persona fisica o giuridica che presta un servizio della società dell'informazione (art. 2, lett. b), mentre il "destinatario del servizio" è la persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione (art. 2, lett. d).

I servizi della società dell'informazione abbracciano pertanto una vasta gamma di attività economiche svolte on-line, tra cui quella delle maggiori piattaforme, la cui attività ricade nell'alveo della normativa in esame[27].

Venendo ai principi ispiratori della disciplina, la direttiva sancisce la libertà di iniziativa economica online, senza la necessità di un'autorizzazione preventiva (art. 4), la possibilità di stipulare contratti per via elettronica, garantendo che le regole civilistiche sulla formazione del contratto non impediscano in concreto l'uso dei nuovi strumenti informatici e telematici, e non ostacolino la validità dei negozi stipulati in tal modo (art. 9). Al fine di tutelare gli interessi dei consumatori, la normativa disciplina l'accesso alle informazioni generali e contrattuali (art. 5 e 10) e l'invio delle comunicazioni commerciali da parte dei prestatori di servizi (artt. 6-8), prevedendo anche meccanismi di risoluzione stragiudiziale delle controversie.

Le disposizioni contenute nella sezione 4 (rubricata "responsabilità dei prestatori intermediari") sono quelle che maggiormente interessano l'oggetto del presente studio. Nel disciplinare la responsabilità del provider la direttiva regola, anzitutto l'attività di semplice trasporto (*mere conduit*), come il caso del fornitore del servizio di connessione ad Internet, prevedendo che il prestatore non sia responsabile delle informazioni trasmesse alla triplice condizione che egli: «*a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; e c) non selezioni né modifichi le informazioni trasmesse*» (art. 12). Per l'attività di memorizzazione intermedia e temporanea di informazioni effettuata allo scopo di rendere più efficace il suo successivo inoltro ad altri destinatari che ne hanno fatto richiesta, (*caching*), è dettata una disciplina più articolata a mente della quale il prestatore non è responsabile purché: «*a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore, d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni, e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso*» (art. 13).

Disposizioni analoghe disciplinano l'attività di memorizzazione di informazioni fornite dal destinatario del servizio (*hosting*), rispetto alla quale, come anticipato, opera la esimente di responsabilità a condizione che il prestatore: «*a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*» (art. 14).

Quale che sia la specifica attività svolta dal prestatore, viene comunque riconosciuta la possibilità per gli organi giurisdizionali e le autorità amministrative, in conformità agli ordinamenti giuridici nazionali, di esigere che il prestatore "ponga fine ad una violazione o la impedisca", nonché per gli hosting provider, di "definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime".

A chiusura del sistema è collocata la disposizione che prevede *expressis verbis* l'assenza di

[25] In quegli anni il Consiglio europeo puntava a rendere l'economia del mercato interno estremamente competitiva e dinamica, sottolineando la necessità urgente per l'Europa di sfruttare rapidamente le possibilità offerta dalla *new economy* e, in particolare, da Internet.
[26] La normativa si pone come obiettivo quello di contribuire al buon funzionamento del mercato comune garantendo la libera circolazione dei servizi della società dell'informazione tra gli Stati membri (art. 1, par. 1).
[27] Il complesso delle regole in esame è formalmente rivolto agli Stati membri – destinatari della Direttiva – che nel recepire la normativa comunitaria hanno adeguato i propri ordinamenti nazionali per renderli conformi alle disposizioni in essa contenute.

un obbligo generale di sorveglianza a carico dei prestatori dei servizi della società dell'informazione i quali, oltre a non dover vigilare preventivamente sulle informazioni che trasmettono o memorizzano, non sono neppure tenuti a "ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite" (art. 15). Gli Stati membri potranno imporre ai prestatori di servizi soltanto l'obbligo di informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati.

Il quadro fin qui delineato lascia ben intendere come il provider non vada *tout court* esente da responsabilità per il fatto illecito commesso dagli utenti della piattaforma. Si parla infatti di un regime c.d. di responsabilità limitata, che opera alle condizioni stabilite dalla direttiva, ferma restando l'assenza di un dovere generalizzato di controllo preventivo[28].

Ad ogni modo, la normativa sul commercio elettronico non prevede sanzioni a carico del fornitore di servizi in caso di omessa rimozione dei contenuti illeciti o di omessa collaborazione con l'Autorità, lasciando alla discrezionalità degli Stati membri la previsione di disposizioni sanzionatore per siffatte violazioni.

Soltanto con l'emanazione della Direttiva 2017/541/UE il legislatore dell'Unione ha imposto agli Stati membri di adottare le misure necessarie per assicurare la tempestiva rimozione dei contenuti online ospitati nel loro territorio che costituiscono una pubblica provocazione per commettere un reato di terrorismo e di adoperarsi per ottenere la rimozione di tali contenuti ospitati al di fuori del loro territorio, prevedendo altresì «*sanzioni per la violazione delle norme nazionali di attuazione della [presente] direttiva e tutti i provvedimenti necessari per la loro applicazione*»[29]. Gli obblighi di rimozione e blocco dei contenuti dovranno essere stabiliti seguendo procedure trasparenti e assicurando il rispetto del principio di proporzionalità. Tuttavia la previsione di tali obblighi «*non dovrebbe pregiudicare le disposizioni della direttiva 2000/31/CE del Parlamento europeo e del Consiglio. In particolare, non dovrebbe essere imposto ai fornitori di servizi alcun obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite*»[30]. Si ribadisce inoltre che i fornitori di servizi di *hosting* non siano responsabili a condizione che non siano effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e non siano al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione.

II.2. *La posizione della Corte di Giustizia sul requisito della* "actual knowledge"

Nella prassi applicativa il riferimento alla "conoscenza effettiva" dei contenuti trattati dall'*hosting provider* ha dato luogo a un ampio dibattito giurisprudenziale sugli elementi idonei a far ritenere "attivo" il ruolo del provider.

La Corte di Giustizia, chiamata a pronunciarsi in via pregiudiziale, ha affermato che le limitazioni di responsabilità previste dalla direttiva sul commercio elettronico riguardano i soli casi in cui l'attività del provider sia di ordine «*meramente tecnico, automatico o passivo*», rimettendo ai giudici nazionali la valutazione sulla "neutralità" dell'*hoster* in base alle specifiche circostanze del caso. Più precisamente la Corte ha affermato, in due noti casi[31], che «*in order to establish whether the liability of a referencing service provider could be limited under Article 14 of Directive 2000/31/EC, it was necessary to examine whether the role played by that service provider was neutral […] Article 14(1) of Directive 2000/31/EC was to be interpreted as applying*

[28] Nella prassi applicativa sono tuttavia emersi alcuni dubbi, poiché il legislatore non ha specificato l'ambito di operatività della limitazione di responsabilità. Ci si è chiesti, ad esempio, se la clausola possa assumere rilievo come esimente di responsabilità penale, e nello specifico escludere la sussistenza di una posizione di garanzia in capo al *provider*. La soluzione affermativa e quella più largamente prevalente in dottrina e in giurisprudenza.

[29] Cfr. art. 20 della Direttiva 2017/541/UE secondo cui le sanzioni dovranno essere effettive, proporzionate e dissuasive.

[30] In questi termini il considerandum n. 23

[31] CGUE, Corte Giust. UE, 23 marzo 2010, *Google France c. Louis Vuitto*n, C-236/08–C-238/08; C-324/09 *L'Oréal and Others*. Sul concetto di hosting provider attivo nella giurisprudenza della Corte di Giustizia si vedano anche Corte Giust. EU, 24 marzo 2014, UPC Telekabel Wien Gmbh c. Constantin Film Verleigh, C-314/12; Corte Giust. EU, 16 febbraio 2012, Sabam c. Netlog, C-360/10; Corte Giust. EU, 24 novembre 2011, Scarlet Extended c. Sabam, C-70.

to the operator of an online marketplace where that operator had not played an active role allowing it to have knowledge of or control over the data stored». La Corte richiama il quarantaduesimo considerando della direttiva 2000/31 secondo cui le deroghe alla responsabilità in essa previste riguardano esclusivamente i casi in cui il provider «*non conosce né controlla le informazioni trasmesse o memorizzate*».

Tuttavia, i principi affermati in queste pronunce non sembrano aver indirizzato univocamente i giudici nazionali a cui spetta la valutazione sulla neutralità del ruolo dei fornitori dei servizi digitali. Sicché permane il dubbio sulla estensione della limitazione di responsabilità a quei provider che utilizzano strumenti automatizzati di indicizzazione e classificazione di contenuti i quali, pur comportando un intervento sui dati e sulle informazioni trasmesse dall'utente, non sono sintomatici di una effettiva conoscenza del relativo contenuto.

II.3. *Le prospettive di regolazione futura: il* Digital Services Act

Date tali premesse sul quadro normativo eurounitario, e rinviando al paragrafo successivo l'analisi della normativa nazionale di recepimento[32], si dovrà esaminare l'attuale proposta di regolamento sui servizi digitali (c.d. *Digital Services Act*). Tale atto, oltre a prevedere obblighi più stringenti a carico delle piattaforme, si occupa anche del contrasto alla disinformazione in un'ottica preventiva, volta a responsabilizzare gli operatori del settore. Dalla proposta possono trarsi utili elementi per l'elaborazione di indicazioni di *policy* per le istituzioni pubbliche e private che intendono dotarsi di strumenti e processi volti a contenere il rischio di manipolazione dell'informazione in rete.

La proposta in materia di servizi digitali[33] trae fondamento dalla comunicazione con cui la Commissione[34] sottolineava la necessità di dare attuazione al considerando n. 40 della Direttiva 2000/31/CE per «*costruire una base adeguata per elaborare sistemi rapidi e affidabili idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime*». In quest'ottica si proponeva di valorizzare anche un coinvolgimento *ex ante* delle piattaforme online che «*dovrebbero adottare misure proattive efficaci volte a individuare e rimuovere i contenuti illegali online e non solo limitarsi a reagire alle segnalazioni ricevute*».

Per far fronte in modo razionale alle contrapposte esigenze, il DSA adotta un approccio *risk-based*, proprio anche di altri settori (si pensi alla disciplina antiriciclaggio e la normativa NIS sulla sicurezza informatica), prevedendo a carico dei provider obblighi proporzionati al loro ruolo, alle loro dimensioni e al loro impatto sull'ecosistema digitale. Si intende inoltre promuovere l'innovazione, la crescita, la competitività ed a facilitare l'espansione delle piattaforme digitali più piccole, delle PMI e delle start-up in un'ottica concorrenziale.

I fornitori interessati dalla disciplina sono i provider nel loro complesso e nelle loro diverse articolazioni di servizi *hosting* e piattaforme di *e-commerce*. Appare degno di nota il considerandum n. 13 che distingue, all'interno della categoria più ampia dei prestatori di servizi di *hosting* la sottocategoria delle piattaforme online. Viene tracciata una differenza tra piattaforme online e fornitori di servizi di hosting (tra cui certamente rientrano le prime), da cui deriva anche una diversa estensione degli obblighi. Difatti, al fine di evitare l'imposizione di obblighi eccessivamente ampi, «*i prestatori di servizi di hosting non dovrebbero tuttavia essere considerati piattaforme online quando la diffusione al pubblico è solo una funzionalità minore e meramente accessoria di un altro servizio e, per ragioni tecniche oggettive, tale funzionalità non può essere utilizzata senza tale altro servizio principale e l'integrazione di tale funzionalità non è un mezzo per eludere l'applicabilità delle norme del presente regolamento applicabili alle piattaforme online*»[35]. Si fa l'esempio del quotidiano online che ospita una sezione relativa ai commenti, accessoria al servizio principale di pubblicazione delle notizie, che non dovrebbe essere considerato una

[32] *Infra*, § III.1

[33] Commissione Europea, *Proposta di regolamento del Parlamento Europeo e del Consiglio relativa a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE,* (COM(2020) 825 final), 15 dicembre 2020

[34] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online,* COM(2017) 555 del 28 settembre 2017

[35] Il concetto di "diffusione al pubblico" utilizzato nel regolamento implica «*la messa a disposizione di informazioni a un numero potenzialmente illimitato di persone, ossia il fatto di rendere le informazioni facilmente accessibili agli utenti in generale senza che sia necessario un ulteriore intervento da parte del destinatario del servizio che le ha fornite, indipendentemente dall'accesso effettivo alle informazioni in questione da parte di tali persone*» (*considerandum* n. 14).

piattaforma online per la sola erogazione di questa funzionalità aggiuntiva.

Particolare attenzione è rivolta alle piattaforme online di grandi dimensioni (per tali intendendosi quelle che raggiungono più del 10 % dei 450 milioni di utenti in Europa) in ragione dell'elevato grado di rischio che esse presentano di diffusione di contenuti illegali. Per questo si introducono meccanismi di segnalazione dei contenuti illeciti e si pone l'obbligo per le piattaforme di collaborare con i "segnalatori attendibili", nonché nuovi obblighi circa la tracciabilità degli utenti commerciali nei mercati online al fine di identificare nel miglior modo i venditori di beni illegali o contraffatti. La proposta prevede adempimenti più puntuali a carico dei provider e disciplina le procedure di notifica e di rimozione dei contenuti illegali; istituisce obblighi di valutazione dei rischi derivanti dalla gestione dei servizi, allo scopo di sviluppare adeguati strumenti di prevenzione.

Per quel che qui interessa, nel plasmare la nozione di "contenuto illegale" si fa riferimento alle *«informazioni, indipendentemente dalla loro forma, che ai sensi del diritto applicabile sono di per sé illegali, quali l'illecito incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori illegali, o che riguardano attività illegali, quali la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il cyberstalking, la vendita di prodotti non conformi o contraffatti, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore o le attività che comportano violazioni della normativa sulla tutela dei consumatori»*. Per quanto tale nozione non richiami espressamente le c.d. *fake news*, il successivo il *considerandum* n. 63 precisa che le piattaforme online di dimensioni molto grandi dovrebbero garantire l'accesso del pubblico ai registri della pubblicità visualizzata sulle loro interfacce online per facilitare la vigilanza e la ricerca sui rischi emergenti derivanti dalla distribuzione della pubblicità online, ad esempio in relazione alle tecniche di manipolazione dell'informazione che hanno ripercussioni negative reali e prevedibili sulla salute pubblica, sulla sicurezza pubblica, sul dibattito civico, sulla partecipazione politica e sull'uguaglianza. In tal senso, sembra che la notizia falsa – pur non costituendo contenuto di per sé illecito – sia considerata dal DSA un fattore di rischio estremamente sensibile che i gestori delle piattaforme dovranno monitorare e contenere[36].

La proposta di regolamento non incide sulle disposizioni della direttiva sul commercio elettronico in materia di responsabilità del *provider*, che rappresentano ormai un fondamento dell'economia digitale[37]. Pur abrogando gli articoli da 12 a 15 della direttiva del 2000, ne riproduce pressoché testualmente il contenuto tenendo ferme le esenzioni di responsabilità per i prestatori di servizi, conformemente all'interpretazione datane dalla Corte di giustizia dell'Unione europea[38]. Si precisa inoltre che il beneficio non viene meno qualora i prestatori di servizi intermediari si attivino di propria iniziativa. Nella specie l'art. 6 DSA dispone che nessuna limitazione all'esenzione dalla responsabilità sarà prevista per il solo fatto che il *provider* si trovi a svolgere *«indagini volontarie o altre attività di propria iniziativa volte ad individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi, o di adottare le misure necessarie per conformarsi alle prescrizioni del diritto dell'Unione, comprese quelle stabilite nel presente regolamento»*. Così facendo la Commissione vorrebbe incentivare la previsione, da parte del fornitore di servizi, di procedure interne di monitoraggio e controllo senza che ciò possa in qualche modo estendere l'ambito di responsabilità.

Il DSA definisce poi i doveri di diligenza per un ambiente online trasparente e sicuro[39], tra cui spicca l'obbligo per tutti i prestatori di servizi di istituire un punto di contatto unico per agevolare la comunicazione diretta con le autorità degli Stati membri e la Commissione (art. 10); di designare un rappresentante legale nell'Unione per i prestatori che non sono stabiliti in uno Stato membro (art. 11); di prevedere nelle condizioni generali di contratto le restrizioni

[36] La definizione di "contenuto illegale" (art. 2, lett. g) della proposta) si riferisce a qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni. Ne consegue che anche una norma nazionale potrà concorrere a qualificare in determinato contenuto come illecito. Ciò assume rilevanza per la tematica della disinformazione, con riferimento a quelle norme nazionali che puniscono o qualifica espressamente come illecito la diffusione di notizie false. Per approfondimenti sulla rilevanza penale delle condotte di disinformazione, *infra* § Cap. III, § III.1.

[37] Il DSA ribadisce il divieto di imporre a tali prestatori obblighi generali di sorveglianza o di accertamento attivo dei fatti (art. 7), imponendo a provider soltanto un obbligo in relazione agli ordini delle autorità giudiziarie o amministrative nazionali di contrastare i contenuti illegali (art. 8) e di fornire informazioni (art. 9).

[38] Più precisamente il capo II regola la limitazione di responsabilità dei prestatori di servizi intermediari, distinguendo le condizioni alle quali i prestatori di servizi di semplice trasporto (*mere conduit*, art. 3), memorizzazione temporanea (*caching*, art. 4) e *hosting* (art. 5) sono esenti da responsabilità per le informazioni fornite da terzi che essi trasmettono e memorizzano.

[39] Capo III, sezionj I-V della proposta di regolamento (artt. 10.37)

sui contenuti caricati dagli utenti, con indicazione specifica delle procedure e delle misure utilizzate ai fini della moderazione dei contenuti (art. 12). Quanto agli obblighi informativi, si prevede che tutti i provider – eccetto quelli che si qualificano come microimprese o piccole imprese – debbano pubblicare almeno una volta all'anno un *report* sulle attività di moderazione dei contenuti, che includa anche il numero di segnalazioni ricevute dalle autorità e dagli utenti per ciascuna tipologia di contenuto illegale, le eventuali azioni intraprese a seguito della notifica, nonché il numero dei reclami presentati dagli utenti (art. 13).

Altri obblighi fanno capo ai soli prestatori di servizi di *hosting*, tra cui quello di predisporre sistemi e interfacce per la segnalazione di contenuti illegali (art. 14). Inoltre, qualora tali prestatori decidano di rimuovere informazioni specifiche fornite da un destinatario del servizio o disabilitare l'accesso alle stesse, il DSA impone l'obbligo di adottare un provvedimento motivato[40].

Disposizioni ulteriori si applicano ai soli *hosting provider* che operano come "piattaforme online", con la sola eccezione delle piattaforme gestite da microimprese o piccole imprese. Tali fornitori di servizi dovranno istituire un sistema che consenta di presentare per via elettronica e gratuitamente un reclamo contro le decisioni adottate dalla piattaforma nei confronti dell'utente, relativo a contenuti illegali o incompatibili con le sue condizioni generali[41]. I reclami dovranno essere decisi tempestivamente e con diligenza in modo da garantire che, qualora le ragioni addotte dall'utente siano idonee a far ritenere che il contenuto non è illegale o incompatibile con le condizioni generali del servizio, ovvero che la decisione di sospensione dell'account o del servizio è sproporzionata, la piattaforma online annulli senza indebito ritardo la decisione (art. 17). Inoltre, qualora il reclamo presentato dall'utente non abbia l'esito sperato, si prevede la possibilità di ricorrere a organismi certificati di risoluzione extragiudiziale delle controversie, costituiti presso gli Stati membri. Le piattaforme online dovranno comunque garantire che le notifiche presentate dai c.d. "segnalatori attendibili"[42] siano trattate in via prioritaria rispetto alle altre.

Con riferimento ai contenuti illeciti, l'art. 20 del DSA dispone che le piattaforme siano tenute a sospendere per un periodo di tempo ragionevole l'accesso al servizio per coloro che abbiano condiviso "con frequenza" contenuti manifestamente illegali. Analogamente, dovranno impedire la presentazione di segnalazioni da parte degli utenti che "con frequenza" hanno presentato notifiche o reclami manifestamente infondati[43].

Qualora l'attività compiuta o il materiale trasmesso presenti gli estremi di un reato grave, che comporta una minaccia per la vita o la sicurezza delle persone[44],la piattaforma online dovrà informare senza indugio le autorità giudiziarie dello Stato membro o degli Stati membri interessati[45], fornendo tutte le informazioni pertinenti disponibili.

La proposta di regolamento prevede anche obblighi di tracciabilità per quelle piattaforme

[40] La motivazione dovrà contiene almeno le informazioni seguenti: a) una precisazione volta a confermare se la decisione comporti la rimozione delle informazioni o la disabilitazione dell'accesso alle stesse e, ove opportuno, la portata territoriale della disabilitazione dell'accesso; b) i fatti e le circostanze su cui si basa la decisione adottata; c) ove opportuno, informazioni sugli strumenti automatizzati usati per adottare la decisione; d) se la decisione riguarda presunti contenuti illegali, un riferimento alla base giuridica invocata e una spiegazione delle ragioni per cui l'informazione è considerata contenuto illegale in applicazione di tale base giuridica; e) se la decisione si basa sulla presunta incompatibilità delle informazioni con le condizioni generali del prestatore, un riferimento alla clausola contrattuale invocata e una spiegazione delle ragioni per cui le informazioni sono ritenute incompatibili con tale clausola; f) informazioni sui mezzi di ricorso a disposizione del destinatario del servizio in relazione alla decisione, in particolare attraverso i meccanismi interni di gestione dei reclami, la risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria.

[41] Trattasi delle decisioni relative alla rimozione dei contenuti e quelle di sospensione o cessazione del servizio o dell'account registrato dall'utente.

[42] La qualifica di segnalatore attendibile verrà riconosciuta dal coordinatore dei servizi digitali dello Stato membro, a condizione che quest'ultimo abbia dimostrato di soddisfare alcuni requisiti tra cui: il possesso di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; la rappresentanza degli interessi collettivi degli utenti.

[43] I gestori delle piattaforme dovranno valutare, caso per caso e in modo tempestivo, diligente e obiettivo, le circostanze del caso valutando in particolare: a) il numero, in termini assoluti, di contenuti manifestamente illegali o di notifiche o reclami manifestamente infondati presentati durante l'anno precedente; b) la relativa proporzione rispetto al numero totale di informazioni fornite o di notifiche presentate nell'anno precedente; c) la gravità degli abusi e delle relative conseguenze; d) l'intenzione del destinatario, della persona, dell'ente o del reclamante.

[44] Più precisamente l'art. 21 DSA si riferisce alla «*conoscenza di informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato grave che comporta una minaccia per la vita o la sicurezza delle persone*». In questi casi la piattaforma online dovrà informare senza indugio le autorità giudiziarie o di contrasto dello Stato membro o degli Stati membri interessati in merito ai propri sospetti.

[45] Si considera Stato membro interessato quello in cui si sospetta che sia stato commesso, si stia commettendo o sarà probabilmente commesso il reato, o lo Stato membro in cui risiede o si trova il presunto autore del reato oppure lo Stato membro in cui risiede o si trova la vittima del presunto reato. Se la piattaforma non è in grado di individuare con ragionevole certezza lo Stato membro interessato, dovrà informare Europol.

online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali (es. piattaforme di intermediazione B2C). Questi ultimi potranno accedere ai servizi online soltanto previa identificazione da parte della piattaforma[46], la quale dovrà compiere "sforzi ragionevoli" per stabilire se le informazioni fornite dall'operatore business siano attendibili, verificandone se del caso la rispondenza con quanto presente in banche dati ufficiali oppure chiedendo direttamente all'operatore di fornire documenti giustificativi provenienti da fonti affidabili.

Altri adempimenti riguardano le sole "piattaforme online di dimensioni molto grandi" che prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni. Queste sono tenute ad individuare, analizzare e valutare eventuali rischi sistemici significativi derivanti dal funzionamento e dall'uso dei loro servizi, tra cui in particolare quelli connessi alla diffusione di contenuti illegali e alla «*manipolazione intenzionale del servizio, anche mediante un uso non autentico o uno sfruttamento automatizzato del servizio, con ripercussioni negative, effettive o prevedibili, sulla tutela della salute pubblica, dei minori, del dibattito civico, o con effetti reali o prevedibili sui processi elettorali e sulla sicurezza pubblica*» (art. 26, par. 1, lett. c)[47].

Quanto alla gestione dei rischi, il DSA prevede che le piattaforme *de quibus* debbano adottare, sulla base degli esiti della valutazione, misure di attenuazione ragionevoli, proporzionate ed efficaci, tra cui ad esempio l'adeguamento dei sistemi di moderazione dei contenuti e dei processi decisionali interni, la modifica del funzionamento del *software* o delle condizioni generali del servizio, il rafforzamento dei processi di vigilanza sulle loro attività, la cooperazione con i segnalatori attendibili o con altre piattaforme online attraverso i codici di condotta e i protocolli. Le piattaforme di grandi dimensioni devono inoltre sottoporsi a audit esterni e indipendenti aventi ad oggetto il rispetto degli obblighi previsti dal capo III del regolamento e a quelli fissati nei codici di condotta.

Vi sono poi obblighi informativi qualificati per le piattaforme online che si avvalgono di algoritmi di raccomandazione e che visualizzano pubblicità sulle loro interfacce. Le prime sono tenute a specificare nelle loro condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati da tali algoritmi; le seconde dovranno compilare e rendere disponibile per almeno un anno mediante API un registro contenente alcune informazioni rilevanti[48]

La sezione fissa inoltre le condizioni alle quali le piattaforme online di dimensioni molto grandi forniscono l'accesso ai dati al coordinatore dei servizi digitali del luogo di stabilimento o alla Commissione; stabilisce l'obbligo di nominare uno o più responsabili della conformità per garantire il rispetto degli obblighi sanciti dal regolamento, nonché ulteriori obblighi specifici di comunicazione trasparente (artt. 31 ss.).

La proposta di regolamento incoraggia l'adozione di fonti autoregolamentari per far fronte al rischio di diffusione di contenuti illegali e di scarsa trasparenza e controllo sulle pubblicità. Al riguardo la Commissione potrà invitare le piattaforme online e i *provider* di servizi a partecipare all'elaborazione dei codici di condotta oppure a aderire a protocolli di crisi, anche stabilendo impegni ad adottare misure specifiche di attenuazione dei rischi nonché un quadro di comunicazione periodica sulle misure adottate e sui relativi risultati.

La parte finale della proposta contiene le disposizioni sui controlli da parte degli Stati membri[49], particolarmente stringenti per le piattaforme online di dimensioni molto grandi,

[46] Cfr. Art. 22 DSA. Nella specie, la piattaforma dovrà ottenere le seguenti informazioni: nome, l'indirizzo, il numero di telefono e l'indirizzo di posta elettronica dell'operatore commerciale; una copia del documento di identificazione dell'operatore commerciale o qualsiasi altra identificazione elettronica; le coordinate bancarie dell'operatore commerciale, se quest'ultimo è una persona fisica; qualora l'operatore commerciale sia iscritto in un registro delle imprese o analogo registro pubblico, il registro presso il quale è iscritto ed il relativo numero di iscrizione o mezzo equivalente di identificazione contemplato in detto registro; un'autocertificazione da parte dell'operatore commerciale, con cui quest'ultimo si impegna a offrire solo prodotti o servizi conformi alle norme applicabili del diritto dell'Unione.

[47] Nell'attività di valutazione dei rischi, le piattaforme online di grandi dimensioni devono tener conto del modo in cui i loro sistemi di moderazione dei contenuti, di raccomandazione e di selezione e visualizzazione della pubblicità possano influenzare la diffusione di contenuti illegali e di informazioni incompatibili con le loro condizioni generali (art. 26, par. 2 della proposta). Si introduce così una sorte di onere qualificato di *risk-assessment* per gli operatori che si avvalgono di strumenti di indicizzazione dei contenuti e profilazione degli utenti.

[48] Nel registro previsto dall'art. 30 DSA dovranno figurare le seguenti informazioni: a) il contenuto della pubblicità; b) la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità; c) il periodo durante il quale è stata visualizzata la pubblicità; d) un'indicazione volta a precisare se la pubblicità fosse destinata ad essere mostrata a uno o più gruppi specifici di destinatari del servizio e, in tal caso, i principali parametri utilizzati a tal fine; e) il numero totale di destinatari del servizio raggiunti e, ove opportuno, i dati aggregati relativi al gruppo o ai gruppi di destinatari ai quali la pubblicità era specificamente destinata.

[49] Gli Stati dovranno nominare una autorità competente e i coordinatori dei servizi digitali, con poteri di ispezione, verifica, inibitoria e

per le quali è prevista una vigilanza rafforzata nel caso in cui tali piattaforme violino le disposizioni del regolamento.

In ogni caso, gli Stati membri dovranno introdurre sanzioni effettive, proporzionate e dissuasive per le violazioni commesse dai prestatori di servizi. L'importo massimo delle sanzioni non dovrà eccedere il 6% del fatturato annuo; mentre per le informazioni inesatte, incomplete o fuorvianti, o in caso di mancata risposta il limite massimo è fissato all'1% del fatturato annuo del *provider* interessato. Nel caso in cui questi non ponga fine alle violazioni commesse, potrà essere applicata una penalità di mora non eccedente il 5 % del fatturato giornaliero medio.

In alcuni casi il potere di intervento spetta alla Commissione[50], la quale disporrà del potere sanzionatorio per le violazioni del regolamento commesse dalle piattaforme online di dimensioni molto grandi. Nel dettaglio, l'art. 59 commina sanzioni pecuniarie non superiori al 6 % del fatturato totale relativo all'esercizio precedente, qualora constati che la piattaforma, intenzionalmente o per negligenza, abbia violato le pertinenti disposizioni del presente regolamento o le decisioni adottate dalla Commissione[51].

L'impianto normativo fin qui esaminato darà luogo a un radicale mutamento di prospettiva nella lotta alla disinformazione, contribuendo a responsabilizzare gli operatori che diffondono contenuti in rete. Va riconosciuta particolare rilevanza agli obblighi gravanti sulle piattaforme di grandi dimensioni[52], per le quali il rischio di manipolazione dell'informazione sembra essere elevato a "rischio sistemico" da prevenire.

In questa direzione le fonti di *soft law* assumeranno una importanza crescente, tanto che le norme sui codici di condotta previste nel DSA *«potrebbero in particolare servire da base per un codice di buone pratiche sulla disinformazione rivisto e rafforzato, basato sugli orientamenti della Commissione, che potrebbe integrare tali norme».* Sul punto il considerandum n. 68 fa riferimento agli accordi di autoregolamentazione e di coregolamentazione che dovranno *«prendere in considerazione [..] gli eventuali effetti negativi dei rischi sistemici sulla società e sulla democrazia, quali la disinformazione o le attività di manipolazione e abuso»*. Vi è peraltro un riferimento espresso alle "operazioni coordinate" volte ad amplificare informazioni attraverso l'utilizzo di bot o di account falsi per la creazione di informazioni false e notizie fuorvianti, anche a scopo di lucro. In relazione a tali ambiti lo stesso considerandum n. 68 prevede che *«l'adesione a un determinato codice di condotta e il suo rispetto da parte di una piattaforma online di dimensioni molto grandi possono essere ritenuti una misura di attenuazione dei rischi adeguata»,* mentre il fatto che una piattaforma online rifiuti, senza adeguate spiegazioni, l'invito della Commissione a partecipare all'applicazione di un tale codice di condotta *«potrebbe essere preso in considerazione, se del caso, nel determinare se la piattaforma online abbia violato gli obblighi stabiliti dal presente regolamento»*.

In sostanza, le fonti di *self-regulation* assumeranno una portata quasi vincolante, producendo da un lato l'effetto di limitare la responsabilità per la piattaforma che le abbia osservate, dall'altro l'esposizione a possibili sanzioni per il *provider* che ad esse non si sia conformato.

Sulla stessa scia si collocano i protocolli di crisi, che la Commissione potrà elaborare per far fronte a circostanze straordinarie quali terremoti, gli uragani, pandemie, guerre e attentati terroristici. In simili circostanze le piattaforme online sono esposte maggiormente al rischio di un utilizzo improprio e alla rapida diffusione di contenuti illegali o informazioni false; pertanto dovrebbero essere incoraggiate a elaborare e applicare protocolli di crisi specifici per un periodo di tempo limitato[53].

imposizione di sanzioni nei confronti dei soggetti obbligati (capo IV, artt. 38 ss.). A livello europeo di prevede invece la costituzione di un Comitato per i servizi digitali, con compiti di proposta, consultazione e impulso nei confronti dei coordinatori dei servizi digitali degli Stati membri (art. 47 ss.).

[50] In tali casi la Commissione potrà svolgere indagini, anche tramite richieste di informazioni, audizioni e ispezioni *in loco*, adottare misure provvisorie, rendere vincolanti gli impegni delle piattaforme, e monitorare la conformità a legge della condotta delle stesse (artt. 51 ss.).

[51] La proposta di regolamento fissa anche le garanzie procedurali dinanzi alla Commissione, in particolare il diritto di essere ascoltati e di accesso al fascicolo, e la pubblicazione delle decisioni (art. 63 ss.).

[52] Capo III Sezione IV DSA (artt. 25 ss.)

[53] Cfr. Considerandum n. 71 DSA

III. Ordinamenti nazionali e misure di contrasto alla disinformazione

III.1. *La disciplina italiana sulla responsabilità del* provider

Il D. Lgs. 9 aprile 2003, n. 70 (c.d. Codice del commercio elettronico), adottato in attuazione della direttiva 2000/31/CE, ha disciplinato l'attività dei prestatori di servizi in termini pressoché analoghi alla normativa comunitaria.

Avuto riguardo al tema della responsabilità del *provider*, il Codice riprende la distinzione in tre tipologie di prestatori di servizi. Per l'attività consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione (c.d. *mere conduit*), il prestatore non è considerato responsabile delle informazioni trasmesse a condizione che: «*a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; c) non selezioni né modifichi le informazioni trasmesse*» (art. 14); quanto alla memorizzazione automatica, intermedia e temporanea delle informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta (c.d. *caching*), il prestatore è esente da responsabilità purché: «*a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione*» (art. 15); parimenti, nella prestazione di un servizio di memorizzazione di informazioni fornite da un destinatario del servizio (c.d. *hosting*), il provider non è responsabile delle informazioni memorizzate o trasmesse quando: «*a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*» (art. 16).

Con riferimento a ciascuna delle tre tipologie di provider il Codice del commercio elettronico prevede (artt. 14, comma 3, 15, comma 2, 16, comma 3) che «*L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività, impedisca o ponga fine alle violazioni commesse*».

Il successivo art. 17, rubricato "Assenza dell'obbligo generale di sorveglianza" dispone che «*Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite*».

Il principio è però temperato dalla previsione, al secondo comma, di un dovere di collaborazione con la pubblica autorità. Il prestatore è infatti tenuto: (i) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; (ii) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

Il concetto di "effettiva conoscenza" ha sollevato diverse problematiche applicative, tanto in sede civile quanto in sede penale[54]. In particolare, affinché venga meno la limitazione di responsabilità è necessario che l'*hosting provider* abbia preso conoscenza del contenuto illecito "su comunicazione delle autorità competenti".

Da un punto di vista letterale sembrerebbe quindi che l'obbligo di rimozione a carico del provider richieda la preventiva comunicazione da parte dell'Autorità della presenza di un

[54] Per riferimenti, *supra* § I.2

contenuto illecito, mentre ogni altra segnalazione dia luogo a una mera facoltà di intervento. L'interpretazione testuale della norma non è condivisa da quella parte della giurisprudenza[55] che ritiene sussistente l'obbligo di rimozione anche in caso di conoscenza acquisita *aliunde*, senza che sia necessario un ordine specifico dell'autorità. Tale soluzione è argomentata facendo leva, anzitutto, sul regime di esonero dalla responsabilità in due fattispecie distinte (lett. a e b) all'interno dell'art. 16 laddove, se si fosse voluto perimetrare l'obbligo di rimozione al solo ordine delle autorità competenti, non avrebbe avuto senso prevedere un'ipotesi autonoma connessa, semplicemente, alla non effettiva "conoscenza del fatto che l'attività o l'informazione è illecita".

Sul piano dell'interpretazione sistematica, si valorizza il contenuto dell'art. 17 nel senso che, se l'obbligo di rimozione derivasse solo da un precedente ordine dell'autorità, il legislatore non avrebbe avuto motivo di sancire l'assenza di un generale obbligo di sorveglianza giacché, in ogni caso, il *provider* non sarebbe tenuto ad attivarsi spontaneamente o volontariamente per impedire l'attività e la diffusione dell'informazione illecita. Inoltre, l'art. 17, nella parte in cui prevede l'assenza di un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite, si presta a una lettura "in positivo", nel senso che un simile obbligo potrà ben sussistere a fronte di specifiche denunce o segnalazioni provenienti da terzi.

III.2. *La disinformazione come illecito. Rimozione di contenuti, obbligo di attivazione e responsabilità del* provider

Volendo ora compendiare il tema della responsabilità del *provider* in relazione alle operazioni coordinate di disinformazione poste in essere da terzi destinatari del servizio (utenti di social network, terze parti commerciali, licenziatari del software etc.), deve in primo luogo chiarirsi se, ed eventualmente a che titolo, una condotta di manipolazione dell'informazione può essere considerata "attività illecita", e se i *files* ad essa relativi siano a loro volta una "informazione" o un "contenuto" illeciti.

La risposta a tale interrogativo richiede la previa disamina della complessa questione concernente la rilevanza penale della diffusione di notizie false, oggetto di approfondimento in altra sezione del presente studio[56]. In tal senso, andrà certamente affermata la natura illecita delle "attività" (e, dunque, delle "informazioni" che costituiscono l'oggetto materiale della condotta o il mezzo esecutivo del reato) che integrano un fatto colpevole e punibile ai sensi delle vigenti leggi penali. A queste si aggiungono anche quelle attività e/o informazioni contrarie a una norma imperativa di legge o all'ordine pubblico, indipendentemente dalla rilevanza penale della condotta e/o dall'applicabilità di una specifica sanzione amministrativa.

Da ultimo, l'attività o l'informazione dovrebbe considerarsi illecita tutte le volte in cui cagioni dolosamente o colposamente un danno ingiusto a terzi (ai sensi della norma generale di cui all'art. 2043 c.c.). In sostanza, per quel che concerne la responsabilità del *provider* per omessa attivazione/rimozione, l'operazione di disinformazione costituirà una "attività" illecita quando contravviene a una norma imperativa di legge quale che sia la natura della sanzione (penale, civile amministrativa).

Ciò posto, alla luce di quanto osservato in precedenza, può ritenersi che nell'ordinamento italiano, benché non vi sia alcun obbligo di controllo preventivo dei contenuti trasmessi dall'utente, né una posizione di garanzia penalistica, sussiste un obbligo successivo di attivazione a carico del prestatore di servizi.

In mancanza di una disciplina *ad hoc* relativa alle operazioni di disinformazione, il *provider* risponderà per omessa attivazione/rimozione in base alle norme comuni. In sede civile l'*hosting provider* potrà rispondere del danno causato agli utenti o a terzi *ex* art. 2043 c.c. qualora non abbia ottemperato a una richiesta di rimozione dei contenuti illeciti proveniente dall'autorità, sia essa giurisdizionale o amministrativa, o anche dal semplice utente titolare del diritto leso.

Su diverse basi va invece ricostruita la responsabilità penale del provider per omessa attivazione successiva alla notizia della commissione dell'illecito, che è affidata alle disposizioni di comuni del codice penale. In caso di omessa denuncia potrebbero ricorrere gli estremi del

[55] Si richiama la già citata sentenza del Trib. Napoli Nord, 3 novembre 2016 n. 9799
[56] Si rinvia in particolare alla sezione relativa alle conseguenze penali connesse alle operazioni di disinformazione (*infra,* Cap. III, § III.1.).

favoreggiamento personale (art. 378 c.p.), che la giurisprudenza ritiene configurabile anche mediante un *non facere* antidoveroso[57]. La violazione dell'obbligo di rimozione del materiale illecito o di inibizione all'accesso su richiesta dell'autorità competente potrebbe integrare il delitto di mancata esecuzione dolosa di un provvedimento del giudice (art. 388 c.p.) soltanto se il fornitore del servizio compia atti fraudolenti diretti ad eludere i predetti obblighi e si tratti di un provvedimento giurisdizionale. Diversamente, il fatto sarà inquadrato nella contravvenzione di cui all'art. 650 c.p. che punisce l'inosservanza di provvedimenti dell'autorità emessi per ragioni di giustizia o di sicurezza pubblica.

La normativa italiana sul commercio elettronico non prevede alcuna sanzione amministrativa per la violazione degli obblighi di segnalazione o di collaborazione con l'autorità, né per l'omessa tempestiva rimozione dei contenuti illeciti. Invero, l'art. 21 D. Lgs. 70/2003 punisce con sanzione pecuniaria soltanto la violazione di alcune norme di disciplina, tra cui quelle relative agli obblighi di informazione per la comunicazione commerciale o agli oneri informativi in caso di conclusione dei contratti a distanza.

Soltanto in alcuni casi previsti da leggi speciali il dovere di collaborazione con l'Autorità è presidiato da sanzioni di carattere amministrativo (si veda, ad esempio l'art. 14-*ter,* comma 3, l. 269/1998 sul contrasto alla pedopornografia[58]). Vi è poi la particolare ipotesi disciplinata dalla legge 29 maggio 2017 n. 71, che ha introdotto disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del "cyberbullismo". La normativa riconosce la possibilità per il minore ultraquattordicenne vittima di uno degli illeciti riconducibili al cyberbullismo, di inoltrare al gestore del sito internet un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore stesso diffuso in Internet, senza tuttavia prevedere alcuna sanzione amministrativa in caso di omessa attivazione del gestore del sito[59].

Quanto alle prospettive *de lege ferenda*, occorre mettere in evidenza che l'intervento del legislatore nell'ambito in esame postula un delicato bilanciamento tra diritti fondamentali. Al riguardo la Corte EDU ha di recente affermato che rientra nella discrezionalità del legislatore nazionale, nel bilanciamento tra libertà di manifestazione del pensiero e tutela dei diritti della personalità, delineare ipotesi di responsabilità del fornitore di servizi per inottemperanza dell'obbligo di rimozione dei contenuti illeciti, senza che ciò possa costituire violazione dell'art. 10 CEDU[60].

III.3. *La responsabilità del provider in alcuni ordinamenti stranieri. Spunti comparatistici con Francia, Germania e Stati Uniti*

Per concludere l'analisi circa il ruolo e le responsabilità del *provider* nel contrasto alla disinformazione, appare utile guardare – sia pur sinteticamente – alle scelte di regolazione

[57] Cfr. Cass. Pen,, Sez. VI, 18 maggio 2004, n. 31346, secondo cui la condotta di aiuto di cui all'art. 378 c.p. si riferisce a «*ogni condotta, anche omissiva – come il silenzio, la reticenza, il rifiuto di fornire notizie – avente ad oggetto il risultato di consentire all'autore di un delitto di eludere le investigazioni dell'autorità*». La giurisprudenza successiva ha tuttavia precisato che l'omissione assume rilevanza solo ove l'autore del reato abbia un dovere di cooperazione derivante da una norma di legge che gli imponga un certo facere (Cfr. Cass. Pen., Sez. VI, 8 febbraio 2006, n. 32573). Tale condizione sembrerebbe soddisfatta con riferimento al ruolo del provider, dacché le norme del codice del commercio elettronico impongono chiari obblighi di attivazione *ex post*.

[58] Rimane peraltro aperta la questione circa la rilevanza penale dell'eventuale inosservanza degli obblighi e il rapporto tra il reato e gli illeciti amministrativi. Una parte della dottrina (Ingrassia (2012), cit., p. 63) ritiene che, laddove l'inosservanza costituisca illecito amministrativo, il principio di specialità previsto dall'art. 9 della legge 689/1981 farebbe venir meno la possibilità di applicare l'art. 650 c.p.

[59] Ai sensi dell'art. 1, comma 3, L. 71/2017 per «*gestore del sito internet» si intende il prestatore di servizi della società dell'informazione, diverso da quelli di cui agli articoli 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, che, sulla rete internet, cura la gestione dei contenuti di un sito*». La relativa previsione non si applica dunque ai *provider* nel senso fin qui esaminato.

[60] CEDU, Grande Camera, Delphi AS c/ Estonia 16 giugno 2015, ric. 64569/09: «*Where third-party user comments are in the form of hate speech and direct threats to the physical integrity of individuals, as understood in the Court's case-law […], the Court consider that the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties (§ 159)*». La Corte di Strasburgo considera l'attività del *provider* essenziale per l'esercizio della libertà di espressione (art. 10 della CEDU), ma afferma che essa non può svolgersi in contrasto con gli altri diritti riconosciuti dalla Convenzione. Pur essendo innegabile che gli Stati hanno un ampio margine di apprezzamento quando vengono in rilievo due diritti in gioco (libertà di espressione da un lato e diritto della persona dall'altro), essi non dovrebbero accordare protezione ai commenti diffamatori o di incitamento all'odio e, anzi, di prevenirne la diffusione. Il principio di diritto appare estensibile anche alla previsione di ipotesi di responsabilità del *provider* per inottemperanza all'obbligo di rimozione di contenuti falsi o fuorvianti, che chiama in causa il bilanciamento tra la libera manifestazione del pensiero e gli altri diritti fondamentali potenzialmente esposti a pericolo a causa della disinformazione (es. diritto alla salute, libera espressione del voto in occasione di consultazioni elettorali, diritto alla sicurezza etc.).

compiute in alcuni ordinamenti stranieri.

Tra le esperienze nazionali più paradigmatiche[61] figura, indubbiamente, quella tedesca a seguito dell'emanazione della Legge per migliorare la tutela dei diritti sui social network (*Netzwerkdurchsetzungsgesetz – NetzDG*). La novella ha introdotto meccanismi di *notice and take down* a carico dei provider, facendo leva sulla responsabilità amministrativa per omessa attivazione successiva alla commissione di un illecito[62]. Nel dettaglio il provvedimento prevede tre principali obblighi a carico del fornitore di servizi di *social network*[63], stabilendo le relative sanzioni amministrative in caso di mancata osservanza. I principali obblighi – che in parte si ritrovano nella recente proposta di regolamento europeo sui servizi digitali – riguardano l'elaborazione di una relazione semestrale sul trattamento dei reclami concernenti i contenuti illegali[64], la rimozione o il blocco di tali contenuti entro un arco temporale ristretto, e la nomina di responsabili del servizio sul territorio nazionale.

I destinatari della disciplina sono tenuti a dotarsi di procedure efficaci e trasparenti per la ricezione e la trattazione delle denunce relative a contenuti illeciti. Nel dettaglio, il *provider* deve assicurare l'immediata presa in carico delle segnalazioni, la verifica dell'illiceità del contenuto e la rimozione entro 24 ore dalla denuncia, salvo che abbia stipulato un diverso accordo con le Autorità competenti[65].

L'ordinamento francese si caratterizza per aver disciplinato in modo specifico il contrasto alla disinformazione in rete, facendo leva sul ruolo delle piattaforme di condivisione dati. Nel dettaglio, la *Loi n° 2018-1202 relative à la lutte contre la manipulation de l'information* prevede misure di contrasto alla disinformazione, con particolare riferimento alla diffusione di notizie false in grado di incidere sui processi elettorali. Il titolo III legge introduce obblighi specifici a carico dei gestori delle piattaforme al fine di limitare la diffusione di informazioni false suscettibili di turbare l'ordine pubblico o di alterare gli esiti di una consultazione elettorale[66]. I destinatari della disciplina devono predisporre un sistema di segnalazione delle violazioni da parte degli utenti e garantire informazioni attendibili sulla natura, sull'origine e sulle modalità di distribuzione dei contenuti.

Vieppiù, i gestori delle piattaforme che si servono di algoritmi per raccomandare o classificare informazioni relative a un dibattito di interesse generale dovranno pubblicare, in formato libero e aperto, statistiche aggregate circa il loro funzionamento (art. 14). Il legislatore francese promuove anche la conclusione di accordi di cooperazione tra i professionisti dell'informazione (tra cui piattaforme online, agenzie di stampa, media audiotelevisivi etc) per combattere la diffusione di informazioni false (art. 15).

La novella ha inoltre modificato il Codice Elettorale stabilendo che nei tre mesi antecedenti una consultazione elettorale, laddove siano diffuse informazioni false o fuorvianti attraverso un servizio di comunicazione pubblica online, suscettibili di alterare lo svolgimento delle prossime, il Tribunale su richiesta del Pubblico Ministero, di un candidato o di gruppo politico, o di chiunque abbia interesse possa imporre tutte le misure proporzionate e necessarie per far cessare tale diffusione[67].

[61] Alcuni profili comparatistici sono già stati trattati nella sezione precedente di questo studio (*supra,* Cap. I, § III) Pertanto in questa sede ci occuperemo dei soli obblighi di cooperazione gravanti sulle piattaforme secondo la legislazione straniera.

[62] Si veda su tema l'approfondimento n. 188/2017 intitolato *"La legge tedesca per il miglioramento dell'applicazione delle norme sulle reti sociali"*, pubblicata dal Servizio Studi del Senato della Repubblica, disponibile su senato.it. Le disposizioni di nuovo conio si rivolgono, in particolare, ai *social media* destinatari di sanzioni pecuniarie da 500 mila fino a 50 milioni di euro per l'omessa rimozione dei contenuti "palesemente illeciti" entro 24 ore dalla segnalazione.

[63] Nello specifico, ai sensi dell'art. 1 (§ 1 *Anwendungsbereich*) la disciplina si applica ai *provider* di piattaforme progettate per condividere contenuti tra utenti o per rendere pubblici tali contenuti (*social networks*); per contro non si applica ai giornali *online* e ai gestori di siti internet editoriali. Sono inoltre esonerati i provider con meno di 2 milioni di utenti registrati sul territorio tedesco.

[64] L'obbligo di segnalazione fa capo ai fornitori di reti sociali che ricevano oltre 100 reclami annui in ordine a contenuti illegali pubblicati sulle proprie piattaforme. Essi dovranno produrre una relazione semestrale sulla gestione di tali reclami, da pubblicarsi sulla Gazzetta federale e sul proprio sito *web* entro il mese successivo alla scadenza del semestre di riferimento. Le relazioni pubblicate sul sito *web* del *provider* dovranno essere facilmente riconoscibili, direttamente accessibili e permanentemente disponibili (Art. 1, § 2 *Berichtspflicht*).

[65] In ogni caso è fissato il termine massimo di 7 giorni dalla denuncia per rimuovere i contenuti, salvo ce la valutazione sull'illiceità dell'informazione dipenda da falsa accusa o da altre circostanze fattuali; in tali casi, il provider può consentire all'utente di rispondere al reclamo prima della decisione. Il termine è elevato a 7 giorni anche nei casi di contestazione o rimessione della decisione ad un organo di autoregolamentazione.

[66] I gestori delle piattaforme sono tenuti, *ex* art. 11 della legge, ad attuare misure complementari su: la trasparenza degli algoritmi utilizzati; la promozione dei contenuti da parte delle imprese e delle agenzie di stampa e dei servizi di comunicazione audiovisiva; la lotta contro gli account che diffondono massicciamente informazioni false; l'identità della persona fisiche o giuridiche che acquistano a pagamento la promozione di contenuti informativi relativi a un dibattito di interesse generale.

[67] Art. 1 della Loi 2018-1202, che ha introdotto la sezione L. 163-2 nel capitolo VI del Codice Elettorale.

La normativa non prevede sanzioni *ad hoc* per la violazione degli obblighi in essa contenuti, fatta eccezione per alcuni particolari violazioni[68] che non solo costuiscono reato, ma fondano anche la responsabilità dell'ente.

Venendo infine all'ordinamento statunitense, il principale referente normativo è dato dal Titolo 47 U.S. Code, § 230 che sancisce una esenzione di responsabilità civile per il *provider*[69], finalizzata ad evitare che questi[70] possa essere considerato l'editore o il divulgatore delle informazioni prodotte dagli utenti o trasmesse su loro richiesta[71].

La disposizione non si applica in ambito penale, sicché in linea di principio il fornitore di servizi potrebbe rispondere in caso di commissione di un reato da parte dell'utente[72].

In materia di proprietà intellettuale la normativa USA detta disposizioni più specifiche, volte a responsabilizzare il *provider* nei rapporti con l'Autorità. Nella specie il titolo II del *Digital Millennium Copyright Act* (DMCA) ha introdotto la *section* § 512 nel codice federale che disciplina gli obblighi a carico dei fornitori di servizi. Essi dovranno designare un responsabile preposto alla ricezione dei reclami dei titolari dei diritti d'autore, che dovrà gestire le segnalazioni nel rispetto del contraddittorio tra le diverse parti e provvedere tempestivamente alla rimozione dei contenuti illeciti[73]. Al fine di contemperare le opposte esigenze, il DMCA introduce una presunzione di non responsabilità del *provider* che abbia in buona fede disabilitato l'accesso o rimosso i contenuti a seguito della ricezione di una notifica, bilanciata dalla previsione di una responsabilità per danni del segnalante per falsa denuncia. Il fornitore di servizi sarà comunque tenuto ad attivarsi per identificare l'autore di una violazione del copyright qualora un interessato richieda e ottenga dall'autorità giudiziaria una ingiunzione *subpoena*. In caso di inottemperanza il provider incorrerà nella violazione del provvedimento giurisdizionale e dovrà quindi pagare l'ammontare della sanzione in esso prevista.

III.4. *Indicazioni di* policy *per il contrasto ad operazioni coordinate di disinformazione attraverso le piattaforme web*

L'ampia premessa sul ruolo e sulle responsabilità del *provider* ci consente ora di fornire alcune indicazioni di *policy* per gli operatori del settore, che tengano conto non solo del vigente

[68] Si veda, ad esempio, la sanzione prevista dall'art. 112 del *code electoral* per le violazioni degli obblighi di trasparenza dell'art. 163-I del medesimo codice come modificati dalla legge 2018-1202 («*Toute infraction aux dispositions de l'article L. 163-1 est punie d'un an d'emprisonnement et de 75 000 € d'amende*»)..L'art. 112 comma 2 estende peraltro tale sanzione anche alle persone giuridiche («*Les personnes morales déclarées responsables pénalement, dans les conditions prévues à l'article 121-2 du code pénal, de l'infraction définie au premier alinéa du présent article encourent, outre l'amende suivant les modalités prévues à l'article 131-38 du même code, les peines prévues aux 2° et 9° de l'article 131-39 dudit code. L'interdiction prévue au 2° du même article 131-39 est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise*»).
Per approfondimenti v. il presente link. In dottrina v. Guerini (2020), p. 76.

[69] La sezione è intitolata "*Protection for private blocking and screening of offensive material*" è stata introdotta dal Communication Decency Act (CDA) emanato nel 1996. Per approfondimenti si veda la prima parte di questo studio (v. *supra,* Cap. I, § III)

[70] Per perimetrare l'ambito di applicazione soggettiva della Section § 230, la normativa statunitense reca le definizioni di *interactive computer services* e di *information content provider*. Quanto alla prima si intendono tutti i servizi di informazione o i provider di *software* che forniscano o abilitino l'accesso ad un server da parte degli utenti finali. Per *information content provider* si intende invece qualsiasi soggetto responsabile, in tutto o in parte, della creazione, dello sviluppo e della diffusione di informazioni trasmesse mediante Internet.

[71] La *common law* statunitense individua tre diverse figure soggettive (*publisher*, *distributor* e *conduit provider*) a cui si applica un regime differenziato di responsabilità in relazione all'attività concretamente svolta. Alcuni noti precedenti tra cui Cubby Inc. v. CompuServe Inc, 776 F. Supp. 135, 137 (S.D.N.Y. 1991) e Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995) hanno contribuito a tracciare il perimetro di responsabilità del *distributor* rispetto a quella del *publisher*. A tal fine rileverà non solo la concreta possibilità di controllo sui contenuti immessi dai terzi, ma anche la eventuale presenza di un moderatore dello spazio digitale, che comporta l'esclusione di qualsiasi potere/dovere di controllo da parte del *service provider*. Per contro, la presenza di strumenti di controllo sui contenuti (quali, ad es., l'impiego di un *software* in grado di svolgere una specifica attività di screening) fa venir meno quel carattere di neutralità che contraddistingue il mero *distributor* rispetto al *publisher*.
Il Communications Decency Act ha inciso sul filone giurisprudenziale in esame, prevedendo *per tabulas* che «*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*». Tale disposizione sembra ricalcare il contenuto dell'art. 15 della Direttiva 2000/31/CE, pur con la differenza data dal fatto che l'esenzione di responsabilità del CDA è circoscritta alla sola responsabilità civile.

[72] Osserva Baccin (2020), cit., pp. 78 ss. come, nonostante l'inapplicabilità della § 230, le Corti statunitensi abbiano affrontato in modo episodico e marginale casi di responsabilità penale del *provider*. Si rinvengono invece numerosi precedenti in sede civile che, analogamente all'esperienza europea, hanno plasmato il regime della responsabilità del *provider* in ragione della sua qualificazione come hoster "attivo" ovvero "neutro".

[73] Per attuare appieno le garanzie del contraddittorio è disciplinata la c.d. *counter notification*, una dichiarazione scritta per contestare l'avvenuta rimozione di un contenuto che il *provider* ritiene abbia violato il diritto d'autore di terze parti. Nel caso in cui l'utente notifichi tale dichiarazione, il fornitore di servizi dovrà seguire una procedura per il riesame della misura di rimozione.

quadro normativo ma anche delle opzioni allo studio delle istituzioni dell'Unione Europea. Le istruzioni di seguito elaborate si propongono l'obiettivo di prevenire possibili condotte di manipolazione dell'informazione e di assicurare una immediata reazione delle parti coinvolte nel caso in cui siano diffuse notizie false su larga scala.

Si farà riferimento, in particolare, al contrasto alle operazioni coordinate di disinformazione attraverso le piattaforme web, per tali intendendosi quelle poste in essere in modo organizzato e sistematico con l'intento di influenzare i processi democratici o orientare le scelte (economiche, politiche e ideologiche) dei cittadini. Al riguardo è utile precisare come il confine tra una operazione coordinata di disinformazione e la semplice diffusione di informazioni false (ascrivibile a uno o più utenti della rete) sia talvolta piuttosto labile. La capacità diffusiva di Internet, unita alla possibilità di condivisione delle informazioni sulle piattaforme social, può facilmente innescare gli "effetti rete" e rendere "virale" un contenuto senza che vi sia alla base un'azione coordinata di più strutture complesse o gruppi criminali. Si faccia l'esempio della diffusione di notizie non veritiere che riguardano un noto esponente politico, al fine di gettare discredito in vista delle prossime elezioni. Qualora tale azione fosse deliberata dai partiti antagonisti darebbe luogo a una "operazione coordinata"; mentre laddove fosse riconducibile ad alcuni cittadini *uti singuli* si avrebbe una semplice diffusione di notizie false. In ogni caso la portata diffusiva del messaggio, così come anche l'influenza sul dibattito democratico, potrebbe essere la medesima. Andrebbe anzi considerata l'eventualità che la disinformazione "coordinata" intervenga in un momento successivo rispetto alla creazione degli *user-generated-contents,* in modo da responsabilizzare alcuni attori (es. partiti politici, sindacati, aziende multinazionali, organizzazioni non governative etc.) anche nelle attività di semplice condivisione di informazioni prodotte da terzi.

L'ambito di riferimento delle *policies* riguarda quelle operazioni di disinformazione commesse mediante piattaforme online, che presentano rischi particolarmente elevati a causa del numero di utenti interessati, della transnazionalità delle comunicazioni e della rapidità delle interazioni tra utenti. Esse si rivolgono *in primis* ai gestori delle piattaforme, affinché adottino strumenti e procedure di controllo e di rimozione di contenuti oggetto di segnalazione, ed aderiscano a fonti di autoregolazione (codici di condotta, linee guida etc.).

Le indicazioni di *policy* si indirizzano anche alle istituzioni pubbliche e private che pubblicano sulle piattaforme notizie sullo svolgimento relative alla propria attività imprenditoriale o istituzionale. Tali soggetti dovrebbero premurarsi di contenere il rischio di manipolazione delle informazioni, monitorando sulla correttezza dei contenuti diffusi in rete che li riguardino, ovvero che abbiano ad oggetto il proprio ambito di attività o di interesse.

Il quadro normativo e giurisprudenziale esaminato in questo studio evidenzia come il sistema di controllo successivo da parte del *provider* sia quello maggiormente in linea con le esigenze della società dell'informazione. I soggetti interessati dovranno dunque predisporre meccanismi di *notice and take down*, fornire certezza dei tempi di intervento, stabilire il contenuto delle notifiche relative alla presenza di informazioni false, offrire informazioni trasparenti e corrette sulle condizioni di utilizzo, garantire il contraddittorio con gli interessati, collaborare con le autorità e contribuire alla responsabilizzazione dei propri utenti.

Sarebbe inoltre opportuno differenziare i tempi e le modalità di intervento e di rimozione dei contenuti in base al grado di gravità e alla tipologia delle informazioni false, distinguendo tra quelle manifestatamente false e quelle apparentemente false. Per queste ultime si dovrebbe prevedere un contraddittorio pieno con l'autore del contenuto, mentre per le prime andrebbe prevista la rimozione immediata e cautelare in attesa della risposta dell'interessato[74].

Inoltre, nell'attesa di una base normativa di matrice sovranazionale che preveda specifici rimedi giuridici, il contrasto alla disinformazione non potrà che essere rimessa alle fonti di auto-regolazione, come più volte sottolineato dalla Commissione europea. Sul punto il considerandum n. 67 della proposta di regolamento sui servizi digitali (DSA) prevede che la Commissione e il Comitato europeo per i servizi digitali debbano «*incoraggiare l'elaborazione di codici di condotta per contribuire all'applicazione del presente regolamento*», con la precisazione che l'adozione dei codici di condotta «*dovrebbe essere misurabile e soggetta a controllo pubblico*», senza tuttavia pregiudicare il carattere volontario di fonti e la libertà delle parti interessate di

[74] Occorre dar conto di alcune tesi formulate in dottrina secondo cui il legislatore non dovrebbe assegnare il compito di rimozione del contenuto alla piattaforma privata, essendovi in tal caso il rischio di legittimare forme di censura privata. Si propone a tal fine di istituire un'autorità amministrativa indipendente, che assicuri imparzialità e professionalità (per considerazioni sul tema si rinvia ad altra parte di questo studio, Cap. III, § III.4.).

decidere se aderirvi.

La previsione di misure di *soft law* risulta di particolare importanza per le piattaforme di dimensioni molto grandi, che dovrebbero cooperare con le Istituzioni nell'elaborazione di specifici codici di condotta. Sarebbe opportuno che tali codici di condotta, anche a valle di accordi di autoregolamentazione e di coregolamentazione (cfr. considerandum n. 68 DSA), prevedano misure di attenuazione dei rischi riguardanti la disinformazione e, in generale, le attività di manipolazione e abuso dell'informazione.

In relazione a tali ambiti l'adesione a un determinato codice di condotta e il suo rispetto da parte di una piattaforma online potrà essere ritenuta una valida misura di attenuazione dei rischi, e soprattutto offrirà una valida esimente di responsabilità in sede giudiziaria, laddove fosse invocata una condotta colposa o negligente della piattaforma stessa in relazione alla diffusione di notizie non veritiere o alla omessa rimozione tempestiva dei contenuti.

Tutto ciò premesso in calce al capitolo successivo sono contenute le indicazioni di *policy* per i gestori delle piattaforme e per le istituzioni pubbliche o private.

Bibliografia

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

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.

Bocchini, Roberto (2017): "La responsabilità di *Facebook* per la mancata rimozione dei contenuti illeciti", *Giurisprudenza italiana*, 3, pp. 632-643.

Bugiolacchi, Leonardo (2015): "Ascesa e declino della figura del *provider* «attivo»? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'*hosting provider*", *Responsabilità civile e previdenza*, 4, pp. 1261-1270.

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

Gullo, Antonio (2019): *Sub* art. 595, in Padovani, Tullio (a cura di): "Codice Penale" (Milano, Giuffrè), pp. 3907-3940.

Ingrassia, Alex (2012): "Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?" in Luparia, Luca (a cura di) "*Internet provider* e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale" (Milano, Giuffrè), pp. 15-66.

Nardi, Valerie (2019): "I discorsi d'odio nell'era digitale: quale ruolo per l'*Internet service provider*?", *Diritto Penale Contemporaneo*, 7 marzo 2019, pp. 1-33.

Pagella, Cecilia (2019): "*La cassazione sulla responsabilità del blogger per contenuti diffamatori (commenti) pubblicati da terzi*", *Diritto penale contemporaneo*, 17 maggio 2019.

Panattoni, Beatrice (2018): "Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di *notice* and *take down*", *Diritto penale contemporaneo – Rivista trimestrale*, 5, pp. 249-263.

Picotti, Lorenzo (1999): "La responsabilità penale dei *service-providers* in *internet*", *Diritto penale e proc*esso, 3, pp. 379-386.

Pitruzzella, Giovanni, Pollicino, Oreste, Quintarelli, Stefano (2017): "Parole e Potere: Libertà d'espressione, *hate speech* e *fake news* (Milano, Egea).

Rozgonyi, Krisztina (2018): "*The impact of the information disorder (disinformation) on elections*" in www.venice.coe.int.

Seminara, Sergio (1997): "La pirateria su *internet* e il diritto penale", *Rivista trimestrale di diritto penale* dell'economia, 1, pp. 71-114.

Vargas Valdez, José Luis (2018): "*Study on the role of social media and the Internet in democratic development*" in www.venice.coe.int.

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

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