CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

Editore Associazione "Progetto giustizia penale", via Altaguardia 1, Milano - c.f. 97792250157
ANNO 2019 - 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.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

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

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

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

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

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

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

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

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

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

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

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

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

Contents

Contents

Financial cybercrime

Cibercrimen financiero

Financial Cybercrime

Contents

La tutela penale della privacy nel cyberspazio

La tutela penal de la privacidad en el ciberespacio

Criminal Law and the Protection of Privacy in Cyberspace

Contents

Contents

Contents

Il diritto penale nel cyberspazio

El derecho penal en el ciberespacio

Criminal Law in Cyberspace

Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme *online*

Los efectos de la automatización en los modelos de responsabilidad: el caso de las plataformas online

The Effects of Automation on Imputation Models: the Case of Online Platforms

Beatrice Panattoni
Dottoranda di Diritto penale presso l'Università di Verona
beatrice.panattoni@univr.it

Reati informatici | Delitos informáticos | Cybercrimes

Abstracts

Già nella seconda metà del secolo scorso, con lo sviluppo degli agenti informatici e l'apertura al pubblico di Internet, si possono rintracciare le prime applicazioni dell'automazione. La novità tecnologica di questo *medium* ha in questi anni vissuto però importanti e profondi evoluzioni, delineando scenari innovativi e bisognosi di adeguata regolamentazione. Sul fronte dei regimi di responsabilità configurabili in capo ai diversi soggetti, la struttura complessa della rete ha posto numerose problematiche, in particolare per quanto concerne le possibili allocazioni di responsabilità penale in capo agli *Internet service provider*, soggetti privati che gestiscono servizi in rete, il cui ruolo ha visto negli ultimi anni importanti trasformazioni. Partendo dalle novità di rilievo giuridico rinvenibili a livello europeo, si cercherà di evidenziare i più recenti sviluppi in materia. In questa prospettiva, il punto che suscita le maggiori perplessità è quello della configurabilità di una responsabilità penale omissiva a carico degli ISP (*Internet Service Provider*) per contenuti illeciti immessi in rete dagli utenti, ipotesi che rappresenta anche un'occasione, per la dottrina e la giurisprudenza, per interrogarsi su possibili ripensamenti di basilari categorie penalistiche, anch'esse bisognose di adeguarsi alle peculiarità delle componenti tecnico-informatiche.

Ya en la segunda mitad del siglo pasado, con el desarrollo de los agentes informáticos y la apertura de internet al público, se pueden rastrear las primeras aplicaciones de la automatización. La novedad tecnológica de este *médium* ha generado profundas e importantes evoluciones, delineando escenarios innovadores que requieren una adecuada regulación. En relación a los regímenes de responsabilidad personal, la compleja estructura de la red ha planteado numerosos problemas, en particular respecto a los proveedores de servicios de Internet, entidades privadas que gestionan servicios en línea, cuyo papel ha visto importantes transformaciones en los últimos años. A partir de los nuevos problemas legales que se han presentado a nivel europeo, se intentará evidenciar los más recientes desarrollos en esta materia. Desde esta perspectiva, la cuestión que genera el mayor grado de perplejidad es el de la posibilidad de configurar una responsabilidad penal omisiva de los ISP por el contenido ilícito ingresado a la red por los usuarios. La anterior hipótesis representa, además, una oportunidad, tanto para la doctrina como para la jurisprudencia, de cuestionarse sobre un posible replanteamiento de las categorías penales básicas, las cuales debiesen adecuarse a las peculiaridades de los componentes técnico-informáticos.

Since the second half of XX century, thanks to the development of ICT and the opening to the public of the internet, automation has been applied for the first time. The new technologic medium significantly and profoundly evolved over the years, shaping new scenarios that need a proper regulation. With respect to the liability of a

number of subjects, the complexity of the web poses several issues, especially with respect to criminal responsibility (if any) of the Internet service provider, i.e. private entities managing web services, whose role has deeply changed in recent years. Starting from the new legal framework at EU level, this paper aims to highlight the most recent developments on the topic. From the said perspective, a really controversial point refers to a criminal liability for omission of the ISP about the unlawful content uploaded by the users. Such a situation can induce scholars and the case law to rethink basic criminal law concepts, to be reshaped in light of the ICT peculiarities.

Sommario

1. Premessa.

Le componenti tecnologiche, o meglio le nuove tecnologie dell'informazione e della comunicazione (TIC), fondate su algoritmi sempre più complessi, compenetrano ormai in modo incisivo ogni aspetto della vita relazionale: ce ne serviamo per il compimento delle più disparate attività e sono diventate parte integrante di una realtà "collegata"[1]. L'insinuarsi di un elemento "estraneo" ed artificiale, come è appunto quello dell'automazione dei processi di elaborazione dei dati, materializzato nella creazione di strumenti tecnologici sempre più avanzati, ha rivoluzionato la nostra esperienza, suscitando l'interesse di studio delle più diverse branche del sapere.

Uno dei grandi campi di applicazione di queste nuove componenti tecnologiche è costituito dalla costruzione e sviluppo della rete Internet, o meglio del c.d. *Cyberspace*[2]. Diventato oggi luogo sociale, all'interno del quale si svolgono le più disparate attività, il *Cyberspace* ospita un'infinità di relazioni globalizzate, delocalizzate, dilatate e dematerializzate[3].

La rete Internet che conosciamo oggi è considerevolmente cambiata rispetto alle sue prime conformazioni. Grazie all'avvento dei *Big data* e alla *Big data analytics,* il *Web* sta oggi entrando nella sua versione 4.0[4]. Il cambiamento determinante può essere già rintracciato nel massivo passaggio dal dato all'informazione[5], a seguito del quale Internet si presenta come un vero e proprio «villaggio globale»[6], all'interno del quale i singoli utenti possono interagire attivamente, potendo altresì diventare vittime e autori di fatti criminosi[7]. Si tratta oggi di uno «spazio-movimento»[8], uno «spazio mobile in cui tutto cambia rispetto a tutto e in cui la distanza non è niente e la velocità è tutto»[9].

Nel tentativo di analizzare e concettualizzare le diverse novità che caratterizzano l'elemento dell'automazione tecnica operante attraverso agenti informatici, emerge chiaramente come le stesse peculiarità che contraddistinguono la natura e il funzionamento della realtà digitale non possano che avere corrispondenti ricadute sul piano linguistico e concettuale, dal momento che le categorie utilizzate per descrivere, comprendere e regolare tali fenomeni risultano necessariamente permeate dalla loro natura. L'impiego di strumenti informatici e telematici, in quanto portatori di nuove realtà ed esperienze, la cui descrizione e regolamentazione sfugge agli schemi concettuali "tradizionali" (basti pensare alle diverse dimensioni di tempo e spazio del *Cyberspace*), può condurre alla "creazione" di nuovi concetti e categorie;

[1] Definita dal filosofo Luciano Floridi attraverso il neologismo *"onlife"* con il quale si intende definire la realtà che viviamo quale simbiosi tra l'essere *online* e *offline*: la nuova esperienza di una «*hyperconnected reality within which it is no longer sensible to ask whether one may be online or offline*», Floridi (2015); in modo più approfondito Floridi (2017).

[2] Nozione derivante dagli Stati Uniti, la quale non ha preciso contenuto tecnico o giuridico, ma è frequentemente utilizzata per richiamare l'idea del c.d. spazio virtuale quale prodotto dell'integrazione fra sistemi di comunicazione e connessione che utilizzano le nuove tecnologie informatiche, v. Picotti (2011), p. 830. Si tratta di un termine che secondo alcuni è stato utilizzato per la prima volta da William Gibson, nel racconto fantascientifico Burning Chrome (1982) e nel successivo romanzo Nueromancer (1984).

[3] Berlingò (2017), pp. 641-643.

[4] Definito come un *web* "simbiotico". Aghaei (2012), p. 8: «*the dream behind of the symbiotic web is interaction between humans and machines in symbiosis. It will be possible to build more powerful interfaces such as mind controlled interfaces using web 4.0. In simple words, machines would be clever on reading the contents of the web and react in the form of executing and deciding what to execute first to load the websites fast with superior quality and performance and build more commanding interfaces*».

[5] Cassano (2017), p. 1231, con l'espressione "passaggio dal dato all'informazione" si intende che «alla funzione di registrazione e di memorizzazione elettronica dei dati come rappresentazione elementare di un fatto, si affianca l'attività complementare di elaborazione e di organizzazione logica, con formazione di un insieme coordinato di "informazioni"». Nello stesso senso Floridi (2017), p. 96; nonché Berlingò (2017), pp. 641- 675, secondo la quale «il campo d'osservazione è destinato per vero a mutare angolatura appuntandosi più che sul singolo dato, sul processo della c.d. *datafication,* dove tutto è riducibile a informazione e dove la dittatura degli algoritmi rappresenta come scientifiche ed oggettive scelte prodotte da modelli matematico-informatici».

[6] Seminara (1997), p. 72.

[7] Picotti (2012), pp. 2554-2556.

[8] Amato Mangiameli (2017), p. 151.

[9] Ibidem.

oppure, modellando sotto nuove forme esperienze sussumibili entro concetti esistenti (l'investimento di un pedone, accadimento legato alla comune esperienza, ma da parte di un agente autonomo quale una *self-driving car*), può condurre a nuove configurazioni di concetti ancora validi e applicabili.

Il diritto non può dunque rimanere esente da questi mutamenti, evolvendo con il mutare dei mezzi espressivi e delle tecnologie a questi connesse[10]: come la nascita della scrittura ha determinato l'avvento dell'interpretazione, anche la rivoluzione cibernetica non può che coinvolgere la scienza giuridica, in un rapporto di reciproca interazione e condizionamento. Come è stato sostenuto da diverse voci in dottrina[11] infatti, la relazione tra strumento giuridico e tecnologico non deve sfociare in alcuna prevaricazione dell'uno sull'altro, ma il "codice tecnico"[12] deve trovare necessariamente una regolamentazione giuridica che ne plasmi il corso e l'evoluzione entro vie che garantiscano la tutela dei diritti dei soggetti che operano al suo interno o per suo tramite[13].

Tale esigenza è resa ancora più pressante laddove lo strumento di tutela richiesto sia rappresentato dal diritto penale, il cui coinvolgimento nelle dinamiche del *Cyberspace* risulta ormai da numerosi casi giurisprudenziali nonché contributi dottrinali. Essendo infatti il *Cyberspace* caratterizzato da una potenzialità criminale molto elevata[14], data dai suoi caratteri di facile accessibilità, anche in modo anonimo, illimitata diffusione dei contenuti e immediatezza di effetti, la lotta al crimine cibernetico, o meglio ai c.d. «reati cibernetici»[15], è un campo in continuo e necessario aggiornamento.

2. Il *Cyberspace* quale realtà plurisoggettiva.

Nella sua odierna configurazione, il *Cyberspace* si presenta come una realtà in cui operano diversi soggetti, portatori di istanze ed esigenze di tutela diversificate e in un gran numero di casi contrastanti le une con le altre. È possibile individuare tre grandi tipologie di soggetti coinvolti: gli utenti, i *provider* (prestatori di servizi o gestori di piattaforme *online*) e le istituzioni pubbliche.

Occorre precisare che con il termine *provider* si farà qui riferimento alla categoria maggiormente rilevante, ossia ad una particolare tipologia di *Internet service provider* (prestatori di servizi in rete): gli *hosting provider,* intermediari che gestiscono servizi di memorizzazione di dati altrui[16] attraverso piattaforme di *social network, blog* o altre tipologie di siti internet.

Il ruolo degli utenti e dei *provider* è considerevolmente cambiato nel tempo, le capacità e le potenzialità di queste due categorie si sono ampliate e articolate attraverso modalità nuove e disparate.

Per quanto riguarda gli utenti, vi è stato un cambiamento sia sul piano qualitativo sia su quello quantitativo. Sotto il primo profilo, nell'era del web 4.0, essi sono divenuti parte interattiva nel *Cyberspace,* vengono spesso definiti quali *prosumer*[17], produttori e non solo fruitori di contenuti e servizi *online*. Sotto il secondo profilo, il numero di utenti che interagiscono in rete è esponenzialmente aumentato[18], grazie alle capacità di accesso continuo, rese possibili dai

[10] Pascuzzi (2016), p. 12.
[11] Picotti (2019), pp. 33-96; nello stesso senso Fiandaca (2005), p. 7-23; nonché Luberto e Zanetti (2008), p. 497 ss., secondo il quale il diritto può «incidere sull'architettura – intesa come insieme delle caratteristiche tecniche, comprensive del *software* e dell'*hardware*, che rendono la rete così com'è – e regolare i comportamenti degli utenti».
[12] Lessing (2006).
[13] Applicazione di questo approccio è la c.d. *privacy by default* e *by design* regolata dal GDPR. Sul punto Finocchiaro e Avitabile (2017).
[14] Gli atti delittuosi all'interno del *Cyberspace* coinvolgono ormai un gran numero di settori e fattispecie criminose. Essi possono essere suddivisi, come riportato in Sabella (2017), pp. 149-151, in: *Cybercrime* comune; *Cyber hactivism; Cyber espionage; Cyber war; Cyber terrorism.*
[15] Definiti quali reati che «si commettono o si possono commettere in rete o nel *web* o, meglio "nel" *Cyberspace,* in quanto la formulazione legale delle relative fattispecie incriminatrici contiene un elemento essenziale o circostanziale che *espressamente* richiama la rete ("reati cibernetici in senso stretto"), ovvero prevede elementi di tipizzazione del "fatto" di reato che solo *implicitamente* od in via ermeneutica sono *compatibili* con la concreta realizzazione nel *Cyberspace* ("reati cibernetici in senso ampio")»; così Picotti (2019), pp. 77-78.
[16] Così come definiti dall'art. 14 della direttiva 31/2000/UE (c.d. direttiva sul commercio elettronico, o direttiva *e-commerce*), relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno: prestatori di un «*servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio*».
[17] Gli utenti che producono in modo amatoriale contenuti a cui hanno accesso anche gli altri utenti vengono chiamati *prosumer*, crasi dei termini *producer* e *consumer*; si tratta di un termine introdotto da Alin Toffler nel 1980 (A. Toffler, *The third wave*, New York, 1980), così come viene riportato in Montanari (2017), p. 260; nello stesso senso Scialdone (2013), p. 8.
[18] Nel marzo 2018 il fondatore di Facebook annunciava che gli utenti iscritti al suo *social network* avevano raggiunto i 2,2 miliardi (https://www.facebook.com/zuck/posts/10104878807622211).

numerosi dispositivi elettronici, i quali sono ormai parte integrante della quotidianità.

Anche gli *Internet Service Provider* (ISP) hanno conosciuto importanti cambiamenti sul fronte degli strumenti tecnici a loro disposizione, i quali hanno contribuito ad accrescere le loro potenzialità e il loro ruolo nella Rete. Andando ben oltre il mero servizio di memorizzazione di informazioni, questi soggetti si sono ormai allontanati dalla definizione contenuta nella direttiva europea sull'*e-commerce*, la cui disciplina risulta – come si vedrà meglio *infra* – non più adeguata ai tempi[19]. L'evoluzione più importante risiede nel cambiamento della loro posizione rispetto ai contenuti presenti sulle piattaforme da essi gestite, non più fondata su mere operazioni automatizzate, tecniche e passive, essendo piuttosto divenute "attive", come rilevato dalla stessa giurisprudenza europea e nazionale[20].

La continua ed inarrestabile crescita del web e della mole di contenuti che in esso vengono quotidianamente immessi, trasportati e memorizzati, è stata in gran parte resa possibile dalle nuove attività svolte dai *provider*. Quelle che assumono maggiore rilevanza sono, per l'appunto, quelle che si basano sull'automazione tecnologica di analisi, organizzazione e relazione dei contenuti memorizzati, che rendono possibile agli ISP il trattamento delle informazioni desiderate[21], reperendole sempre più facilmente all'interno dell'«oceano informativo»[22]. Si tratta di attività che vengono utilizzate dagli intermediari per lo svolgimento del proprio esercizio economico (si pensi alla "profilazione" dell'utente a scopi pubblicitari). Lo sviluppo tecnologico ha reso dunque possibile l'acquisizione di maggiori capacità di controllo ed intervento da parte dei prestatori di servizi *online,* seppur ogni situazione vada considerata nella sua singolarità, dal momento che il grado di incidenza e di operatività nella rilevazione e controllo dei contenuti mutano in base alle tipologie di *softwares* utilizzati, ai servizi e alle *policies* di gestione scelte dall'ISP[23].

L'interazione tra il ruolo maggiormente partecipativo degli utenti e le capacità di gestione ed elaborazione dei dati dei *provider* ha determinato la creazione di nuove tipologie di piattaforme *online*, come i motori di ricerca ed i siti ospitanti i c.d. *user generated content*[24], contenuti che vengono direttamente creati dagli utenti (come accade nei *social network*). Queste ultime sono le realtà che pongono le maggiori problematiche dal punto di vista giuridico: ci si interroga infatti se gli ISP possano essere ritenuti responsabili per i contenuti illeciti caricati, o anche condivisi dai propri utenti, dovendo altresì distinguere tra *user generated content* e *user uploaded content,* contenuti altrui solamente riprodotti *online* senza alterazioni o rielaborazioni[25].

Vi è infine la terza categoria di soggetti coinvolti nelle dinamiche del *Cyberspace,* quella delle istituzioni ed autorità pubbliche, le quali cercano di regolare l'utilizzo ed il funzionamento della rete, sorvegliare le attività che vi si svolgono ed in specie contrastare la criminalità cibernetica attraverso misure preventive od attività investigative.

Per incentivare e strutturare il coinvolgimento del soggetto pubblico, è particolarmente rilevante la scelta di istituire autorità amministrative competenti nei specifici settori d'interesse, così che prestatori di servizi in rete ed utenti possano avere un ente pubblico quale punto di

[19] Secondo diverse voci della dottrina la direttiva 31/2000/CE necessita di un ripensamento o quantomeno aggiornamento; si tratta infatti di una normativa che si trova oggi a disciplinare una realtà diversa – portatrice quindi di differenti esigenze di tutela – rispetto a quella risalente al periodo storico in cui è entrata in vigore. Sul punto: Picotti (2019), pp. 81-89; Petruso (2018), pp. 511-558; Bocchini (2017), pp. 632-643; Pollicino (2014), pp. 1-27.

[20] Corte di giustizia dell'Unione Europea, sentenza del 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France e Google*, EU:C:2010:159; sentenza del 12 luglio 2011, C-324/09, *L'Oréal e a.,* EU:C:2011:474. Secondo questa giurisprudenza occorre distinguere tra *provider* c.d. "attivi" e passivi, dal momento che gli intermediari possono andare esenti da responsabilità – secondo il regime delineato dalla direttiva *e-commerce* – solo se mantengano un comportamento di rigorosa passività nei confronti dei contenuti da essi conservati od ospitati.

[21] Si pensi ai c.d. programmi filtro, *software* «in grado di controllare i contenuti dei materiali che gli utenti immettono in rete tramite il servizio reso dal *provider*», Di Ciommo (2010), p. 831.Oltre a questi sono attualmente utilizzati dagli ISP numerosi algoritmi e *software* di riconoscimento e monitoraggio dei dati, cfr. nota 39.

[22] Bugiolacchi (2013), p. 205.

[23] Di Ciommo (2010), pp. 830-833. La capacità di controllo dipende inoltre dal tipo di *provider*. Per i soggetti che forniscono l'accesso alla rete vi sono possibilità di controllo sia attraverso un esame delle informazioni prima del loro trasferimento che in tempo reale; mentre alcuni *service provider* possono anche non operare un controllo delle informazioni fornite.

[24] Termine che si è iniziato a utilizzare intorno al 2005, con la diffusione delle piattaforme sociali. Secondo l'OCSE, per essere qualificato come *user generated content* un contenuto deve essere: (i) pubblicamente accessibile su un sito Internet o un *social network;* (ii) il risultato di un certo apporto creativo; (iii) creato al di fuori di attività professionali o imprenditoriali. Organization for Economic Co-operation and Development, *Participative web: user-created content,* DSTI/ICCP/IE(2006)7/FINAL, 12.04.2007, disponibile al sito https://www.oecd.org/sti/38393115.pdf. Secondo invece l'Ofcom (Office of Communications, l'autorità competente e regolatrice indipendente per le società di comunicazione nel Regno Unito) si tratta di contenuti multimediali resi disponibili *online*, derivanti da un'attività creativa che non è la principale e diretta fonte di guadagno dell'autore. Ofcom, *The Value of User Generated Content,* 21 June 2013, p. 5, disponibile al sito https://www.ofcom.org.uk/__data/assets/pdf_file/0016/32146/content.pdf. Sul punto cfr. D'Ippolito (2017), pp. 524-529.

[25] Ibidem.

riferimento a cui ricorrere in caso di necessità. Autorità di questo tipo sono già oggi esistenti, un esempio si può rintracciare in tema di lotta alla pedopornogragia *online*: in questo ambito l'art. 14 *bis* della legge n. 269 del 3 agosto 1998, introdotto dalla L. n. 38/2006, ha previsto l'istituzione del Centro nazionale per il contrasto della pedopornografia sulla rete Internet[26]. Ulteriori interventi in questo senso sono stati fatti anche in materia di lotta al terrorismo, campo nel quale la collaborazione tra istituzioni pubbliche e soggetti privati si è fatta sempre più stringente[27].

In quanto realtà plurisoggettiva il *Cyberspace* costituisce un contesto nel quale si scontrano diverse esigenze, portartici di diversi diritti ed interessi di difficoltoso contemperamento, e nel quale è quindi complesso attribuire in modo generalizzato forme di responsabilità ai singoli soggetti. Uno degli aspetti più controversi si sostanzia nel complesso bilanciamento tra i diritti facenti capo agli utenti, vittime di crimini cibernetici – i cui diritti dovrebbero essere garantiti e protetti attraverso l'intervento di autorità pubbliche e non (soltanto) enti privati – e gli interessi degli ISP esercenti attività di libera impresa nel *Cyberspace.* La complessità nasce soprattutto dal tradizionale approccio dicotomico che contrappone due istanze in termini contrastanti, come nel caso più frequente di conflitto tra diritto alla libertà d'espressione e tutela dei diritti della personalità, quando (anche in rete) gli uni sono strumentali all'esercizio degli altri ed è, dunque, ancor più delicata l'attribuzione di prevalenza ad uno di essi[28].

Le tre categorie di soggettività sopra richiamate, in considerazione delle modalità di realizzazione delle proprie attività in rete o per la loro natura pubblicistica, sono parti imprescindibili per la costruzione di una equilibrata regolamentazione delle responsabilità nel *Cyberspace*. In questo ambiente, per la stessa evoluzione che lo sta segnando, sembra infatti difficile allocare una generale responsabilità per violazioni e contenuti illeciti in capo ad un singolo attore o categoria di attori, emergendo molto spesso l'utilità delle teorie del *"risk sharing"* e del *"problem of many hands"*[29].

Non considerare questa interazione tra le diverse soggettività nel delineare una forma di regolamentazione fondata su un sistema normativo "integrato" e multilivello[30] può, da una parte, creare incertezze applicative, dall'altra, lasciare troppa discrezionalità in capo a soggetti privati, quali appunto gli ISP, che agiranno in ogni caso seguendo logiche economico-imprenditoriali. Il paradigma economico su cui si fondano le scelte operative dei prestatori di servizi *online* guarda infatti all'*audience* come a una «vera e propria merce di scambio, dal momento che il potere della stessa è prodotto, venduto, acquistato e consumato»[31]. Considerando che le nuove tecnologie di *user data profiling* rendono possibile la predisposizione di pubblicità mirate e calibrate in base alle preferenze degli utenti[32], i cui dati diventano sempre più preziosi nel mercato digitale, le scelte degli ISP saranno sempre più dirette all'incremento del numero di utenti che usufruiscano dei servizi e delle piattaforme da essi gestiti. E una tale logica non può che condurre a dei rischi per i diritti della persona e a dei vuoti di tutela, dal momento che elevati numeri di utenti possono essere attirati dall'alto grado di libertà e autonomia che il gestore della piattaforma concede loro nel caricamento di contenuti o, nei casi più gravi,

[26] Centro istituito presso il servizio di Polizia postale e delle comunicazioni del dipartimento della Pubblica Sicurezza a Roma, che ha il compito di raccogliere tutte le segnalazioni, provenienti da organi di polizia stranieri, da soggetti pubblici, da associazioni di volontariato, da *provider* e da privati cittadini, riguardanti siti che diffondono materiale pedopornografico, ma anche gestori o eventuali beneficiari che, in caso di riscontro positivo, vengono inseriti dalla Polizia in un elenco tenuto costantemente aggiornato, la cosiddetta *"black list"*. Tale elenco viene poi fornito agli ISP, che provvedono ad inibire la navigazione attraverso sistemi tecnici di filtraggio. Sul punto cfr. Picotti (2007), pp. 1196-1211.

[27] Si pensi al d.l. n. 7 del 18 febbraio 2015, con il quale è stata prevista la redazione di un elenco di siti web utilizzati per attività e condotte di associazione terroristica da parte dell'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, nonché l'obbligo per i fornitori di connettività di inibire l'accesso ai siti inseriti nella lista quando ne faccia richiesta la magistratura, (sul punto Scardino (2015), pp. 215-239). Per esperienze in altri ordinamenti, si pensi alla legge francese che ha introdotto un obbligo per gli intermediari (ma non per i *social network*) di rimozione o blocco di tutti i siti che inneggiano all'apologia al terrorismo sulla base di una *black list* predisposta da un organo *ad hoc* del Ministro degli Interni (*Decret* n. 2015-125 *du fevrie* 2015, http://www.legifrance.gouv.fr, (sul punto Abbondante (2017), p. 64).

[28] Di Tano (2017), p. 126. Sul tema del bilanciamento dei diritti fondamentali in rete si è espressa più volte la Corte europea dei diritti dell'uomo, si ricordano le seguenti pronunce: *Neij e Sunde Kolmisoppi v. Sweden (The Pirate Bay),* ricorso n. 40397/12, sentenza del 19/02/2013; *Delfi AS v. Estonia,* ricorso n. 64569/09, sentenza del 16/06/2015; *Pihl v. Sweden,* ricorso n. 74742/14, sentenza del 9/03/2017.

[29] Helberger *et al.* (2018), pp. 1-14.

[30] Sabella (2017), pp. 140-142.; Militello (2014), pp. 106-132

[31] Smythe (2009), pp. 238-240; così come riportato in Montanari (2017), p. 261.

[32] Molti intermediari traggono profitto dalla raccolta dei dati personali e sensibili degli utenti, di cui gli inserzionisti pubblicitari si servono per individuare i profili a cui destinare pubblicità mirate in base a gusti, preferenze e attitudini. Inoltre, gli intermediari possono evidenziare contenuti popolari (i quali registrano grandi numeri di interazioni), concentrando intorno a questi ultimi pubblicità mirate. Cfr. Allegri (2017), pp. 70-72.

potrebbero essere attirati dagli stessi contenuti illeciti ospitati dalla piattaforma.

La giurisprudenza, europea e nazionale, nonché i contributi dottrinali che hanno affrontato il tema delle responsabilità nel *Cyberspace,* si sono concentrate nel tempo proprio sulla complessa tematica della responsabilità dei prestatori di servizi[33]. È infatti su questi ultimi, in virtù del ruolo di primaria importanza che rivestono nella gestione della realtà digitale, che si concentrano i dubbi relativi ad attribuzioni di forme di responsabilità per gli illeciti commessi tramite le piattaforme ed i servizi da loro offerti.

L'esigenza di una maggior responsabilizzazione di questi soggetti[34] – i cui termini e condizioni saranno analizzati in seguito – si fonda quindi non solo sulla loro posizione di «custodi materiali»[35] dei contenuti della rete, ma soprattutto sulle capacità di intervento di cui dispongono e che attualmente già utilizzano, senza che queste possano dunque considerarsi fonte di costi eccessivi da sostenere. L'attività di rilevazione ed analisi dei contenuti illeciti *online* all'interno delle piattaforme può essere infatti effettuata grazie a *softwares*, i quali, «basati sull'utilizzo di 'impronte digitali' abbinate univocamente al contenuto digitale tutelato, non richiedono irragionevole impiego di risorse preposte allo scopo»[36]. Inoltre, gli ISP di grandi dimensioni dispongono già di *staff* di persone dedicate alla gestione delle segnalazioni concernenti contenuti illeciti presenti sulle proprie piattaforme[37]. Naturalmente regimi di responsabilità fondati su tali capacità devono partire necessariamente da una distinzione fra le diverse tipologie di intermediari, differenziando quelli più solidi da un punto di vista imprenditoriale ed economico da quelli di più modeste dimensioni e strutture tecniche, in modo da evitare che un regime troppo severo di responsabilità espella dal mercato i *provider* «non in grado di sopportare i costi di un sistema capillare di prevenzione degli illeciti oppure di un allargamento del fronte dei risarcimenti dovuti»[38].

3. La responsabilità penale degli ISP in caso di caricamento e/o diffusione di contenuti illeciti in rete.

Gli *hosting provider* assumono un ruolo di particolare rilevanza nei casi in cui vengano caricati e diffusi per il tramite delle piattaforme da questi gestite contenuti aventi carattere lesivo di diritti altrui. Si tratta, in particolare, di quei reati cibernetici commessi attraverso la comunicazione di informazioni in rete, o, meglio, attraverso la «messa a disposizione» di dati in rete[39]. Tra le fattispecie maggiormente rilevanti basti qui richiamare il reato di diffamazione

[33] Anche se recentemente l'attenzione si è spostata anche sugli utenti, in quanto autori materiali degli illeciti commessi nel *Cyberspace.* Sul punto giova richiamare la proposta di legge a firma del senatore Nazario Pagano (atto n. 895 Senato) la quale propone di introdurre un obbligo di identificazione degli utenti, aggiungendo all'interno del D.lgs. n. 70/2003 (attuativo della direttiva sull'*e-commerce* 31/2000) l'art. 16 *bis,* ai sensi del quale «*1. I fornitori di servizi di memorizzazione permanente hanno l'obbligo di richiedere, all'atto di iscrizione del destinatario del servizio, un documento d'identità in corso di validità. 2. L'inosservanza dell'obbligo di cui al comma 1 comporta l'irrogazione di una sanzione amministrativa pecuniaria da 500 a 10.000 euro. 3. Le sanzioni amministrative pecuniarie di cui al comma 2 sono applicate dall'Autorità per le garanzie nelle comunicazioni con provvedimento motivato, previa contestazione degli addebiti agli interessati, da effettuare entro un mese dall'accertamento. 4. Le disposizioni del presente articolo si applicano a decorrere dal 1° gennaio 2020*».

[34] In questo senso, nella giurisprudenza europea: Corte di giustizia europea, sentenza del 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France e Google*, EU:C:2010:159; sentenza del 12 luglio 2011, C-324/09, *L'Oréal e a.,* EU:C:2011:474; sentenza del 27 marzo 2014, C-314/12, *UPC Telekabel Wien,* EU:C:2014:192. Nella giurisprudenza italiana: Corte d'Appello di Roma, 19 febbraio 2018, n. 1065, inedita; Corte d'Appello di Roma, 28 aprile 2017, n. 2833, in *Quotidiano giuridico,* 10 maggio 2017; Tribunale di Torino, 7 aprile 2017, n. 1928, in *Danno resp.*, 2018, 1, p. 87 ss.; Tribunale di Napoli Nord, 3 novembre 2016, in *Giur. it.*, 2017, 3, p. 629 ss.; Tribunale di Milano, 7 giugno 2011, n. 7680, inedita.

[35] Di Tano (2017), p. 114.

[36] Tosi (2017), pp. 75-122. Altri esempi possono essere il blocco dei numeri IP e la manomissione o blocco del DNS (*Domain Name Server*), con il limite tuttavia di impedire l'accesso a qualsiasi contenuto, anche se innocuo, ospitato su un sito oscurato. Inoltre, si ricordano alcuni strumenti già utilizzati da alcuni *provider:* l'algoritmo di *scaling* multimediale (MDS) per rappresentare e individuare la somiglianza tra siti contenenti espressioni d'odio; il *software* Perspective, che utilizza modelli di apprendimento automatico per rilevare automaticamente insulti, molestie e parole ingiuriose, valutandone il grado di nocività in modo più accurato e veloce; l'algoritmo Edgerank, che valorizza taluni contenuti in base al numero e alla frequenza delle interazioni fra gli utenti; gli algoritmi di Instagram e Twitter che organizzano i contenuti in base alle preferenze degli utenti e non alla cronologia del caricamento; il *software* Content ID con cui YouTube esamina ogni video caricato e lo confronta con un database di file realizzato in accordo con i titolari dei diritti d'autore.

[37] Di Tano (2017), p. 121.

[38] Piraino (2017), p. 155.

[39] Il principio che fa coincidere, nei casi di comunicazioni illecite in rete, il momento in cui il comportamento commesso *online* assume rilevanza giuridica con il momento della "messa a disposizione" dei dati è ricavabile dalla legge tedesca del 22 luglio 1997 sui servizi di informazione e telecomunicazione, così come analizzata da Picotti (1999) pp. 379-380.

online ex art. 595 c. 3 c.p[40].; il reato di diffusione di materiale pedopornografico ex art. 600 *ter* c. 3 c.p.[41]; il reato di istigazione o apologia a commettere reati ex art. 414 c.p., il quale ha assunto particolare rilevanza in materia di lotta contro il terrorismo[42]; nonché, da ultimo, anche il reato di diffusione illecita di immagini o video sessualmente espliciti ex art. 612 *ter* c. 3 c.p.[43].

Occorre precisare che tra gli *hosting provider* qui presi in considerazione si escluderanno le c.d. testate telematiche, le quali si differenziano in virtù del particolare servizio che offrono. Non verrà dunque presa in considerazione la problematica legata all'eventuale applicabilità del regime delineato dall'art. 57 c.p.[44], che non può che escludersi nei casi esaminati, rilevando per i soli servizi *online* di informazione professionale, in virtù dell'equiparabilità funzionale e ontologica degli stessi con la stampa tradizionale[45].

Il regime di responsabilità penale del *provider* in questi casi può distinguersi sulla base della condotta posta in essere dallo stesso. Non costituiscono casi di dubbia ricostruzione dogmatica le ipotesi di condotte commissive – quali quelle di caricamento, condivisione o modifica di dati – integranti reato, poste in essere dallo stesso ISP. Il prestatore di servizi risponderà infatti in quanto autore o co-autore della «messa a disposizione» o della diffusione di contenuti illeciti[46].

La condotta commissiva penalmente rilevante dell'ISP in questi ultimi casi dovrà però consistere nell'immissione (o diffusione) dolosa di dati, a seguito di un vaglio contenutistico degli stessi, non potendo essere ritenuta sufficiente la mera predisposizione dei supporti tecnici di funzionamento della rete, la fornitura degli accessi o la gestione delle piattaforme *online*. Le attività normalmente poste in essere dagli ISP vengono infatti considerate quali giuridicamente legittime e socialmente adeguate, non determinando di per sé il pericolo di verificazione dell'evento offensivo tipico[47].

Di maggiore interesse sono i casi in cui la condotta attribuibile all'intermediario sia di natura omissiva, per la quale egli potrà rispondere o a titolo autonomo secondo il paradigma dell'art. 40 cpv. c.p. o, per combinato disposto con l'art. 110 c.p., a titolo di concorso omissivo nel reato realizzato dall'utente, ipotesi resa particolarmente rilevante dalle nuove tipologie di piattaforme e servizi *online* descritte in precedenza, in cui il ruolo dell'utente è evoluto da passivo ad attivo.

Prima di procedere occorre tuttavia distinguere due differenti ipotesi: la condotta omissiva del prestatore di servizi può infatti consistere, da una parte, nel mancato controllo e censura preventiva del contenuto illecito caricato o diffuso da un proprio utente sulla piattaforma; o, dall'altra parte, nella mancata rimozione dello stesso contenuto, pubblicamente accessibile sul proprio sito *web*. Si profilano dunque due diverse ipotesi di responsabilità: una *ex ante,* operante prima che i dati vengano resi disponibili in rete; una *ex post*, legata alla fase di perdurante disponibilità che caratterizza le informazioni caricate nel *web*.

La prima ipotesi di responsabilità è esclusa dalla maggioranza della giurisprudenza[48] e della dottrina. In particolare, è stato evidenziato come non sarebbe riscontrabile *de jure condito*

[40] La giurisprudenza è conforme nel ritenere Internet, in virtù della sua potente diffusività e pubblicità, elemento compreso nella definizione «*qualsiasi altro mezzo di pubblicità*», legittimando l'applicazione della fattispecie aggravata del reato di diffamazione ex art. 595 c. 3 c.p.. In questo senso: Cass. Pen., sez. V., 27 dicembre 2000, n. 4741, in *Crit. dir.*, 2000, p. 504 ss.; Cass. Pen., sez. I, 15 marzo 2011, n. 16307, in *Guida al diritto,* 2011, 24, p. 71 ss.; Cass. Pen., sez. I, 21 dicembre 2010, in *Cass. pen.,* 2011, p. 4315 ss.; Cass. Pen., sez. V, primo febbraio 2017, n. 4873, in *Foro it.,* 2017, p. 251 ss.. In dottrina: Tabarelli de Fatis (2013), p. 221; Curreli (2017), p. 189-191.

[41] In materia cfr. Picotti (2006), p. 175; Delsignore (2019), p. 446.

[42] Flor (2017), p. 325.

[43] Fattispecie di reato che è stata introdotta nel codice penale dalla L. del 19 luglio 2019, n. 69 (c.d. Codice rosso), approvato definitivamente dal Senato il 17 luglio 2019. Per un'analisi più ampia: Caletti (2018), pp. 63-100.

[44] La giurisprudenza di legittimità ha evidenziato più volte la profonda differenza che sussiste tra testate telematiche *online* e altri siti *web* veicolanti informazioni, come *blog*, *forum* o *social network*. Da ultimo: Cass. pen., 1° febbraio 2017, n. 4873 in *Foro it.,* 2017, n. 4, p. 258 ss.; Cass. pen., 23 gennaio 2019, n. 3148, in *Dir. inf.*, 2018, n. 6, p. 901 ss.

[45] L'evoluzione giurisprudenziale in materia è stata altalenante: (i) in una prima stagione la giurisprudenza di legittimità aveva escluso l'applicabilità dell'art. 57 c.p. ai direttori delle testate telematiche (Cassazione n. 35511 del 1° ottobre 2010 e n. 44126 del 29 novembre); (ii) la pronuncia a Sezioni Unite del 20 luglio 2015, n. 31022, ha optato per la riconducibilità delle testate giornalistiche *online* nella definizione di stampa, estendendo a queste ultime le garanzie costituzionali previste per la carta stampata; (iii) recentemente, con la pronuncia dell'11 gennaio 2019, n. 1275, la Corte ha ritenuto applicabile alle testate telematiche anche il regime delineato dall'art. 57 c.p. (commento a questa ultima pronuncia: Mauri (2019), disponibile al sito: www.penalecontemporaneo.it). Criticamente sull'analogia *in malam partem*: Catullo (2019); Petrini (2017).

[46] Seminara (1997), pp. 96 ss.; Ruggiero (2001), pp. 586-602; Petrini (2004) p. 151; Bartoli (2013), p. 604.

[47] Sieber (1997), pp. 1206-1212; Ruggiero (2001), p. 591.

[48] Corte di giustizia europea, sentenza del 24 novembre 2011, C-70/10, *Scarlet Extended*, EU:C:2011:771; sentenza del 16 febbraio 2012, C-360/10, *SABAM*, EU:C:2012:85; Corte europea dei diritti dell'uomo, 9 marzo 2017, *Pihl c. Svezia*. Nella giurisprudenza nazionale basti richiamare il noto caso Google c. ViviDown, Cass. Pen., Sez. III, 17 dicembre 2013, n. 5107, in *Dir. fam.*, 2014, 2, p. 675 ss.

alcuna fonte giuridica che preveda a carico degli intermediari un obbligo di impedire il reato. Riassumendo brevemente le argomentazioni di questo orientamento[49], ad ostacolare l'attribuzione di una posizione di garanzia in capo a tali soggetti vi sarebbe, in primo luogo, il divieto di imporre un obbligo generale di controllo preventivo stabilito dalla direttiva *e-commerce* e attuato dall'art. 17 D.lgs. n. 70/2003, il quale prevede espressamente che i prestatori di servizi in rete non possano essere assoggettati ad un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite[50]. Un simile obbligo richiederebbe ai *provider* di porre in essere un'attività eccessivamente onerosa, inesigibile e tecnicamente irrealizzabile (un controllo e filtraggio di tutte le informazioni che passano attraverso un *server* sarebbe infatti impraticabile).

In secondo luogo, oltre a non ritenersi configurabile in capo a tali soggetti una posizione di protezione o di controllo[51], essi non disporrebbero nemmeno di specifici poteri impeditivi che consentirebbero loro di impedire o interferire con il realizzarsi della condotta dell'autore del reato.

Seppure quest'ultimo punto susciti qualche perplessità – sulle quali ci si soffermerà in seguito –, in effetti, se si guarda alla responsabilità *ex ante* degli intermediari, gli orientamenti giurisprudenziali, nonché le recenti evoluzioni europee in materia[52], conducono all'esclusione di una sua configurabilità, in particolare per le criticità a cui condurrebbe un filtraggio in entrata dei colossali quantitativi di dati che transitano sui *server* dei diversi prestatori di servizi in rete. L'onerosità che caratterizzerebbe un tale obbligo minerebbe gravemente il diritto alla libertà d'impresa, tutelato dall'art. 16 della Carta di Nizza, facente capo agli ISP[53]. Inoltre, il sistema potrebbe non distinguere sempre le comunicazioni lecite da quelle illecite, rischiando così di compromettere il diritto fondamentale degli utenti alla libertà di ricevere o di comunicare informazioni, tutelato dall'art. 11 della Carta di Nizza[54].

Rimane dunque da verificare la configurabilità della seconda ipotesi sopra individuata, integrante una responsabilità dell'intermediario *ex post*. Ed è proprio questa che suscita il maggior interesse, nonché numerosi dubbi.

Sospendendo per un momento l'analisi della configurazione che questa seconda ipotesi di responsabilità possa assumere secondo i dettami dell'ordinamento penalistico interno, è necessario proseguire tenendo conto del quadro europeo normativo di riferimento che si sta delineando negli ultimi tempi. Dai recenti interventi che coinvolgono la figura degli intermediari a livello europeo emerge infatti come la valorizzazione del ruolo degli ISP nella regolamentazione delle attività nel *Cyberspace* sia sempre più connessa al periodo di perdurante disponibilità di contenuti illeciti in rete.

L'importanza del tema della responsabilità degli intermediari è stata infatti colta dalle istituzioni europee, le quali si sono fatte promotrici di diversi interventi mirati ad un aggiornamento della disciplina (ferma alla direttiva *e-commerce* del 2000) che li riguarda. Anche la figura dell'ISP si inserisce, infatti, all'interno della Strategia per il Mercato Unico Digitale dell'Unione Europea[55], e tale consapevolezza ha condotto a diverse Comunicazioni e Raccomandazioni della Commissione, il cui contenuto tende ad integrare e attualizzare i vari punti irrisolti in tema di responsabilità degli operatori nel *Cyberspace*.

[49] Seminara (1998), pp. 745-774; Seminara (2014), pp.594-605; Manna (2001), pp. 145-151; Ruggiero (2001), pp. 586-602; Petrini (2004); Spagnoletti (2004), pp. 1922-1937; Ingrassia (2012), pp. 47-67.
[50] È da evidenziarsi tuttavia che la tenuta di questo divieto è stata di recente messa in discussione nella domanda di pronuncia pregiudiziale proposta alla Corte di Giustizia europea dall'*Oberster Gerichtshof* il 10 gennaio 2018, nella causa Eva Glawischnig-Piesczek/Facebook Ireland Limited (Causa C-18/18).
[51] Petrini (2004), p. 169; Bartoli (2013), p. 603.
[52] Cfr. paragrafo 3.1.
[53] Corte di giustizia europea, sentenza del 24 novembre 2011, C-70/10, *Scarlet Extended*; sentenza del 16 febbraio 2012, C-360/10, *SABAM*. Sul punto: D'Ambrosio (2012), p. 85; Pollicino (2014), p. 634; Sammarco (2012), p. 301-303; Picotti (2012), p. 2555.
[54] Ibidem.
[55] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Strategia per il mercato unico digitale in Europa*; COM(2015) 192 *final* del 6 maggio 2015.

3.1. *Le recenti evoluzioni in ambito europeo in materia di piattaforme online.*

Prima di indicare i nuovi interventi normativi che sono stati adottati in seno all'Unione Europea, è opportuno operare una ricostruzione delle novità che il tema della responsabilità dei gestori dei servizi in rete ha vissuto negli ultimi anni, sulla base delle diverse Comunicazioni della Commissione al Parlamento europeo e al Consiglio[56].

La prima di queste, come sopra menzionato, è quella riguardante la Strategia per un Mercato Unico Digitale europeo[57], nella quale la Commissione, conformandosi alle risultanze giurisprudenziali sul tema, ribadisce che la sola forma di responsabilità delineabile a carico di questi soggetti è una forma di responsabilità "*ex post*"[58], fondata, in virtù di un dovere di diligenza facente capo agli stessi, sulla mancata rimozione di contenuti illeciti di cui gli intermediari siano effettivamente a conoscenza.

Lo sviluppo di queste premesse ha condotto a due successive Comunicazioni[59], con le quali si è deciso di adottare un approccio settoriale in materia, privilegiando una normazione mirata su alcune questioni specifiche particolarmente sensibili e bisognose di regolamentazione, preservando invece quale base giuridica generale – in quanto ritenuta «sufficientemente flessibile»[60] – la disciplina delineata dalla direttiva del 2000 sul commercio elettronico[61].

Sono state individuate dalla Commissione europea quattro differenti aree di intervento, alle quali hanno fatto seguito altrettante proposte di provvedimenti normativi. La prima riguarda la proliferazione di piattaforme di condivisione di video *online* con contenuti nocivi per minori e istigazioni all'odio, alla quale ha fatto seguito la direttiva sui servizi di media audiovisivi 2018/1808/UE[62]; la seconda riguarda l'utilizzo *online* di contenuti protetti dal diritto d'autore, alla quale ha fatto seguito una nuova direttiva in materia di diritto d'autore[63]; la terza concerne la lotta contro gli abusi sessuali sui minori e la pedopornografia *online*, rispetto alla quale vi è già la direttiva 2011/93/UE[64]; e infine l'ultima area di intervento è rappresentata dalla lotta al *cyber*-terrorismo, cui ha fatto seguito dapprima la direttiva 2017/541/UE[65] e, successivamente, la proposta di Regolamento relativo alla prevenzione della diffusione di contenuti terroristici *online*[66].

In tutte le fonti sopra elencate sono presenti disposizioni che contemplano, direttamente a carico degli ISP o per il tramite dei prossimi interventi nazionali, obblighi giuridici di diverso contenuto e portata. Brevemente, le direttive in materia di contrasto alla pedopornografia ed al terrorismo in rete impongono agli Stati membri di adottare le «*misure necessarie*», senza che queste vengano meglio articolate o spiegate, per assicurare la tempestiva rimozione di pagine web o contenuti *online* che, rispettivamente, consistano in materiale pedopornografico o in pubblica provocazione a commettere un reato di terrorismo, come delineato dall'art. 5 della direttiva 541/2017[67].

[56] Per una esaustiva esposizione sul tema cfr. Montagnani (2018).
[57] Comunicazione della Commissione, *Strategia per il mercato,* cit.
[58] L'ipotesi di una responsabilità *ex ante* è stata esclusa dalla giurisprudenza: Corte di giustizia europea, sentenza del 24 novembre 2011, C-70/10, *Scarlet Extended*, EU:C:2011:771; sentenza del 16 febbraio 2012, C-360/10, *SABAM*, EU:C:2012:85; nella giurisprudenza nazionale basti richiamare il noto caso Google c. ViviDown, Cass. Pen., Sez. III, 17 dicembre 2013, n. 5107, in *Dir. fam.*, 2014, 2, p. 675 ss.
[59] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Le piattaforme* online *e il mercato unico digitale. Opportunità e sfide per l'Europa,* COM(2016)288 *final;* Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Lotta di contenuti illeciti* online. *Verso una maggiore responsabilizzazione delle piattaforme* online, COM(2017)555 *final.*
[60] Nordemann (2017)*:* documento preparato per il *Policy Department* A su richiesta della commissione del Parlamento europeo per il mercato interno e la protezione dei consumatori del Parlamento europeo, 2017, disponibile al sito http://www.europarl.europa.eu.
[61] In questo senso la Commissione nella Comunicazione del 2016: «la Commissione manterrà l'attuale regime di responsabilità relativo agli intermediari, adottando al contempo un approccio di regolamentazione di tipo settoriale».
[62] Direttiva 2018/1808/UE del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.
[63] Direttiva 2019/790/UE del Parlamento Europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.
[64] Direttiva 2011/92/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio.
[65] Direttiva 2017/541/UE del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio.
[66] COM(2018) 640 *final,* nella sua ultima versione approvata a seguito della discussione al Consiglio del 22 maggio 2019.
[67] Art. 25 direttiva 2011/92/UE e art. 21 direttiva 2017/541/UE.

Scende più nel dettaglio la proposta di Regolamento per la prevenzione della diffusione di contenuti terroristici *online*, che coinvolge i prestatori di servizi di *hosting* su diversi fronti. Infatti, essi: (i) laddove siano a conoscenza o siano consapevoli dell'esistenza di contenuti terroristici nei loro servizi, dovranno informare le autorità competenti ed eliminare tali contenuti rapidamente; (ii) dovranno rimuovere i contenuti terroristici o disabilitarne l'accesso il prima possibile, e in ogni caso entro un'ora dal ricevimento di un ordine di rimozione ricevuto dalla competente autorità; (iii) potranno adottare «*misure specifiche*», efficaci, mirate e proporzionate per proteggere i loro servizi dalla diffusione pubblica di contenuti terroristici; (iv) infine dovranno predisporre «*misure di salvaguardia efficaci e appropriate per garantire l'accuratezza e la fondatezza delle decisioni*» di rimozione di contenuti ritenuti terroristici fondate su strumenti automatizzati, misure che consistono in particolare nella previsione di una sorveglianza umana e di meccanismi di verifica dell'adeguatezza della decisione di rimuovere un contenuto o di negarvi l'accesso.

Non altrettanto articolata è la disciplina prevista dalla direttiva in materia di servizi di media audiovisivi, il cui art. 1 introduce l'art. 28 *ter* nella direttiva 2010/13[68], ai sensi del quale gli Stati membri dovranno assicurare, in sede di attuazione, l'adozione – da parte dei fornitori di servizi – di «*misure adeguate*»[69], praticabili e proporzionate, «*per tutelare*» i minori nonché il grande pubblico da contenuti nocivi, che istighino alla violenza e all'odio, ovvero contenuti la cui diffusione integri una fattispecie di reato ai sensi del diritto dell'Unione Europea.

Per quanto riguarda, infine, la direttiva in materia di diritto d'autore, assume importante rilievo la formulazione del molto discusso articolo 13, il quale prevedeva inizialmente – nella versione elaborata dalla Commissione – l'obbligo a carico dei prestatori di servizi, che memorizzano e danno pubblico accesso a grandi quantità di opere o altro materiale caricato dagli utenti, di adottare misure «*volte ad impedire*» che il materiale identificato dai titolari dei diritti fosse messo a disposizione sui propri servizi. Il testo di questo articolo, criticato sotto diversi aspetti, in particolare perché aggravava considerevolmente la posizione dei *provider* e non si coordinava con la disciplina della direttiva *e-commerce*[70], è stato successivamente modificato, per poi diventare l'art. 17 della direttiva approvata.

Tale norma dispone, in primo luogo, al paragrafo 4, che il *provider* che abbia agito in assenza d'autorizzazione dei titolari dei diritti d'autore[71] sia ritenuto responsabile, a meno che non dimostri di: (a) aver fatto il possibile per ottenere l'autorizzazione; (b) aver fatto il possibile, conformemente agli elevati standard industriali di diligenza professionale, per assicurare l'indisponibilità di materiale protetto dal diritto d'autore per il quale i titolari abbiano fornito all'intermediario sufficienti e necessarie informazioni; (c) aver, in ogni caso, agito speditamente, una volta ricevuta una notifica sufficientemente motivata da parte del titolare di diritti, rimuovendo o disabilitando l'accesso al contenuto segnalato, facendo il possibile per prevenire futuri caricamenti di quello stesso contenuto. Nel successivo paragrafo, inoltre, il nuovo testo dell'art. 17 descrive alcuni dei criteri[72] che devono essere tenuti in considerazione nella valutazione delle misure che permettono ai *provider* di andare esenti da responsabilità. È da specificare, infine, che nel sesto paragrafo viene previsto un regime diversificato sulla base della dimensione del *provider*. Infatti, i *content sharing service provider* che prestano servizi nell'Unione Europea da meno di 3 anni e con fatturato annuale sotto i 10 milioni di Euro, per andare esenti da responsabilità, dovranno dimostrare solamente di: (a) aver fatto il possibile per ottenere l'autorizzazione, (b) aver agito speditamente, una volta ricevuta una notifica sufficientemente motivata da parte del titolare di diritti, rimuovendo o disabilitando l'accesso

[68] Direttiva 2010/13/UE del Parlamento europeo e del Consiglio relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi).

[69] Misure che devono essere predisposte in base ai seguenti criteri: natura del contenuto illecito; danno che questo può provocare; categoria dei destinatari che le misure mirano a tutelare; i diversi diritti coinvolti; le dimensioni della piattaforma per la condivisione di video; la natura del servizio offerto dalla piattaforma; infine le misure non possono condurre a forme di controllo *ex ante* o filtraggio dei contenuti nel momento in cui vengono caricati.

[70] Montagnani (2018), pp. 192-198; Colangelo e Maggiolino, (2018), pp. 142-159; Colangelo e Torti (2019), pp. 75-90; Van Vegchel (2018), pp. 1-9.

[71] Secondo quanto previsto dall'art. 3 della direttiva 2001/29/UE (direttiva sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione), la quale dispone che: «*gli Stati membri riconoscono agli autori il diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente*».

[72] Tra gli altri: la tipologia, il pubblico e la dimensione del servizio e la tipologia di opere o altri materiali caricati dagli utenti del servizio; la disponibilità di strumenti adeguati ed efficaci e il relativo costo per i prestatori di servizi.

al contenuto segnalato. Mentre i *service provider* con un numero medio di visitatori mensili di più di 5 milioni (calcolato sulla base dell'anno precedente) dovranno dimostrare anche di aver fatto il possibile per prevenire *futuri* caricamenti del contenuto segnalato.

Una simile formulazione dell'art. 17, che, da una parte, prevede obblighi "attivi" incidenti direttamente sui contenuti ospitati a carico dei *provider* – senza quindi più delegare ad accordi di licenza tra privati il compito di regolamentare le responsabilità in materia –, e, dall'altra, pur utilizzando generiche locuzioni quali «*assicurare l'indisponibilità*», «*agire per rimuovere*» o «*prevenire futuri caricamenti*», cerca di specificare e descrivere maggiormente nel dettaglio l'apparato degli obblighi a carico degli ISP, sembra rappresentare una soluzione più equilibrata, che contempera le diverse istanze soggettive alla stregua di parametri oggettivi.

Si nota in ogni caso una chiara evoluzione tra le più risalenti e le più recenti proposte: dall'utilizzo di formule ampie quali «*misure necessarie*» o «*misure adeguate*», la cui predisposizione ed articolazione sarebbe stata rimessa agli Stati membri, o addirittura ad accordi privati, si sta passando a norme, aventi quali destinatari direttamente i *provider,* che delineano in modo più preciso e dettagliato le misure che è necessario adottino per essere esentati da responsabilità.

Benché dunque l'approccio che le istituzioni europee hanno deciso di adottare sia di tipo settoriale, si evince una linea che accomuna i diversi interventi in materia di responsabilità per la gestione delle piattaforme *online* a livello europeo: l'attenzione viene concentrata sulla necessità di interventi di rimozione, da parte degli intermediari, di contenuti lesivi di interessi e posizioni soggettive giuridicamente rilevanti, con un'urgenza ed un'incisività delle misure che cresce proporzionalmente alla gravità del contenuto illecito, parametrata alla gerarchia dei beni giuridici offesi.

Dal quadro delineato, integrato dalle diverse pronunce giurisprudenziali[73], emerge quindi come ormai consolidata l'esigenza di una maggior responsabilizzazione dei prestatori di servizi in rete[74], in virtù del fondamentale ruolo che essi possono svolgere nel contrasto ai fenomeni criminosi nel *Cyberspace*[75]. E tale esigenza, che trova diversi riscontri anche nello scenario nazionale[76], sarà almeno in parte soddisfatta dalle future norme europee e dalla loro attuazione.

4. La configurabilità di una responsabilità penale ex post in capo agli ISP.

Perché si possa prevedere una responsabilità penale dell'intermediario per omessa rimozione di un contenuto illecito il cui caricamento da parte di un utente costituisce reato, occorre risolvere in prima istanza il nodo problematico relativo alla sussistenza di una posizione di garanzia in capo a questi soggetti.

In merito a questo problema, quella parte di dottrina che non ritiene individuabile in capo agli ISP un obbligo di impedimento dei reati commessi dai propri utenti, non lo ritiene sussistente nemmeno in questa seconda fase. Ai sensi della normativa vigente, vi sarebbero in capo agli ISP (e più precisamente agli *hosting provider*) solamente due obblighi: un mero obbligo di *notice,* «ossia di informazione dell'autorità competente del carattere illecito del contenuto del servizio ospitato»[77], ed un obbligo di *take down,* «ossia di rimozione del dato su richiesta

[73] Cfr. nota n. 29.

[74] Circostanza confermata anche dalla Relazione del Parlamento europeo sulle piattaforme *online* e il mercato unico digitale del 31 maggio 2017, A8-0204/2017; nonché dalla Raccomandazione (UE)2018/334 della Commissione del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali *online*.

[75] Secondo Andrew Shapiro «in democratic societies, those who control the access to information have a responsibility to support the public interest. (…) these gatekeepers must assume an obligation as trustees of the greater good»: cfr. Shapiro (2000), p. 225 così come riportato da Frosio (2018), p. 7.

[76] All'interno della legislazione italiana assumono particolare rilevanza, oltre all'art. 16 D.lgs. n. 70/2003, attuativo della direttiva sull'*e-commerce*, anche gli artt. 14 *ter* e 14 *quater* L. n. 269/1998, introdotti dalla L. n. 38/2006 in attuazione della decisione del Consiglio dell'Unione europea del 29 giugno 2000 relativa alla lotta contro la pedopornografia infantile in Internet, i quali impongono a carico dei fornitori di servizi obblighi di segnalazione di materiale pedopornografico e di filtraggio di siti segnalati dall'organismo competente, senza tuttavia toccare procedure o obblighi di rimozione (sul punto cfr. Torre (2013), pp. 163-191). Così come è da ricordare l'art. 2 c. 3 e 4 del d.l. n. 7/2015, secondo il quale i fornitori di connettività e di servizi in rete hanno l'obbligo, rispettivamente, di inibire l'accesso a siti contenenti materiale terroristico o di rimuovere (entro 48 ore) contenuti terroristici, sempre a seguito di un ordine dell'autorità.

[77] Manna e Di Florio (2019), p. 913.

dell'autorità competente»[78]; ma né l'uno né l'altro potrebbero essere considerati quali fonte di una posizione di garanzia.

Tuttavia, è da sottolineare che, seppur la questione rimanga controversa anche in giurisprudenza[79], in una recente sentenza[80] la Cassazione ha statuito che l'*hosting provider*, di fronte ad una situazione di illiceità "manifesta" dell'altrui condotta, di cui non ne ha impedito la protrazione, mediante la rimozione delle informazioni o la disabilitazione all'accesso, risponderà per fatto proprio colpevole, essendogli rimproverabile una responsabilità commissiva mediante omissione, per avere concorso nel comportamento lesivo altrui. Ed una tale ricostruzione è resa possibile in virtù del fatto che «l'art. 16 d.lgs. n. 70 del 2003 fonda una cd. posizione di garanzia dell'*hosting provider*, che, se per definizione è indispensabile alla stessa originaria perpetrazione dell'illecito del destinatario del servizio, ne diviene giuridicamente responsabile solo dal momento in cui gli possa essere rimproverata l'inerzia nell'impedirne la protrazione»[81].

Muovendo da queste recenti evoluzioni, è inoltre da evidenziare come, secondo una parte minoritaria della dottrina[82], vi siano da tempo disposizioni normative extra-penali che prevedono obblighi specifici in capo agli ISP in materia di reati di diffusione di materiale pedopornografico, in materia di violazioni di diritto d'autore e nello stesso D.lgs. n. 70/2003, capaci di integrare in capo al prestatore di servizi una responsabilità penale per reato omissivo improprio.

Guardando quindi alle novità in ambito europeo, agli sviluppi giurisprudenziali sopra richiamati, uniformemente orientati verso una maggior responsabilizzazione dei prestatori di servizi in rete, nonché alle nuove discipline normative che stanno delineandosi in seno alle istituzioni europee, le quali prefigurano «obblighi giuridici derivanti dal diritto dell'UE e nazionale»[83] ed un «dovere di diligenza»[84] nell'esercizio delle predette attività, non sembra più poter escludersi, in capo agli intermediari, la configurabilità di obblighi giuridicamente rilevanti di attivarsi per impedire reati.

Gli *hosting provider* infatti, in virtù della posizione di "signoria" che rivestono nei confronti dei dati trattati sulle proprie piattaforme[85], «(…) hanno la pesante responsabilità, nei confronti della società, di proteggere gli utenti e il pubblico in generale, nonché prevenire lo sfruttamento dei loro servizi da parte di criminali e altri soggetti coinvolti in attività illegali *online*»[86]. Guardando in effetti al contenuto sostanziale, prima ancora che formale, dell'obbligo giuridico di impedimento, esso trova valido fondamento nello stesso dato di fatto che le vittime del crimine cibernetico – in particolare quando si tratta di reati che si consumano interamente nel *Cyberspace* – si trovano nell'impossibilità di proteggere il bene giuridico leso, dato che un utente non ha possibilità di rimuovere un contenuto illecito una volta che questo è immesso in rete.

Inoltre, la dimensione sociale che ha assunto il *Cyberspace,* strumento attraverso cui si esercitano i più diversi diritti anche fondamentali[87], fa assumere al suo corretto e buon utilizzo il valore di interesse diffuso, la cui tutela può costituire ulteriore ragione per il ricorso

[78] Ibidem.
[79] La V sezione penale della Corte di Cassazione non ha ritenuto configurabile una posizione di garanzia in capo agli ISP in una recente sentenza, la n. 12546 del 20 marzo 2019, (in *Diritto di Internet,* 2019, 3, p. 575 ss.). Di avviso opposto sono invece: Cass. Pen., sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, p. 251 ss.; Cass. civ., sez. I, 19 marzo 2019, n. 7708, in *Dir. inf.*, 2019, 1, p.152 ss. e in *Foro it.,* 2019, 6, I, p. 2045 ss., con nota di Di Ciommo, *Oltre la direttiva 2000/31/CEE, o forse no. La responsabilità dei* provider *di Internet nell'incerta giurisprudenza europea.*
[80] Cass. civ., sez. I, 19 marzo 2019, n. 7708, cit.
[81] Ibidem.
[82] Picotti (1999), pp. 504-506; Picotti (2007), pp. 1207-1208; Flor (2010), pp. 457-460; Flor (2012), pp. 662-693; Torre (2013), pp. 183-191.
[83] Comunicazione della Commissione, *Lotta di contenuti illeciti,* cit., p. 7.
[84] Ibidem.
[85] In base ai dettami della c.d. teoria funzionale, il vincolo che legherebbe il comportamento doveroso dell'ISP sarebbe accompagnato da una situazione di fatto ad esso corrispondente, la quale è caratterizzata da un potere, un dominio, nei confronti del processo di produzione dell'evento dannoso che deriva da un potere di organizzazione o disposizione fondante un relativo obbligo di controllo. Tra i fondamentali riferimenti dottrinali sul punto si richiamano: Sgubbi (1975); Fiandaca (1979); Fiandaca (1983), cc. 27-45; Grasso (1983); Romano (1995), pp. 337-366; Bisori (1997), pp. 1339-1394; Leoncini (1999).
[86] Comunicazione della Commissione, *Lotta di contenuti illeciti,* cit., p. 2. Ai prestatori di servizi in rete, proprio in ragione del significato sociale e culturale che il *Cyberspace* sta assumendo, è quindi riconosciuto un preciso *ruolo economico e sociale*, il quale costituisce spinta per le istituzioni pubbliche, anche europee, all'elaborazione di obblighi positivi di condotta in virtù di quella che è ancora una vocazione solidaristica del potere pubblico.
[87] Il *Cyberspace* ha infatti prodotto «una espansione e diversificazione dei beni giuridici meritevoli di tutela penale»: tra questi basti menzionare la riservatezza informatica nonché la *privacy* in senso stretto. Sul punto cfr. Picotti (2019), p. 52; Picotti (2004), pp. 21-95.

al meccanismo proprio delle fattispecie omissive improprie[88]. L'attivazione della clausola di equivalenza sarebbe per di più legittimata nei casi in cui i beni giuridici oggetto di tutela siano di rango primario, come quelli offesi dalla pedopornografia *online*[89].

Passando al profilo formale, l'attribuzione di una posizione di garanzia in capo agli ISP può trovare riscontro, come già rilevato, nella previsione di obblighi giuridici aventi fonte normativa, primo fra tutti quello delineato, per gli *hosting provider,* dall'art. 16 c. 1 D.lgs. n. 70/2003[90], il quale, tuttavia, andrebbe, oltre che meglio articolato, ritenuto applicabile a tutti gli *hosting provider*.

Secondo un orientamento giurisprudenziale alquanto consolidato[91], infatti, il regime delineato dalla direttiva *e-commerce*, al cui considerando 42 specifica come «*le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi (…) sia di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore non conosce né controlla le informazioni trasmesse o memorizzate*», non sarebbe applicabile ai c.d. *hosting* attivi. Si tratta di quegli intermediari che completano ed arricchiscono con un qualche apporto la fruizione dei contenuti da parte degli utenti[92], elementi idonei a delineare la figura di *hosting provider* attivo, o "indici di interferenza" – da accertare in concreto –, sono, ad esempio, «le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione»[93].

Il persistere su questa posizione conduce, tuttavia, a diversi rischi, dovuti al fatto che la stessa distinzione tra *hosting* attivi e passivi comincia a rivelarsi non sufficientemente efficace. Il prevedere infatti, da una parte, obblighi aventi ad oggetto misure incidenti (sia in termini di rimozione, che di filtraggio) sulle informazioni ospitate dai *provider* e il sostenere, dall'altra, che il regime di esenzione da responsabilità non sia applicabile ai c.d. *hosting* attivi, conduce ad una contraddizione, poiché vi è il rischio che gli stessi obblighi previsti a carico degli ISP rendano quest'ultimi "attivi"[94].

Inoltre, la distinzione tra *hosting* attivi e passivi rivela la propria inadeguatezza se si considera la variabilità a cui è soggetto il parametro dell'attività posta in essere dai singoli intermediari, dal momento che la stessa, strettamente legata all'incessante e veloce sviluppo tecnologico, è in costante e repentino mutamento ed adeguamento[95]. Ancorare una categorizzazione ad un parametro instabile comporta innumerevoli rischi. Pertanto, come è stato sostenuto in dottrina[96], il criterio di valutazione delle responsabilità dovrebbe spostarsi dal campo della soggettività a quello dell'oggettività, non considerando (esclusivamente) le posizioni che soggettivamente assumono i prestatori in virtù delle attività poste in essere – le quali, peraltro, risultano oggi essere per la maggior parte segnate da caratteri "attivi", non esistendo più attività

[88] Ritornando utili e ancora attuali le parole di Giovanni Fiandaca, il quale, riferendosi alla tutela dell'ambiente e della salute del consumatore, sostiene che si tratti di tutelare beni primari «che risultano più esposti alle potenzialità lesive di un sistema produttivo di massa tecnologicamente sempre più complesso ma non altrettanto attrezzato nella prevenzione dei danni». E ancora: «una più efficace difesa contro la moderna fenomenologia dannosa richiede un controllo dell'attività produttiva che finisce con l'incidere in senso restrittivo sul conseguimento di un profitto d'impresa tendenzialmente illimitato», in Fiandaca (1979), p. 56.

[89] D'Ambrosio (2012), pp. 79-81.

[90] Secondo il quale: «*Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: 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*». Oltre agli obblighi di rimozione che stanno nascendo all'interno delle discipline di settore sopra esaminate. Nell'ordinamento nazionale il riferimento va inoltre; agli artt. 14 *ter* e *quater* L. n. 269/1998 (su cui cfr. Picotti (2007), pp. 1196-1211; Salvadori (2007), pp. 1074-1075); nonché agli artt. 156, 156 bis e 163 L. n. 633/1941 (su cui cfr. Flor (2010), pp. 457-460).

[91] Per la giurisprudenza europea cfr. nota n. 20. Nella giurisprudenza nazionale: Corte di Appello di Milano, 7 gennaio 2015, n. 29, in *Dir. Industriale*, 2015, 5, p. 455 ss. con nota di Marvasi; Tribunale di Torino, 07 aprile 2017, n. 1928, in *Diritto & Giustizia*, 3 luglio 2017; Corte d'Appello di Roma, 28 aprile 2017, n. 2833, inedita.

[92] Così come definiti da ultimo da Cass. civ., sez. I, 19 marzo 2019, n. 7708, cit.

[93] Ibidem.

[94] Dove con "attivi" si intendono, secondo quanto si evince dalla giurisprudenza europea (cfr. nota n. 19), quei prestatori di servizi che eseguono attività che gli permettono di controllare o conoscere le informazioni trasmesse o memorizzate, come le attività di posizionamento, indicizzazione ed organizzazione dei contenuti.

[95] In dottrina è stato proposto di ancorare la valutazione giuridica dei fenomeni ad una nuova componente: la "variabile tecnologica", di modo che l'organo giudicante o le parti, nel soddisfare i propri oneri probatori, possano dare una lettura giuridica della situazione coinvolgente le piattaforme sulla base delle tecnologie che esse avevano a disposizione: Piraino (2017), p. 153.

[96] Ivi, p. 197.

di *hosting* autenticamente e meramente passive[97] –, ma concentrando l'attenzione invece sulle «fattispecie concrete nelle quali gli intermediari sono a conoscenza, o avrebbero potuto essere a conoscenza, adottando la diligenza professionale, di elementi di fatto che rivelano in modo manifesto la commissione di un illecito da parte di loro utenti»[98].

Per quanto riguarda l'elemento soggettivo, l'art. 16 D.lgs. 70/2003 richiede che vi sia in capo all'*hosting provider* l'«*effettiva conoscenza*» del contenuto illecito, la quale quindi dovrà tradursi in termini di dolo diretto (escludendosi il dolo eventuale in virtù dell'inciso "*effettiva*"[99]) e, in particolare, in termini di dolo di partecipazione, se si tratti di concorso omissivo nel reato commissivo dell'utente. Anche l'elemento soggettivo risentirà tuttavia dei più recenti sviluppi nella materia. Infatti, da una parte, le nuove attività poste in essere dagli *hosting provider*, caratterizzati dall'esercizio di operazioni sui dati a volte invasive, nonché da maggiori capacità di monitoraggio, analisi e controllo, forniscono al giudice importanti indici sintomatici per l'accertamento dell'elemento soggettivo[100]. Dall'altra parte, la partecipazione attiva degli utenti potrebbe influenzare l'oggetto dello stesso: ad esempio, difficilmente si potrebbe richiedere, ai fini dell'integrazione dell'elemento soggettivo, che il *provider* conosca l'identità del singolo utente che ha caricato il contenuto illecito integrante reato[101].

In conclusione, l'obbligo di impedimento del reato, la cui omissione potrebbe fondare una responsabilità del *provider*, si articolerebbe sulla base del sistema di responsabilità *ex post* fondato sul binomio effettiva conoscenza-mancata rimozione[102], il cui contenuto si potrà ricavare o dalla futura attuazione delle singole norme europee di settore sopra riportate, ovvero da quelle già esistenti, o, infine, dal generale obbligo di rimozione ex art. 16 D.lgs. n. 70/2003, il cui contenuto andrebbe tuttavia meglio articolato.

4.1. *Una disciplina non al passo coi tempi.*

La decisione di non intervenire sulla direttiva *e-commerce* rappresenta un'occasione mancata per dare certezza, coerenza e uniformità alla disciplina della responsabilità dei prestatori di servizi in rete. Benché un approccio settoriale presenti indiscussi i vantaggi – e risulti irrinunciabile data la complessità e diversità delle attività e dei contenuti presenti in rete –, una maggior articolazione della base giuridica comune alle singole materie sembra essere quanto meno opportuna.

La direttiva del 2000 è stata infatti definita da più voci[103] come inadeguata e non più attuale. Il rischio quindi di elaborare dettagliati interventi in settori particolarmente sensibili, mantenendo la direttiva del 2000 quale base normativa comune, in quanto sufficientemente elastica e ampia, è quello di creare uno scenario a macchia di leopardo, in cui vi sono settori dettagliatamente regolamentati ed altri affidati alla discrezionalità dei soggetti privati che vi operano. Una simile deriva priverebbe la regolamentazione delle comunicazioni in Internet di una logica unitaria e di sistema, pretesa invece «dal carattere a-territoriale della rete»[104].

Si possono schematicamente riscontrare due differenti lacune nel regime delineato dagli artt. 12 ss. della direttiva 31/2000: (i) vi è un mancato adeguamento delle diverse definizioni degli ISP, i quali vanno distinti, utilizzando criteri elastici capaci di adeguarsi allo sviluppo tecnologico, sulla base sia delle diverse attività, sia della loro dimensione – in termini di quantità di dati processati, nonché di numero di utenti; (ii) si rende opportuna una maggiore articolazione e specificazione del regime di responsabilità di cui all'art. 14 della direttiva – sulla scorta dei modelli riscontrabili nelle direttive e proposte di direttive sopra esaminate.

[97] Cfr. paragrafo 2 sulle evoluzioni degli strumenti tecnologici a disposizione delle piattaforme.
[98] Piraino (2017), p. 198.
[99] Seminara (1998), p. 101; Flor (2010), p. 463.
[100] D'Ambrosio (2012), pp. 67-93.
[101] In questo senso Cass. Pen., Sez. V, 11 dicembre 2017, n. 13398, in *Foro it.*, 2018, 5, 2, cc. 305-309.
[102] Questo punto dovrebbe essere arricchito da una riflessione sulla portata dell'inciso «*su comunicazione delle autorità competenti*» presente nel testo dell'art. 16 c. 1 lett. b) D.lgs. n. 70/2003, che non è possibile articolare per ragioni di brevità. Sulla natura "superflua" di questo inciso si segnalano in ogni caso: Tribunale civile di Torino, 7 aprile 2017, n. 1928, in *Danno resp.*, 2018, 1, p. 87 ss.; Tribunale civile di Napoli Nord, 3 novembre 2016, in *Giur. it.*, 2017, 3, p. 629 ss.; Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, p. 251 ss.; Corte d'Appello di Milano, 7 gennaio 2015, in *Dir. ind.*, 2015, 5, p. 455 ss.; Tribunale di Roma, 22 gennaio 2010, inedita; Tribunale di Trani, 14 ottobre 2008, in *Danno resp.*, 2009, 1059.
[103] Cfr. nota n. 18.
[104] Petruso (2018), pp. 511-558.

Per quanto riguarda l'art. 14 della direttiva del 2000, le due condizioni d'esenzione delineate andrebbero maggiormente articolate e specificate. Ai sensi della lettera a) (prima condizione), l'ISP deve restare esente da responsabilità se non è «*effettivamente a conoscenza*» del contenuto illecito o di «*fatti o di circostanze che rendono manifesta l'illegalità*» del contenuto. Tale requisito dovrebbe essere rivisto alla luce delle interpretazioni della Corte di Giustizia europea, secondo la quale l'ISP è «effettivamente a conoscenza»[105] quando «viene ad essere, in qualunque modo – sia attraverso la segnalazione da parte di terzi *sia attraverso un esame effettuato di propria iniziativa* –, al corrente di fatti o circostanze in base ai quali un operatore economico diligente[106] avrebbe dovuto constatare l'illiceità dei contenuti dalla stessa ospitati»[107].

Ai sensi della lettera b) dell'art. 14 della direttiva 31/2000 (seconda condizione d'esenzione), l'ISP deve restare esente da responsabilità se, «*non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*». Per quanto riguarda tale ipotesi, la rimozione dovrebbe inserirsi all'interno di un meccanismo attraverso il quale sia più semplice provarne, a seconda dei casi, l'eventuale omissione ed il grado di esigibilità. La formalizzazione di un meccanismo generale di *notice and take/stay down* – non limitato a singoli settori – potrebbe garantire un grado di certezza e di tutela sufficienti. Una tale regolamentazione costituirebbe uno strumento adeguato per un equilibrato contemperamento dei diritti ed interessi dei soggetti interessati[108], nonché eviterebbe agli ISP di assumere il ruolo di censori della rete, con prerogative che sono piuttosto di carattere prettamente pubblicistico.

Partendo dal modello offerto dalla legislazione tedesca con il c.d. *Facebook Act,* in vigore dal 1° ottobre 2017[109], ed accogliendo un orientamento riscontrabile in seno alla Corte europea dei diritti dell'uomo[110], la predisposizione di un meccanismo unico – applicabile quindi in ogni settore – di *notice and take down,* articolato attraverso una diversificazione degli obblighi di rimozione in base al grado di illiceità che il contenuto manifesta, potrebbe orientare un adeguato e uniforme sistema di tutele.

Il pregio di un modello fondato su questo parametro è quello di articolarsi attraverso il coinvolgimento di tutte e tre le soggettività che operano nel *Cyberspace*: coinvolge gli utenti, i quali saranno responsabilizzati attraverso il compito di fornire segnalazioni informate e dettagliate; coinvolge i *provider*, sui quali ricadono i maggiori oneri e obblighi; coinvolge le autorità pubbliche, a cui gli utenti possono rivolgersi e con le quali gli operatori instaurano continui flussi comunicativi per la risoluzione dei casi più problematici.

Vi sono infatti, da un lato, casi in cui determinati contenuti richiedono una diversa quantità di informazioni contestuali, al fine di determinarne la liceità o meno (ad esempio nei casi dubbi di diffamazione o di violazione dei diritti d'autore)[111]: ed in questi casi – prendendo ad esempio la legge tedesca[112] – l'intermediario dovrebbe poter contare sull'intervento delle autorità competenti aventi le prerogative necessarie. Dall'altro lato, vi sono invece ipotesi di contenuti manifestatamente e gravemente illeciti (ad esempio nei casi di contenuti aventi carattere terroristico) la cui rapida od anzi immediata rimozione è particolarmente importante.

Parallelamente, le procedure di cancellazione o sospensione potranno essere completa-

[105] Tradizionalmente si richiama il concetto di *actual knowledge* derivante dal DMCA (cfr. nota n. 76), con il quale si intende in modo univoco un dato cognitivo effettivo cui non può essere equiparata la conoscibilità, neppure se qualificata dalla conoscenza di particolari circostanze: in questo senso De Cata (2010), pp. 99-129.

[106] La cui diligenza andrebbe valutata sulla base dell'adozione dei meccanismi di filtraggio e rimozione di cui l'ISP era nella disponibilità, meccanismi e obblighi che tuttavia andrebbero maggiormente specificati e formalizzati.

[107] Corte di giustizia europea, sentenza del 12 luglio 2011, C-324/09, *L'Oréal,* punti 120 e 121.

[108] Come sottolineato dalla stessa Corte europea dei diritti dell'uomo nelle sentenze: *Magyar Tartalomszolgáltatók Egyesülete and Index.HU ZRT v. Hungary,* ricorso n. 22947/13, sentenza del 2/02/2016; *Delfi AS v. Estonia,* ricorso n. 64569/09, sentenza del 16/06/2015. Sul punto cfr. Falconi (2016), pp. 235-254.

[109] Cfr. nota n. 62.

[110] Corte dei diritti dell'uomo, *Pihl v. Sweden,* ricorso n. 74742/14, sentenza del 9/03/2017; *Magyar Tartalomszolgáltatók Egyesülete and Index.HU ZRT v. Hungary,* ricorso n. 22947/13, sentenza del 2/02/2016; *Delfi AS v. Estonia,* ricorso n. 64569/09, sentenza del 16/06/2015. La differenza delle soluzioni adottate nelle diverse sentenze è dovuta proprio al «principale discrimine della diversa natura dei commenti incriminati», Falconi (2016), p. 251. In dottrina cfr. anche Petruso (2018), pp. 511-558, secondo il quale «si potrebbe pensare che la Corte EDU segnali, sia pure indirettamente, la necessità di un ripensamento delle regole di responsabilità degli intermediari della rete di matrice unitario-europea da incanalarsi non più verso un principio generale, ma verso regole di volta in volta enucleabili in relazione agli specifici contenuti presenti in linea, al loro disvalore, alla loro idoneità a limitare altri diritti fondamentali di pari rango».

[111] Cfr. montagnani e Trapova (2018), p. 304, secondo cui «è altamente dubbio che qualsiasi sistema di filtraggio attualmente in uso, costoso o poco costoso, sia abbastanza sofisticato per tracciare in modo sufficientemente adeguato la linea tra una parodia e un uso illecito o una qualsiasi delle altre eccezioni previste dall'articolo 5 della direttiva 2001/29/CE e nelle diverse leggi sui diritti d'autore degli Stati membri».

[112] Ai sensi del § 3 comma 2 della *NetzDG* tedesca l'ISP può rimettere, entro sette giorni, la decisione sulla natura illecita di un contenuto ad un organo di autoregolamentazione, accreditato da un'autorità amministrativa competente.

mente automatizzate e autonome solo quando non vi siano dubbi sull'illiceità dei contenuti (come accade nel caso di contenuti terroristici e di incitamento al terrorismo)[113]; mentre nei casi di illiceità meno manifesta, si dovrà ricorrere a procedure non completamente automatiche ma contemperate da correttivi, quali l'analisi dei casi controversi da parte di operatori interni all'intermediario nonché la collaborazione con organismi esterni e pubblici aventi le competenze giuridiche, oltre che tecniche, necessarie per definire un contenuto quale illecito.

Ulteriori correttivi, ricavabili dalla giurisprudenza della Corte di giustizia europea[114] e già peraltro utilizzati dalla giurisprudenza nazionale[115], potrebbero consistere, da una parte, nella possibilità lasciata agli intermediari di scegliere le specifiche misure tecniche concrete, attraverso cui conformarsi all'obbligo, secondo quelle che sono le proprie capacità; dall'altra parte, nel concedere l'esenzione da responsabilità all'ISP che dimostri di aver adottato tutte le misure ragionevoli, in quanto mirate ed efficaci alla rimozione dei contenuti illeciti, e che garantiscano la possibilità agli utenti di accedere in modo lecito alle informazioni disponibili a loro destinate.

È opportuno considerare tuttavia che la distinzione fondata sulla "manifesta illeceità" dei contenuti presenti sulle piattaforme *online* potrebbe porre problemi in termini di tassatività e determinatezza. Non è infatti di semplice delimitazione il concetto di «*manifesta illiceità*»[116], il quale dovrebbe essere puntualmente definito dai legislatori attraverso tecniche di richiamo o nuove elaborazioni. Si tratta dunque di possibili evoluzioni che necessitano di ulteriori approfondimenti.

4.2. *Le problematiche poste dalla previsione di una responsabilità* ex post.

La configurabilità di una responsabilità penale dell'intermediario per la mancata rimozione di un contenuto illecito, della cui presenza sulla propria piattaforma il prestatore sia effettivamente a conoscenza, si scontra, tuttavia, con due perplessità da superare: la prima attinente a ragioni di politica criminale; la seconda alla costruzione dogmatica di questa ipotesi.

Sotto il primo profilo, il permettere di ricorrere allo strumento penale contro gli ISP per qualsiasi reato cibernetico commesso dagli utenti potrebbe condurre ad un inasprimento di quello che è stato definito il «dilemma»[117] del *provider*. Il prestatore di servizi, per tutelarsi, potrebbe infatti ricorrere ad una rimozione massiva ed indiscriminata di ogni informazione potenzialmente lesiva di diritti altrui.

La diversificazione degli obblighi (di rimozione, ma anche di filtraggio), che si è cercata di delineare nei precedenti paragrafi, sulla base del tipo e della gravità del contenuto illecito aiuterebbe ad evitare tale deriva, indirizzando e modellando gli interventi che gli operatori privati mettono in pratica in un'ottica di prevenzione e controllo[118].

Sotto il secondo profilo, non può che rilevarsi come la tenuta dogmatica di un simile sistema si fondi su un presupposto: la rimozione dell'informazione illecita da parte dell'ISP

[113] Comunicazione della Commissione, *Lotta ai contenuti illeciti*, cit., p. 15.

[114] Corte di giustizia europea, sentenza del 27 marzo 2014, *UPC Telekabel Wien*, C-314/12, EU:C:2014:192. Secondo la Corte è lecito un provvedimento inibitorio tramite il quale si vieta a un ISP di concedere ai suoi abbonati l'accesso ad un sito web che metta in rete materiali protetti senza il consenso dei titolari dei diritti, purché tale provvedimento: (i) non specifichi quali misure il *provider* deve adottare; (ii) l'*access provider* possa evitare sanzioni per la violazione di tale provvedimento attraverso la prova di aver adottato tutte le misure ragionevoli, le quali non devono privare inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili, ma devono impedire o, almeno, rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e scoraggiare seriamente gli utenti di Internet che ricorrono ai servizi del *provider* dal consultare tali materiali messi a loro disposizione in violazione del diritto di proprietà intellettuale.

[115] Tribunale di Milano, Ord., 11 giugno 2018, in *Quotidiano Giuridico*, 2018.

[116] L'espressione «*contenuto manifestatamente illecito*» contenuta nel paragrafo 3 del *NetzDG* lascia, attraverso una delega in bianco, il compito valutativo a un privato: cfr. Abbondante (2017), p. 66.

[117] De Cata (2010), p. 204; Bartoli (2013), p. 606.

[118] La regolamentazione puntuale del contenuto e delle modalità di esplicazione dell'obbligo giuridico di attivarsi (in questo caso di rimozione) dell'ISP risponderebbe anche alle obiezioni che vengono sollevate dalla dottrina al sistema di responsabilità fondato sull'art. 40 cpv., secondo le quali il regime dei reati omissivi impropri rischierebbe di non rispettare pienamente il principio di legalità da una parte (quando si ricorrere alla teoria funzionale) o il principio di determinatezza dall'altra parte (quando si ricorre alla teoria formale). Per quanto riguarda le discipline normative già oggi esistenti, oltre al modello del c.d. *Facrbook Act* sopra menzionato, è opportuno richiamare l'esempio della legge italiana sul *cyber*-bullismo, L. n. 71/2017.

deve *poter impedire* l'evento o, meglio, il reato, in caso di concorso[119]. Quindi l'omissione, ossia la mancata rimozione del contenuto illecito, deve assumere il valore di contributo causale all'integrazione del reato cibernetico, poiché se così non fosse non sarebbe prospettabile una responsabilità penale dell'intermediario per la realizzazione del reato, rappresentando il suo comportamento un mero *post factum*[120].

La problematica descritta, stimolata da due pronunce della Corte di Cassazione[121], rappresenta l'occasione per una riflessione che investe la costruzione ermeneutica delle categorie penalistiche nell'ambito di una realtà sempre più segnata da processi automatizzati e autonomi. L'individuazione della consumazione dei reati, aventi quale condotta tipica la "messa a disposizione" di un contenuto in rete, nel momento della pubblicazione, sembra infatti non tener conto della complessa fenomenologia che connota i processi tecnologici ed informatici. Il trattamento automatico che segna l'informazione immessa dall'utente in rete – la quale viene "mantenuta", riprodotta, trasmessa, diffusa nel *Cyberspace* e risulta quindi permanentemente reperibile – conduce ad una protrazione, un'espansione ed eventualmente a una riproduzione (non più riconducibile alla sfera di dominio del singolo utente), non tanto degli "effetti", ma piuttosto degli stessi elementi essenziali del fatto tipico[122].

Come ha evidenziato la giurisprudenza[123], la lesione del bene giuridico protetto, in caso di reato cibernetico, non si esaurisce nell'atto della pubblicazione, ma «continua per tutto il tempo di permanenza»[124] dell'informazione in rete.

La fase successiva al caricamento di un determinato contenuto illecito in rete è infatti connotata da un'evidente portata offensiva, connessa alla circostanza che quello stesso contenuto non solo rimane potenzialmente accessibile ad un numero indeterminato di soggetti, ma il suo grado di pubblicità è suscettibile di essere altamente incrementato dalle innumerevoli occasioni e strumenti di condivisione, che permettono ad una stessa informazione di diffondersi illimitatamente in un lasso di tempo rapidissimo.

Vi è dunque una doppia dimensione da considerare. Da una parte, una volta che un determinato contenuto viene caricato nello spazio digitale, esso entra in una «eternità mediatica»[125], capace di influire fortemente, per la sua incontrollabile capacità di pubblicizzazione e diffusione, sull'esperienza dei soggetti che risultano coinvolti. Dall'altra parte, l'architettura del *Cyberspace* permette un «effetto moltiplicatore del messaggio»[126], che, se può essere un beneficio in termini di capacità informativa, conduce inevitabilmente, quando quel messaggio ha carattere illecito, a una moltiplicazione delle potenzialità del danno, rendendo sempre più difficoltosa l'individuazione dei potenzialmente molteplici responsabili[127]. I flussi digitali, infatti, grazie alla persistenza che connota la dimensione temporale dell'informazione, rimangono replicabili all'infinito, offrendo numerose occasioni per comportamenti criminosi: possono essere reindirizzati o inoltrati illegalmente a determinati o indeterminati destinatari, mentre i riceventi hanno la possibilità di eluderli così come di accedervi[128].

Questo aspetto si inserisce all'interno di uno dei rischi che connotano in generale il *Cyberspace,* per come individuati da Bert-Jaap Koops[129]: Internet, secondo l'autore, può infatti "far esplodere" la portata di un crimine, tramutandolo da piccolo inconveniente a grave danno[130]. Quando si tratta, in particolare, di comportamenti criminali sostanziatesi in comunicazioni veicolanti contenuti lesivi di diritti altrui – non solo di carattere diffamatorio, ma pensiamo

[119] Per riferimenti dottrinali cfr. nota n. 108.
[120] Su tale ultima categoria si rimanda a Prosdocimi (1979), pp. 522-553; Prosdocimi (1982).
[121] Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, con nota di Di Ciommo (2017), pp. 252-263; e da ultimo, la discussa Cass. Pen., sez. V, 20 marzo 2019, n. 12546, in *Diritto di Internet,* con nota di Guercia (2019), pp. 576-584.
[122] Picotti (2019), p. 90-96, secondo il quale si può parlare di un «evento cibernetico» capace di includere in sé la fase di prolungamento ed estensione del reato che si consuma nel *Cyberspace*. Sul concetto del "prolungamento" degli elementi essenziali del fatto tipico si segnala anche Brunelli (2000), pp. 28-33.
[123] Cass. Pen., Sez. V, 11 dicembre 2017, n. 13398, in *Foro it.,* 2018, 5, 2, cc. 305-309.
[124] Ibidem.
[125] Cass. pen., sez. V, 11 dicembre 2017, n. 13398, in *Foro it.,* 2018, 5, 2, c. 305 ss.
[126] Ansuàtegui Roig (2017), p. 38.
[127] Ibidem.
[128] Khanna (2016), p. 453, così come riportato da Maestri (2017), p. 16.
[129] Koops (2010), p. 735.
[130] Ibidem. Sottolinea l'autore come una fotografia a contenuto sessuale postata *online* acquisisca una portata globale e permanente o come molestie scritte nel cyberspazio integranti ipotesi di bullismo abbiano un impatto molto maggiore di qualsiasi attacco compiuto a scuola. In questo senso anche: Franks (2010), p. 1-10, la quale sottolinea come la fondamentale differenza che connota il *cyber harassment* non sta nei contenuti ma nelle forme: esso non è infatti limitato nel tempo, dal momento che post, commenti, immagini e video integranti molestie sono spesso impossibili da cancellare, impedendo alla vittima di poter superare e dimenticare l'offesa subita.

anche a tutti i casi di *cyber harassment* o di contenuti a sfondo sessuale diffusi senza il consenso del soggetto raffigurato – occorre tenere in considerazione come «il *Cyberspace* faciliti l'amplificazione, l'accrescimento e la permanenza del danno»[131].

In questa prospettiva, la libera disponibilità di un contenuto illecito nel *web* non costituisce un semplice «fattore di aggravamento delle conseguenze del reato»[132], ma comporta invece una *protrazione* dell'offesa al bene giuridico protetto, la quale può così risultare aggravata e approfondita.

Quale conseguenza di tale assunto, la valutazione del fatto tipico va effettuata con riferimento sia al momento del caricamento del dato *online*, sia al momento successivo della permanenza dello stesso in rete, «allo scopo di accertare se, in relazione ad entrambi i momenti, sia in concreto rimproverabile all'imputato la mancata osservanza di regole di condotta, che, ove rispettate, avrebbero impedito la lesione del bene giuridico protetto dalle norme penali»[133].

Questo rilievo ha condotto la dottrina ad interrogarsi sull'esigenza di delineare categorie dogmatiche nuove, capaci di definire e coordinarsi con la pur tradizionale distinzione tra momento di perfezione formale, che in rete si realizza con la prima messa a disposizione del dato, e momento di consumazione sostanziale, che coincide con l'esaurimento del reato, del suo contenuto di offesa, dovuto ad intervento dell'uomo od a ragioni tecniche[134]. Un tale inquadramento dogmatico condurrebbe a rilevanti conseguenze in tema di responsabilità dell'I-SP a titolo di concorso omissivo nel reato commissivo dell'utente. La condotta di mancata consapevole rimozione del contenuto illecito da parte degli ISP non sarebbe più infatti un comportamento qualificabile come *post factum*, ma diventerebbe penalmente rilevante e base per una responsabilità concorsuale per omesso impedimento, rispondendo alle esigenze politico-criminali, che chiedono una maggiore responsabilizzazione anche penale degli operatori in Internet.

Da tutto quanto sopra emerge, in ogni caso, la necessità di una rimodulazione di talune categorie del diritto penale, le quali continueranno a reggersi sui propri tratti costitutivi tipici, ma dovranno essere pervase da un apporto interdisciplinare, che renda possibile regolare e interpretare correttamente in ambito giuridico penale le dinamiche innescate dalle nuove tecnologie[135].

5. I nuovi scenari aperti dal digitale.

Le peculiarità della natura e del funzionamento della realtà digitale hanno ormai permeato molti aspetti dell'esperienza soggettiva. Il particolare funzionamento delle TIC, che va sempre considerato nelle sue componenti tecniche, non si limita infatti a migliorare i risultati delle prestazioni poste in essere per loro tramite, ma «crea e ri-costruisce interamente la realtà che l'utente è in grado di abitare»[136].

E il risultato dell'azione del digitale che percepiamo, in termini di pervasività, non è altro che il risultato del funzionamento del complesso apparato di procedure tecniche che governando la rete, le cui dinamiche necessitano di inserirsi in forme di regolamentazione che possano dare maggior certezza e garanzia di tutela dei diritti fondamentali degli individui.

La natura della vita nel *web* influenza quindi anche i modelli di responsabilità configurabili in capo ai protagonisti della rete, gli *Internet provider*. La scelta, sempre più confermata dalle numerose pronunce giurisprudenziali, nonché dalle recenti evoluzioni in ambito europeo, di concentrare la costruzione di eventuali ipotesi di responsabilità degli intermediari sulla base delle condotte realizzate nel periodo di persistenza dei dati illeciti in rete si articola proprio a partire dalle specifiche dinamiche tecniche che governano il *Cyberspace*. La particolare natura tecnico-informatica del digitale è portatrice infatti di nuove dimensioni, come quella a cui

[131] Franks (2010), p. 3.
[132] Qualifica in questo senso la persistenza dell'informazione lesiva in rete il Tribunale di Torino, nell'ordinanza del 18 dicembre 2018, così come riportata da Cass. pen., sez. V, 13 maggio 2019, n. 20545, inedita.
[133] Ibidem.
[134] Picotti (2019), p. 90-96.
[135] Sabella (2017), p. 143.
[136] Floridi (2017), p. 78. Questa «migrazione» che caratterizza la nostra epoca è diretta, secondo il filosofo dell'informazione, verso quella che egli definisce come l'«infosfera», realtà informazionale fondata sulla contaminazione tra mondo analogico offline e mondo virtuale online, resa possibile dalla grande potenza che connota l'azione delle TIC. Esse, in quanto capaci di condizionare profondamente gli schemi informazionali che costituiscono l'individuo (noi siamo le nostre informazioni), si caratterizzano infatti per essere potenti tecnologie del sé.

conduce la particolare temporalità delle informazioni, che non possono che avere ricadute sui modelli di responsabilità dei soggetti che ne attivano e gestiscono – in diversi modi e parti – il funzionamento.

Partendo da questa consapevolezza e scendendo nel merito della questione che qui si è cercato di ricostruire, è da sottolineare come l'analisi dell'eventuale configurabilità di un regime di responsabilità penale *ex post* degli ISP debba articolarsi su due linee di indagine, diverse ma in necessario rapporto dialettico l'una con l'altra.

La prima riguarda le peculiarità che caratterizzano i reati cibernetici. Quando i comportamenti posti in essere nel *Cyberspace* integrano ipotesi di reato, occorrerà considerare ed esaminare il ruolo e la rilevanza che le componenti tecnico-informatiche, sempre più connotate da un elevato grado di automazione e autonomia – grazie all'impiego delle complesse metodologie del *machine learning* –, assumono nella configurazione della fattispecie criminosa. Diverse voci della dottrina e della giurisprudenza[137] hanno evidenziato come il fatto tipico costitutivo del reato cibernetico debba necessariamente includere anche le fasi di natura tecnica, sostanziate nei diversi processi di codificazione, decodificazione, trattamento, trasmissione e memorizzazione di dati.

Il grado d'automazione dei processi che elaborano sempre più imponenti quantitativi di dati pone importanti dubbi al penalista, primo fra tutti quello concernente le forme di responsabilità prospettabili nei casi di illeciti realizzati attraverso l'impiego di strumenti automatizzati ed autonomi come quelli regolati da algoritmi, sempre più sofisticati e complessi[138]. Il diritto penale infatti, nei casi e modi opportuni e sempre secondo una logica di *extrema ratio*, non può che essere coinvolto nelle logiche di regolamentazione dei comportamenti realizzati nel *Cyberspace*, soprattutto quando tali comportamenti criminosi vanno ad offendere diritti fondamentali e beni giuridici di primaria importanza, a partire dall'integrità dello sviluppo psico-fisico dei minori.

La seconda linea d'indagine riguarda invece la valorizzazione della previsione di precisi obblighi di notifica e rimozione, ai quali gli intermediari dovranno conformarsi; obblighi diversificati sulla base di diversi parametri – tra i quali, il più rilevante sarà il grado di illiceità del contenuto disponibile in rete così come la sua portata offensiva – aventi ad oggetto l'adozione di misure tecnico-organizzative volte alla individuazione e rimozione di contenuti illeciti in rete. È grazie alla formalizzazione di queste procedure che si avranno gli elementi necessari per l'eventuale costruzione di una responsabilità penale dell'intermediario per concorso omissivo nel reato realizzato dai propri utenti.

La previsione di un simile regime darebbe certezza ai prestatori, i quali avrebbero in mano un efficace strumento per andare esenti da responsabilità, dimostrando di essersi conformati agli obblighi attraverso l'adozione delle misure necessarie.

Un sistema di questo tipo sarebbe, peraltro, facilmente compatibile con la natura degli intermediari, per la maggior parte soggetti privati, che agiscono quali aziende complesse e, quindi, attraverso strutture e logiche organizzative d'impresa[139]. In questo modo si costruirebbero forme di responsabilità basate non solo sulla natura illecita del contenuto ospitato, quanto piuttosto su di una «responsabilità organizzativa»[140] («*responsibility for the design of organizations*»[141]), derivante dall'aver disegnato la piattaforma in modo da non essere in grado di controllare, prevenire o rimuovere la disponibilità di contenuti illeciti accessibili o gestiti dagli utenti[142].

Tale soluzione sembra essere, peraltro, in linea con le posizioni evincibili dalle diverse fonti europee in materia, sia giurisprudenziali che normative, le quali, per quanto siano ancora in una fase di definizione ed assestamento, quando affrontano la complessa tematica della regolamentazione di ciò accade nel *Cyberspace*, convengono nel ritenere necessario e imprescindibile il coinvolgimento degli *Internet provider*.

Questi soggetti rivestono infatti un ruolo sempre più rilevante nella gestione di servizi e

[137] Picotti (2019), p. 35 ss. Cfr. nello stesso senso Picotti (2011), p. 843; Pica (2004), p. 425; Catullo (2003), p. 3963; Cornils (2002), p. 891. In giurisprudenza: Sezioni Unite della Corte di Cassazione in materia di accesso abusivo, sentenza del 24 aprile 2015, n. 17325, in *Dir. pen. e proc.*, 2015, n. 10, p. 1291 ss., con nota di Flor, cfr. in particolare p. 1299.
[138] Sul tema si segnalano: Kroll *et al.* (2016), pp. 1-66; Fioriglio (2015), pp. 113-141; Pagallo (2013).
[139] La scelta di imporre alle imprese l'adozione di opportune misure tecnico-organizzative quale soluzione alle diverse minacce *cyber* richiama, peraltro, il regime di *accountability* delineato dal GDPR, punto che meriterebbe ulteriori approfondimenti.
[140] Montagnani (2018), p. 200, concetto che si sposa con quello di *cooperative responsibility* sopra menzionato (cfr. Helberger *et al.* (2018), pp. 1-14). Nello stesso senso anche montagnani e Trapova (2018), p. 296.
[141] Helberger *et al.* (2018), p. 4.
[142] Montagnani (2018), p. 200.

piattaforme, arrivando ad influenzare la nostra quotidianità, che si articola ormai in gran misura tramite quelle stesse piattaforme. La circostanza per cui circa 30 *corporations* controllano il 90% del traffico mondiale della rete[143], e che procedure d'analisi e rimozione di contenuti illeciti sono diventate "una questione privata", mostrano come il continuare a qualificare gli intermediari quali meri «operatori tecnici e neutrali»[144] sia una via ormai da abbandonare.

Bibliografia

Abbondante, Fulvia (2017): "Il ruolo dei social network nella lotta all'*hate speech*: un'analisi comparata fra l'esperienza statunitense e quella europea", *Informatica e diritto*, 1-2, pp. 41-68

Allegri, Maria Romana (2017): "Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei *social network provider*, per i contenuti prodotti dagli utenti", *Informatica e diritto*, 1-2, pp. 69-112

Amato Mangiameli, Agata (2017): "Tecno-regolazione e diritto. Brevi note su limiti e differenze", *Diritto dell'Informazione e dell'Informatica*, pp. 147-167

Ansuàtegui Roig Francisco Javier (2017): "Libertà di espressione, discorsi d'odio, soggetti vulnerabili: paradigmi e nuove frontiere", *Ars interpretandi,* 1, pp. 29-48

Bartoli, Roberto (2013): "Brevi considerazioni sulla responsabilità penale dell'*Internet Service Provider*", *Diritto penale e processo*, 5, pp. 600-606

Berlingò, Vittoria (2017): "Il fenomeno della *datafication* e la sua giuridicizzazione", *Rivista trimestrale di diritto pubblico*, 4, pp. 641- 675

Bisori, Luca (1997): "L'omesso impedimento del reato altrui nella dottrina e giurisprudenza italiane", Rivista italiana di diritto e procedura penale, pp. 1339-1394

Bocchini, Roberto (2017): "Responsabilità dell'*hosting provider* – la responsabilità di Facebook per la mancata rimozione dei contenuti illeciti", *Giurisprudenza italiana*, pp. 632-643

Brunelli, Daniele (2000): *Il reato portato a conseguenze ulteriori. Problemi di qualificazione giuridica* (Torino, Giappichelli)

Bugiolacchi, Leonardo (2013): "Evoluzione dei servizi di *hosting provider*, conseguenze sul regime di responsabilità e limiti dell'attuale approccio *case by case*", *Responsabilità civile e previdenza*, pp. 1997-2007

Caletti Gian Marco (2018): "*Revenge porn* e tutela penale", *Diritto penale contemporaneo Rivista trimestrale,* 3, pp. 63-100

Cassano, Giuseppe (2017): Stalking*, atti persecutori, cyberbullismo e diritto all'oblio* (Milano, Wolters Kluwer)

Catullo Francesco Giuseppe (2019): "La responsabilità penale del direttore del giornale telematico tra legislatore pigro e giudice intraprendente", *Diritto di Internet,* 1, pp. 173-177

Catullo Francesco Giuseppe, *Diffamazione telematica attraverso la decontestualizzazione dell'identità,* in *Cass. pen*., 2003, pp. 3963-3970.

[143] Maestri, Lex inforamtica *e diritto,* cit., p. 15.
[144] Sul superamento della teoria della neutralità cfr. Allegri, Ubi Social, Ibi Ius, cit., p. 224 s.; Thompson, *Beyond Gatekeeping,* cit., p. 785 ss. il quale si chiede, visto il grande potere che hanno gli intermediari, "censori ufficiosi" della rete che decidono cosa è legale e cosa non lo è: «non è forse peggio per la libertà di espressione, e in definitiva per la legge stessa, se le loro decisioni non vengono controllate? (…) Le risorse e la saggezza che gli intermediari investono nel raggiungere tali decisioni saranno, infatti, tanto potenti quanto gli intermediari stessi. Peggiore sarà l'intermediario, peggiore sarà la decisione; più è potente l'intermediario, più pervasivo sarà l'effetto di quella stessa decisione».

Codiglione, Giorgio Giannone (2017): "La nuova legge tedesca per l'*enforcement* dei diritti sui social media", Diritto dell'Informazione e dell'Informatica, pp. 723-735

Colangelo, Giuseppe (2017): "*Digital Single Market Strategy*, diritto d'autore e responsabilità delle piattaforme *online*", *Analisi Giuridica dell'Economia*, 2, pp. 603-637

Colangelo, Giuseppe e Maggiolino, Mariateresa (2018): "ISP's copyright liability in the EU digital single market strategy", *Informational Journal of Law and Information Technology*, 26, pp. 142-159

Colangelo, Giuseppe e Torti, Valerio (2019): "Copyright, online news publishing and aggregators: a law and economic analysis of the EU reform", *International Journal of Law and Information Technology*, 27, pp. 75-90

Cornils Karin, *Il luogo di commissione dei reati di manifestazione del pensiero in Internet*, in *Diritto dell'Informazione e dell'Informatica,* 2002, n. 4-5, pp. 891-901.

Curreli Carlo (2017): "La diffamazione su facebook, tra diritto sostanziale e profili probatori", *Responsabilità civile e previdenza,* 1, pp. 189-198.

D'Ambrosio, Luca (2012): "Responsabilità degli *Internet provider* e Corte di Giustizia dell'Unione Europea: quali spunti per il sistema penale italiano?" in Luparia, Luca (eds.): Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale* (Milano, Giuffrè), pp. 67-93

D'Ippolito, Guido (2017): "L'esigenza di un nuovo bilanciamento per il diritto d'autore: gli *user generated content* e l'ipotesi di un'eccezione per le opere creative e trasformative", *Cyberspazio e Diritto*, 3, pp. 513-569

De Cata, Marcello (2010): *La responsabilità civile dell'*internet provider (Milano, Giuffrè)

Delsignore Stefano (2019): "La tutela dei minori e la pedopornografia telematica: i rati dell'art. 600 ter c.p"., in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (eds.): *Cybercrime*, (Milano, Utet Giuridica), pp. 374-486

Di Ciommo, Francesco (2010): "Programmi filtro e criteri di imputazione/esonero della responsabilità *online*. A proposito della sentenza Google/ViviDown", *Diritto dell'Informazione e dell'Informatica*, pp. 829-857

Di Ciommo, Francesco (2017): "Responsabilità dell'*Internet hosting provider*, diffamazione a mezzo Facebook e principio di tassatività della norma penale: troppa polvere sotto il tappeto", *Foro Italiano,* pp. 252-263

Di Tano, Francesco (2017): "Prospettive *de jure condendo* sulla responsabilizzazione dei *content provider*", *Informatica e diritto*, 1-2, pp. 113-126

Falconi, Federica (2016): "La responsabilità dell'*Internet service provider* tra libertà di espressione e tutela della reputazione altrui", *La Comunità Internazionale*, 71, 2, pp. 235-254

Fiandaca, Giovanni (1979): *Il reato commissivo mediante omissione* (Milano, Giuffrè)

Fiandaca, Giovanni (1983): "Reati omissivi e responsabilità penale per omissione", *Foro Italiano*, 106, V, cc. 27-45

Fiandaca, Giovanni (2005): "Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale", *Diritto & questioni pubbliche*, 5, pp. 1-23

Finocchiaro, Giusella e Avitabile, Alberto (2017): *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali* (Torino, Giappichelli)

Fioriglio, Gianluigi (2015): "La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici", *Bocconi Legal Papers*, 3, pp. 113-141

Flor Roberto (2015): "I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite", in *Diritto penale e processo,* n. 10, pp. 1296-1309

Flor Roberto (2017): "Cyber-terrorismo e diritto penale in Italia", in Wenin R, Fornasari G. (eds.): *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali,* (Trento, Quaderni Facoltà di Giurisprudenza), pp. 325-362

Flor, Roberto (2010): *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale* (Padova, Cedam)

Flor, Roberto (2012): "*Social network* e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?", *Rivista trimestrale di diritto penale dell'economia,* 3, pp. 647-693

Floridi, Luciano (2015): "Introduction", in Floridi, Luciano (eds.): *The Onlife Manifesto. Being Human in a Hyperconnected Era,* disponibile sul sito https://www.springer.com

Floridi, Luciano (2017): *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (Milano, Raffaello Cortina)

Franks Mary Anne (2010): "The banality of cyber discrimination, or, the eternal recurrence of September", *Denver Law Review Online,* 87, pp. 1-6

Frosio Giancarlo (2018): "Why keep a dog and bark yourself? From intermediary liability to responsibility", *International Journal of Law and Information Technology*, 26, pp. 1-33

Grasso, Giovanni (1983): *Il reato omissivo improprio* (Milano, Giuffrè)

Helberger Natali *et al.* (2018): "Governing online platforms: From contested to cooperative responsibility", *The Information Society*, 34:1, pp. 1-14

Ingrassia, Alex (2012): "Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine? Le responsabilità penali dei *provider* nell'ordinamento italiano", in Luparia, Luca (eds): *Internet* provider *e giustizia penale*, (Milano, Giuffrè)

Khanna Parag (2016): *Connectography: Mapping the Future of Global Civilization*, (Penguin Press, New York)

Koops Bert-Jaap (2010): "The internet and its opportunities for cybercrime", in M. Herzog-Evans (eds.): *Transnational Criminology Manual,* (Wolf Legal Publishers, Nijmegen), pp. 1-12

Kroll, Joshua *et al.* (2016): "Accountable Algorithms", *University of Pennsylvania Law review*, 165, pp. 1-66

Leoncini, Isabella (1999): *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza* (Torino, Giappichelli)

Lessing, Lawrence (2006): *Code 2.0*, disponibile al sito http://codev2.cc/download+remix/Lessig-Codev2.pdf.

Luberto, Mario e Zanetti, Gian Francesco (2008): "Il diritto penale dell'era digitale. Caratteri, concetti e metafore", *Indice penale*, pp. 497-510

Maestri Enrico (2017): "Lex inforamtica *e diritto. Pratiche sociali, sovranità e fonti nel* cyberspazio", *Ars interpretandi,* 1, pp. 15-28

Manna, Adelmo (2001): "Considerazioni sulla responsabilità penale dell'*Internet provider* in tema di pedofilia", *Diritto dell'Informazione e dell'Informatica*, pp. 145-151

Manna, Adelmo e Di Florio Mattia (2019): "Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissione dell'*internet provider*", in Cadoppi, Alberto *et al.* (eds.): *Cybercrime* (Milano, Utet Giuridica), pp. 891-940

Mauri Roberta Eleonora (2019): "Applicabile l'art. 57 c.p. al direttore del quotidiano online: un revirement giurisprudenziale della Cassazione, di problematica compatibilità con il divieto di analogia", *Diritto penale contemporaneo,* disponibile al sito https://www.penalecontemporaneo.it/d/6501-applicabile-lart-57-cp-al-direttore-del-quotidiano-online-un-revirement-giurisprudenziale-della-cas

Mcluhan, Marshall (1967): *Gli strumenti del comunicare* (Milano, Il Saggiatore)

Militello, Vincenza (2014): "L'identità della scienza giuridica penale nell'ordinamento multilivello", *Rivista italiana di diritto e procedura penale*, pp. 106-132

Montagnani, Maria Lillà (2018): *Internet, contenuti illeciti e responsabilità degli intermediari*, (Milano, Egea)

montagnani, Maria Lillà e Trapova, Alina (2018): "Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market", *International Journal of Law and Information Technology*, 26, pp. 294-310

Montanari, Matteo (2017): "La responsabilità delle piattaforme *online* (il caso Rosanna Cantone)", *Diritto dell'Informazione e dell'Informatica*, pp. 254-283

Nordemann, Jan Bernd (2017): "Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?", disponibile al sito http://www.europarl.europa.eu.

Pagallo, Ugo (2013): *The Laws of Robots: Crimes, Contracts, and Torts* (Berlino, Springer)

Pascuzzi, Giovanni (2016): *Il diritto dell'era digitale* (Bologna, Il Mulino)

Petrini Davide (2017): "Diffamazione online: offesa recata con "altro mezzo di pubblicità?" o col mezzo della stampa?", *Diritto penale e processo,* 11, pp. 1485-1492

Petrini, Daniele (2004): *La responsabilità penale per i reati via internet* (Napoli, Jovene)

Petruso, Rosario (2018): "Responsabilità delle piattaforme *online*, oscuramento di siti web e libertà di espressione nella giurisprudenza della Corte europea dei diritti dell'uomo", *Diritto dell'Informazione e dell'Informatica*, pp. 511-558

Pica Giorgio (2004): "Internet (diritto penale)", voce in *Digesto delle discipline penalistiche*, *Aggiornamento* (Utet, Milano), pp. 425-483

Picotti Lorenzo (2006): "Sub art. 600 ter III comma c.p.", in Cadoppi Alberto (eds.): *Commentario delle norme contro la violenza sessuale e contro la pedofilia,* IV ed., (Padova, Cedam), pp. 175-212

Picotti, Lorenzo (1999): "La responsabilità penale dei *service providers* in Italia", *Diritto penale e processo*, 4, pp. 501-506

Picotti, Lorenzo (2004): "Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati," in Picotti, Lorenzo (eds.): *Il diritto penale dell'informatica nell'epoca di Internet* (Padova, Cedam)

Picotti, Lorenzo (2007): "La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in Internet (L. 6 febbraio 2006, n. 38) (Parte seconda)", *Studium Iuris*, 11, pp. 1196-1211

Picotti, Lorenzo (2011): "La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee", *Rivista trimestrale di diritto penale dell'economia*, 4, pp. 827-864

Picotti, Lorenzo (2012): "I diritti fondamentali nell'uso ed abuso dei *social network*. Aspetti penali", *Giurisprudenza di merito*, pp. 2522-2547

Picotti, Lorenzo (2019): "Diritto penale e tecnologie informatiche: una visione d'insieme", in Cadoppi, Alberto *et al.* (eds.): *Cybercrime* (Milano, Utet Giuridica), pp. 33-96

Piraino, Fabrizio (2017): "Spunti per una rilettura della disciplina giuridica degli *internet service provider*", *Annali italiani del diritto d'autore*, 1, pp. 152-200

Pollicino Oreste (2014): "Internet nella giurisprudenza delle Corti europee: prove di dialogo?", *Diritto dell' Unione eu*ropea, 3, pp. 601 ss.

Pollicino, Oreste (2014): "Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli *Internet service provider*", disponibile al sito: http://www.giurcost.org

Prosdocimi, Salvatore (1979): "Osservazioni sull'aggravamento o tentato aggravamento delle conseguenze del delitto commesso", *Rivista italiana di diritto e procedura penale*, pp. 522-553

Prosdocimi, Salvatore (1982), *Profili penali del postfatto*, (Milano, Giuffrè)

Romano, Mario (1995): *Commentario sistematico del codice penale*, *sub. Art. 40* (Milano, Giuffrè), pp. 337-366

Ruggiero, Francesco (2001): "Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'*internet provider*", *Giurisprudenza di merito*, pp. 586-602

Sabella, Pietro (2017): "Il fenomeno del *cybercrime* nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali", *Informatica e diritto*, 26, 1-2, pp. 139-176

Salvadori, Ivan (2007): "I presupposti della responsabilità penale del *blogger* per gli scritti offensivi pubblicati su un blog da lui gestito", *Giurisprudenza di merito,* pp. 1069-1079

Salvadori, Ivan (2011): "La normativa penale della stampa non è applicabile, *de jure condito*, ai giornali telematici", *Cassazione penale,* pp. 2982-2994

Sammarco Pieremilio (2012): "Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio", *Diritto dell'Informazione e dell'Informatica,* 2, pp. 297-305

Scardino, Francesco (2015): "Una analisi del "Decreto antiterrorismo" Commento a d.l. 18 febbraio 2015, n. 7", *Rassegna Avvocatura dello Stato*, 2, pp. 215-239

Scialdone, Mario (2013): "Il nuovo ruolo degli utenti nella generazione di contenuti creativi", *Diritto Mercato Tecnologia*, 4, pp. 8-19

Seminara, Sergio (1997): "La pirateria su Internet e il diritto penale", *Rivista trimestrale di diritto penale dell'economia*, 3, pp. 71-114

Seminara, Sergio (1998): "La responsabilità penale degli operatori su internet", *Diritto dell'Informazione e dell'Informatica*, pp. 745-774

Seminara, Sergio (2014): "Internet (diritto penale)", *Enciclopedia del Diritto, Annali VII* (Milano, Giuffrè), pp. 567-606

Sgubbi, Filippo (1975): *Responsabilità penale per omesso impedimento dell'evento* (Padova, Cedam)

Shapiro, Andrew (2000): *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know* (New York, PublicAffairs)

Sieber, Ulrich (1997), "Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di Internet (II parte)", *Rivista trimestrale di diritto penale dell'economia*, 4, pp. 1193-1232

Smythe, Dallas (2009): "On the Audience Commodity and Its Work", in Durham, Meenakshi Gigi e Kellner, Douglas (eds.): *Media and Cultural Studies* (Malden, Blackweel), pp. 230-256

Spagnoletti, Valeria (2004): "La responsabilità del *provider* per i contenuti illeciti di Internet", *Giurisprudenza di merito*, 9, pp. 1922-1937

Tabarelli de Fatis Stefania (2013): "Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione *online*", in Picotti Lorenzo (eds.): *Tutela penale della persona e nuove tecnologie,* (Padova, Cedam), pp. 193-239

Torre, Valeria (2013): "Sulla responsabilità penale del *service provider* e la definizione del comportamento esigibile alla luce delle norme contro la pedopornografia", in Picotti, Lorenzo (eds.): *Tutela penale della persona e nuove tecnologie*, (Padova, Cedam), pp. 163-191

Tosi, Emilio (2017): "Contrasti giurisprudenziali in materia di responsabilità civile degli *hosting provider* – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti", *Rivista di Diritto Industriale*, 1, pp. 75-122

Van Vegchel, Jan (2018): "European Council's amended proposal for a Directive on copyright in the Digital Single Market; is it enough to ward off threat to press freedom?", *SSRN Electronic Journal*, pp. 1-9

Vigliar, Salvatore (2018): "Pirate Bay: evoluzione del concetto di comunicazione al pubblico o nuova frontiera della responsabilità delle piattaforme telematiche?", *Diritto dell'Informazione e dell'Informatica*, pp. 108-122

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

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