Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

EMANUELE LA ROSA*

LA PROTEZIONE DEI BENI GIURIDICI NEL MERCATO UNICO DIGITALE TRA ISTANZE SECURITARIE E TUTELA DEI DIRITTI**

SOMMARIO: 1. Premessa. – 2. Il "contrasto ai contenuti illeciti su internet": profili generali. – 3. La rimozione dei contenuti illeciti. – 4. Il ruolo dell'*Internet service provider* e i suoi profili di responsabilità penale. 5. Considerazioni conclusive.

1. *Premessa*

Il Cyberspazio ha determinato, da un lato, l'emersione di nuovi beni giuridici meritevoli di tutela penale (fede pubblica nei documenti informatici e telematici; integrità e sicurezza dei dati e dei sistemi informatici), e, dall'altro, l'occasione di sperimentare nuove modalità di aggressione a beni giuridici tradizionali (diffamazione, truffa, istigazione a delinquere e apologia di reato, diffusione di materiale pedopornografico o di opere dell'ingegno coperte da diritto d'autore)[1]. Due prospettive destinate talvolta a intersecarsi: si pensi a tutti quei fenomeni "criminali" che ruotano intorno al concetto di "identità digitale" (basti pensare, per esempio, ai frequentissimi casi di *phishing*)[2].

Ma se è vero, da un lato, che quello digitale è un ambiente di coltura particolarmente fertile per la proliferazione di fenomeni criminali, e, dall'altro, che la possibilità di sfruttare

* Ricercatore di Diritto penale, Dipartimento di Giurisprudenza ed Economia, Università "Mediterranea" di Reggio Calabria.

** Testo rielaborato, con l'aggiunta di note, delle relazione presentata il 16 maggio 2016 al Convegno *Un mercato unico digitale per l'Europa tra sfide globali e soluzioni locali*, organizzato dal Centro di Documentazione Europea e dal Dipartimento di Scienze Politiche e Sociali dell'Università di Messina.

[1] L. PICOTTI, *Sistema dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, pp. 53 ss., tripartisce i beni giuridici offesi dai reati informatici in beni "comuni" offesi via internet, beni giuridici analoghi a quelli tradizionali radicati su nuovi "oggetti" passivi della condotta e beni giuridici nuovi nati dall'informatica.

[2] In argomento, tra gli altri, G. MALGIERI, *La nuova fattispecie di "indebito utilizzo dell'identità digitale"*, in *Diritto penale contemporaneo* (*www.penalecontemporaneo.it*), 2015, p. 143 ss.; ID., *Il furto di "identità digitale": una tutela patrimoniale della personalità*, in D. FALCINELLI, R. FLOR, S. MARCOLINI (a cura di), *La giustizia penale nella "rete"*, Milano, 2015, p. 37 ss.; V. DI LEMBO, *La disciplina del* "phishing", in *Rivista penale*, 2013, p. 892 ss.; R. FLOR, Phishing, identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Rivista italiana di diritto e procedura penale*, 2007, pp. 899 ss.

al massimo le potenzialità del "mercato unico digitale" passano (anche) dalla creazione di un clima di sicurezza e di fiducia da parte degli utenti (consumatori, operatori economici, prestatori di servizi di connettività), ben si comprende la necessità di interventi che – attenuando (se non neutralizzando) i rischi connessi alla realizzazione di condotte illecite – contribuiscano a creare quell'ambiente favorevole allo sviluppo della rete e allo sfruttamento massimo delle sue potenzialità.

Non è un caso che la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europea e al Comitato delle regioni, del 6 maggio 2015, avente a oggetto la *«Strategia per il mercato unico digitale in Europa»*[3], dopo aver sottolineato le pesanti perdite economiche derivanti dalla diffusione dei reati informatici e telematici, che *«si traducono in interruzioni del servizio o in violazioni dei diritti fondamentali»*, individua nella rimozione di questi effetti una delle linee di intervento da attuare per *«ripristinare la fiducia dei cittadini nelle attività* on line*»*.

Al fine di perseguire un siffatto obiettivo, servono innanzitutto interventi di tipo tecnico, volti a rafforzare la sicurezza delle reti e dei sistemi di informazione[4]. Questi, però, esulano dal tema e dai limiti del presente contributo, che è, invece, è dedicato ad alcuni profili di carattere giuridico (e giuridico penale, in particolare) relativi al c.d. "contrasto ai contenuti illeciti su internet".

2. *Il "contrasto ai contenuti illeciti su internet": profili generali*

Parlare di "contrasto ai contenuti illeciti su internet" significa sollevare un duplice ordine di questioni:

a) Innanzi tutto, si tratta di stabilire quando un "contenuto" possa definirsi "illecito" (e – per quel che qui interessa più da vicino – quando possa ritenersi penalmente rilevante).
b) In secondo luogo, occorre valutate quali strumenti attivare, sul piano repressivo e (soprattutto) su quello preventivo, per evitare la veicolazione, tramite internet, di questi contenuti illeciti.

Nell'affrontare entrambe le questioni, tenuto conto della prospettiva sovranazionale e delle esigenze di un "mercato unico digitale", ci troviamo a dover fare i conti, da un lato, con la "territorialità" che contraddistingue i sistemi penali, e, dall'altro, con le specificità del "fenomeno digitale"(prima fra tutte proprio quella di sfuggire ad una precisa dimensione spaziale).

Internet, infatti, ignora i confini territoriali, mentre gli ordinamenti giuridici necessitano ontologicamente di uno spazio sul quale esercitare la propria sovranità esclusiva. Non è certo un caso che uno dei problemi più discussi in tema di reati informatici o telematici sia quello dell'individuazione del *locus commissi delicti*, con gli inevitabili riflessi sulla giurisdi-

[3] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europea e al Comitato delle regioni del 6 maggio 2015 *concernente la strategia per il mercato unico digitale in Europa*, in *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52015DC0192*.

[4] In questa direzione si muove la Proposta di Direttiva del Parlamento europeo e del Consiglio *recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione* (COM/2013/048 final), in *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52013PC0048*.

zione e sulla competenza[5]. Sono problemi ben lontani dall'essere stati affrontati e risolti in maniera efficace. Vero che molti strumenti normativi sovranazionali contengono norme specifiche in materia di giurisdizione, competenza e cooperazione giudiziaria tra gli Stati. Nondimeno le distanze tra i singoli ordinamenti restano notevoli; e sono differenze non solo di dettaglio, ma investono gli stessi principi ispiratori della disciplina positiva: basti pensare che ci sono ordinamenti (come quello italiano) ancora legati (almeno in prevalenza) al principio di territorialità, mentre altri (tra cui quello tedesco) mostrano una maggiore apertura verso il principio di personalità. Da qui la necessità di un ulteriore sforzo di armonizzazione.

Ma il cyberspazio non è solo un mondo "deterritorializzato"; è anche molto altro. Alla delocalizzazione delle risorse (anche grazie alla nuova dimensione del *cloud* e delle strutture del *web*) si affianca, per esempio, la «detemporalizzazione delle attività»[6], che possono essere pianificate e svolte attraverso operazioni automatizzate e programmate dall'autore (tanto da far venir meno l'esigenza di un "collegamento" o "contatto fisico" tra persona e sistema informatico). Senza trascurare, infine, la possibilità di agire in una dimensione che – prescindendo dal contatto fisico o personale tra i soggetti – riesce a garantire l'anonimato, così allentando quei freni che, di norma, inibiscono la realizzazione di condotte illecite[7].

Sono proprio queste caratteristiche del mezzo – con il carico di potenzialità criminali e criminogene che ne derivano – a "mettere in crisi" alcune tradizionali categorie penalistiche (a partire dal concetto di "azione", vera e propria architrave della dommatica penale) e a spingere nella direzione di una armonizzazione (se non di una unificazione) dell'intervento repressivo.

Una disarmonia legislativa, unita alla "deterritorializzazione" di *internet*, del resto, non può che indurre fenomeni di "dislocazione" dei fenomeni criminali. Se, infatti, le legislazioni penali nazionali sono disomogenee, si accentuerà la tendenza a realizzare il comportamento illecito in un contesto spaziale presidiato da un ordinamento nelle cui pieghe si annidano maggiori spazi di liceità, ben sapendo che, in ogni caso, gli effetti lesivi si diffonderanno al di là di quei confini territoriali. Del resto, è proprio la sua "a-territorialità", il suo essere un "non luogo", che rende il *cyberspace* un moltiplicatore delle possibilità di comunicazione e di scambio tra le persone e «permette la più ampia diffusione del pensiero umano, consentendo di raggiungere, potenzialmente, miliardi di destinatari»[8].

Il primo strumento per contrastare la diffusione di contenuti illeciti tramite *internet* è, quindi, la creazione di ambienti normativi (il più possibile) omogenei.

Del resto, tale esigenza di un intervento penale coordinato a livello transnazionale – esigenza che è alla base anche della Convenzione del Consiglio d'Europa sulla Criminalità informatica, stipulata a Budapest il 23 novembre 2001 e ratificata con l. 18 marzo 2008, n. 48[9] – è tale che l'art. 83 TFUE ha inserito la "criminalità informatica" tra i fenomeni cri-

---

[5] Per un quadro delle questioni sul tappeto, v. S. SEMINARA, Locus commissi delicti, *giurisdizione e competenza nel cyberspazio*, relazione al Convegno "*Presi nella rete – Analisi e contrasto della criminalità informatica*", Pavia, 23 novembre 2012 (http://informaticagiuridica.unipv.it/convegni/2012/SEMINARA%2023-11-2012.pdf).

[6] R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Diritto penale contemporaneo* (*www.penalecontemporaneo.it*), 2012, p. 1 s.

[7] Sul tema dell'anonimato in *internet*, A. MAGGIOPINTO-M. IASELLI (a cura di), *Sicurezza e anonimato in rete. Profili giuridici e tecnologici della navigazione anonima*, Milano, 2005.

[8] A. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, in *Diritto penale contemporaneo* (*www.penalecontemporaneo.it*), 2012, p. 4.

[9] Sul tema, per tutti, L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, p. 700 ss.

minosi che per la loro gravità e per la loro dimensione transnazionale, «derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni», legittimano una competenza penale dell'Unione europea.

Una competenza che ha avuto già modo di concretizzarsi in una serie di iniziative. Si pensi, per esempio, alla Direttiva 2011/93/UE, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI del Consiglio, del 13 dicembre 2011. O, ancora, alla direttiva 2013/40/UE del Parlamento e del Consiglio europeo del 12 agosto 2013, relativa agli attacchi contro i sistemi d'informazione, che sostituisce la decisione quadro 2005/222/GAI. Senza trascurare le iniziative nel settore della tutela del diritto di autore e della proprietà intellettuale.

Sono tutti strumenti normativi che vanno nella direzione della armonizzazione dell'intervento penale, rendendo meno appetibile la ricerca di spazi territoriali dove i rischi penali connessi alla realizzazione di reati informatici o digitali risultino azzerati o ridotti. Una tendenza apprezzabile e meritevole di un ulteriore rafforzamento.

3. *La rimozione dei contenuti illeciti*

La predisposizione di una disciplina penale omogenea è solo uno dei tasselli della strategia globale di contrasto nei confronti dei comportamenti che si traducono nella diffusione di contenuti illeciti nella rete.

Il problema è che non basta accertare che è stato commesso un reato e punirne il responsabile, atteso che i risultati della condotta criminosa – proprio per la particolare natura della realtà digitale – rischiano di permanere per sempre nel *cyberspace*, moltiplicando a dismisura la portata lesiva del fatto. È, quindi, necessario individuare strumenti tecnici e giuridici atti a evitare questo perdurare dell'offesa a tempo indefinito, evitando ogni ulteriore diffusione di contenuti *contra ius*.

Un sistema sperimentato dal legislatore è – accanto al sequestro e all'oscuramento dei siti – quello che si basa sull'istituzione di una *black list* di siti internet veicolo di contenuti illeciti, sull'ordine di rimozione di questi ultimi e sulla predisposizione di procedure volte a inibire l'accesso alle pagine *web* ivi segnalate.

Non è questa la sede per entrare approfonditamente nel merito dell'effettiva efficacia di simili misure[10]. Basti segnalare alcune possibili ragioni di perplessità. Innanzi tutto, il rischio che i meccanismi di blocco vengano aggirati da sistemi informatici avanzati e che veicolino la diffusione attraverso il c.d. *deep net* o il c.d. *dark web*[11], rendendo più difficile ogni ulteriore attività investigativa. In secondo luogo, a depotenziare gli effetti di un ordine di rimozione di contenuti illeciti o dell'inibizione all'accesso degli stessi è la circostanza che i soggetti tenuti a eseguirlo si trovano spesso in uno Stato diverso da quello dell'Autorità che lo ha emanato. A onor del vero, però, i limiti derivanti dalla transnazionalità del fenomeno

[10] In argomento, L. V. BERRUTI, Black list *e blocco dei contenuti* web *illeciti: dal contrasto alla pedopornografia al* cyber terrorism, in *www.legislazionepenale.eu*, 15 gennaio 2016, p. 1 ss., e S. SIGNORATO, *Le misure di contrasto in rete al terrorismo:* black list, *inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio internet*, in R. E. KOSTORIS-F. VIGANÒ (a cura di), *Il nuovo "pacchetto" antiterrorismo*, Torino, 2015, p. 55 ss.

[11] La differenza tra *deep web* e *dark web* è che il primo include siti non indicizzati nei motori di ricerca, ma comunque accessibili direttamente tramite un normale *browser*, mentre l'accesso al secondo richiede il possesso di particolari *software* in grado di mantenere segreta l'identità dell'utente.

digitale possono essere superati – lo si accennava sopra – attraverso una politica di armonizzazione delle misure e di cooperazione giudiziaria; mentre eventuali spinte verso un "interramento" dei contenuti digitali illeciti – per quanto insidiosi – rappresentano comunque un risultato apprezzabile, atteso che la diffusione verrebbe comunque ristretta a soggetti dotati di elevate conoscenze informatiche o già inseriti in contesti relazionali di tipo criminale. Il vero punto dolente – rispetto al quale non sono oggi ipotizzabili soluzioni realmente definitive – è dato, semmai, dalla estrema facilità con cui i contenuti (anche illeciti) possono essere riprodotti e rimessi nella rete; il che rischia di trasformare ogni azione di contrasto come una frustrante "fatica di Sisifo". Questa, però, non sembra una ragione sufficiente per rinunziare a qualsiasi tentativo d'intervento.

È il caso, a questo punto, di formulare qualche considerazione di carattere generale sulla compatibilità di queste misure con il quadro dei principi costituzionali e sovranazionali.

A livello europeo indicazioni interessanti si possono ricavare dall'art. 25 della Direttiva 2011/93/UE in materia di *lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile*[12]. Tale disposizione prevede che gli Stati adottino le misure necessarie per assicurare la tempestiva rimozione delle pagine *web* contenenti immagini pedopornografiche, che abbiano *host* nel proprio territorio, ma con la possibilità di richiedere la stessa misura anche al di fuori dei limiti territoriali. Gli Stati, inoltre, possono adottare misure di blocco di accesso degli utenti alle pagine *web* contenenti materiali pedopornografici. La direttiva dispone che tale strumento deve essere predisposto attraverso una procedura trasparente e prevedere delle *safeguards* per garantire che la restrizione sia limitata, necessaria e proporzionata, nonché il diritto dell'utente a essere informato del motivo della restrizione. Tale procedura dovrebbe altresì garantire il ricorso giudiziario avverso al provvedimento che dispone il blocco dell'accesso.

La norma in oggetto, quindi, si mostra consapevole della delicatezza della materia, nella quale si annida il rischio di introdurre forme surrettizie di censura o di imbavagliamento, con conseguente illegittima compressione della libertà di espressione, riconosciuta dall'art. 21 Cost., oltre che, a livello sovranazionale, dall'art. 10 CEDU e dall'art. 19 della Dichiarazione universale dei diritti dell'uomo[13].

La libertà di accesso alla rete, del resto, non è altro che una «proiezione nel nuovo universo digitale della tradizionale libertà di espressione»[14]; con la conseguenza che ad essa deve essere riconosciuta quella tutela rafforzata propria di ogni libertà costituzionale. Ciò significa: in primo luogo, che sia il legislatore a delimitare con precisione i presupposti e le condizioni che consentano una limitazione alla fruizione (totale o parziale) di determinati contenuti digitali; in secondo luogo, la gestione di suddette "limitazioni" deve essere affidate a organi giurisdizionali, prevedendo garanzie procedimentali che assicurino l'effettivo esercizio dei diritti di difesa.

Se è vero, quindi, che la rimozione dei contenuti illeciti per essere efficace deve anche essere tempestiva, questa esigenza non può tradursi in un'eccessiva compressione delle garanzie.

In breve, le istanze securitarie sottese al contrasto di contenuti illeciti – tanto di matrice terroristica, quanto di natura pedopornografica, senza trascurare quelli aggressivi di ul-

[12] R. FLOR, *Lotta alla "criminalità informatica"*, cit., p. 6.
[13] Sul punto, v. S. SIGNORATO, *Le misure*, cit., p. 62, nota 18.
[14] O. POLLICINO, Copyright versus freedom of speech *nell'era digitale*, in *Giur. it.*, 2011, p. 1968.

teriori beni giuridici – devono fare i conti con un molteplice fascio di interessi (anche contrapposti) che vengono in rilevo e con i quali devono essere bilanciati.

L'individuazione di un ragionevole punto di equilibrio tra esigenze di sicurezza e rispetto delle garanzie, peraltro, non può prescindere dalla "materia" che si va ad affrontare. Il quadro diventa ancora più chiaro sol che si consideri la vaghezza che connota la portata semantica dell'espressione "contrasto ai contenuti illeciti su internet". Essa è tale da abbracciare una fenomenologia assai variegata, tanto sul piano degli interessi tutelati, quanto su quello della loro portata lesiva: dalla pedo-pornografia alla propaganda e al proselitismo terroristico, passando per le violazioni del diritto d'autore o della *privacy* e la diffamazione *on line*. Ne consegue che anche gli strumenti giuridici di intervento possono non essere omogenei, come pure le tecniche di bilanciamento: ci saranno settori nei quali le esigenze securitarie potranno avere la prevalenza su quelle delle garanzie (senza, ovviamente, comportarne il sacrificio assoluto); in altri casi, una compressione (seppur minima) della tutela di fondamentali diritti individuali non potrà in alcun modo essere giustificata. Per esempio, proprio in materia di violazioni del diritto d'autore l'orientamento della Corte di Giustizia è chiaramente orientato verso il mantenimento di un livello di garanzie particolarmente elevato[15].

Illuminante per comprendere le difficoltà di questo bilanciamento è il raffronto tra la disciplina prevista in materia di pedo-pornografia e quella introdotta in tema di contrasto al terrorismo.

Nel primo caso, un sistema di rimozione dei contenuti illeciti sia già previsto dall'art. 14 *quater* della l. 3 agosto 1998, n. 269 (introdotto dalla l. 6 febbraio 2006, n. 38). In forza di tale disposizione, i fornitori di connettività alla rete Internet «sono obbligati a utilizzare gli strumenti di filtraggio e le relative soluzioni tecnologiche conformi ai requisiti individuati con decreto del Ministro delle comunicazioni, di concerto con il Ministro per l'innovazione e le tecnologie e sentite le associazioni maggiormente rappresentative dei fornitori di connettività della rete Internet». Ciò al fine di impedire l'accesso ai siti segnalati dal Centro nazionale per il contrasto della pedo-pornografia sulla rete Internet. È quindi affidato a tale organismo, istituito presso il Ministero dell'Interno, il compito di raccogliere tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente l'utilizzo sessuale dei minori avvalendosi della rete Internet e di altre reti di comunicazione, nonché i gestori e gli eventuali beneficiari dei relativi pagamenti.

Si tratta, in estrema sintesi, di una procedura affidata alla gestione di organi amministrativi, con un limitato controllo giurisdizionale; quindi non del tutto in linea con le indicazioni del summenzionato art. 25 della Direttiva 2011/93/UE.

Già all'indomani dell'adozione di questa disciplina si era prospettata la possibilità di adattare questi meccanismi alle esigenze repressive e repressive di attività criminose che trovano nel *cyberspace* l'ambiente esclusivo ed ideale di manifestazione.

Ciò è puntualmente avvenuto quando si è trattato di individuare gli strumenti più idonei a fronteggiare il dilagante fenomeno del terrorismo internazionale e la sua capacità di sfruttare le potenzialità del mondo digitale. Il meccanismo previsto dall'art. 14 *quater* l. 3

[15] Particolarmente interessante, in tal senso, la sentenza della Corte di Giustizia dell'Unione Europea del 4 ottobre 2011, cause C-403/08 e C-429/08, *FA Premier League c. QC Leisure* e *Karen Murphy c. Media Protection Services Limited*, in *www.eur-lex.europa.eu*. In argomento, B. CARUSO, *I diritti di ritrasmissione degli eventi sportivi tra tutela della proprietà intellettuale e diritto antitrust: considerazioni a margine della recente sentenza "Murphy"*, in *Concorrenza e mercato*, 2013, p. 801 ss.; L. LONGHI, *La sentenza Murphy: le licenze di ritrasmissione degli incontri di calcio tra diritti di privativa e tutela della concorrenza*, in *Rivista di diritto ed economia dello sport*, 2011, p. 37 ss.

agosto 1998, n. 269, è stato ripreso – sia pure con significative differenze e con finalità marcatamente preventiva – nei commi 2, 3 e 4 dell'art. 2 d.l. 18 febbraio 2015, n. 7 (convertito con l. 17 aprile 2015, n. 43), recante «misure urgenti per il contrasto al terrorismo, anche di matrice internazionale»[16]. In base a tali disposizioni, i fornitori di connettività devono, in seguito a provvedimento dell'autorità giudiziaria procedente, inibire l'accesso alle pagine *web* inserite nella *black list*, e su disposizione del pubblico ministero, rimuovere i contenuti illeciti direttamente riconducibili alle fattispecie in materia di terrorismo.

Anche un superficiale raffronto tra i due fenomeni – pedo-pornografia e proselitismo terroristico – lascia emergere quella certa difficoltà – cui facevo cenno – a ricondurre i meccanismi di contrasto ai contenuti illeciti su internet entro una cornice unitaria. Ciò anche da un punto di vista parzialmente diverso da quello sopra considerato (relativo alla maggiore o minore accettabilità di una limitazione delle garanzie in funzione della diffusività e carica lesiva della condotta considerata).

La valutazione della natura pedo-pornografica di un sito poggia su un sostrato oggettivo – vieppiù dopo che il legislatore, nel recepire la Convenzione del Consiglio d'Europa sulla protezione dei minori dallo sfruttamento e dagli abusi sessuali, stipulata a Lanzarote il 25 ottobre 2007, ha tentato di fornire una definizione del fenomeno[17]. Ciò rende meno "problematica" (per quanto sempre discutibile) la scelta di affidare l'individuazione dei contenuti oggetto delle procedure di rimozione o di inibizione ad un organo non giurisdizionale. Viceversa, il discrimine tra libera manifestazione del pensiero e proselitismo radicale appare più problematico, sottendendo una valutazione squisitamente valoriale tutt'altro che semplice; una valutazione che deve tener conto di svariati fattori: qualità e stile dello scritto, incisività e persuasività dello stesso, idoneità a suscitare un certo grado di condivisione. Non solo: a volte la pericolosità è palese, altre è implicita ed indiretta. Senza considerare come le valutazioni non possano che essere condizionate anche dalla direzione offensiva delle condotte (arruolamento, sostegno ideologico, *etc.*). Una problematicità che è già stata sperimentata "sul campo" in sede di applicazione del delitto di Istigazione a delinquere (art. 414 c.p.)[18].

Alla luce di siffatte premesse, oltre che di quanto detto in ordine alla necessità di garantire un controllo imparziale sulle scelte in ordine alla rimozione di contenuti illeciti o all'inibizione dell'accesso agli stessi, la soluzione adottata col il d.l. 18 febbraio 2015, n. 7, non può ritenersi pienamente appagante. Certo, va riconosciuto come la disciplina in questione, prevedendo un maggior coinvolgimento degli organi giurisdizionali, rappresenti un sicuro avanzamento sul piano delle garanzie (rispetto ai meccanismi previsti in materia di contrasto alla pornografia minorile). Allo stesso modo, non va taciuto il fatto che il legisla-

16 Per un esame di tale normativa, L. V. BERRUTI, Black list, cit., p. 1 ss. ; S. SIGNORATO, *Le misure*, cit., p. 55 ss.

17 La l. 1 ottobre 2012, n. 172, ha introdotto l'art. 600 *ter*, co. VII, c.p., che definisce la "pornografia minorile" come «ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali». In argomento, F. BACCO, *Tutela dei minori contro lo sfruttamento sessuale*, in D. PULITANÒ (a cura di), *Diritto penale. Parte speciale*, I, *Tutela penale della persona*, Torino, 2014, p. 335 ss.; A. PECCIOLI, *La riforma dei reati di prostituzione minorile e pedopornografia*, in *Dir. pen. proc.*, 2013, p. 142 ss.; G. FIANDACA-E. MUSCO, *Diritto penale. Parte speciale. I delitti contro la persona*, Bologna, 2013, p. 168 ss.; B. ROMANO, *Delitti contro la sfera sessuale della persona*, Padova, 2013, p. 211 ss.

18 Basti vedere le diverse valutazioni del PM e del Tribunale di primo grado in merito alla vicenda dello scrittore Erri De Luca: sentenza del Tribunale di Torino del 19 ottobre 2015, n. 4573, in *Diritto penale contemporaneo* (*www.penalecontemporaneo.it*), 8 febbraio 2016, con nota di S. ZIRULIA, *"La Tav va sabotata": Erri De Luca assolto dall'accusa di istigazione a delinquere.*

tore italiano si sia mosso in controtendenza rispetto ad altre esperienze europee più cedevoli sul piano delle garanzie, tanto da ammettere che «venga disposta in via meramente amministrativa, e senza alcun controllo giurisdizionale, persino la misura della rimozione da internet dei contenuti che, seppure non illeciti, appaiano comunque ricollegabili ad una attività a matrice terroristica»[19].

Restano, però, irrisolte talune criticità. Vero che l'art. 2 prevede che il divieto di accesso a determinati siti (comma 3) e la rimozione dei contenuti relativi ad illecite attività terroristiche (comma 4) siano disposti, rispettivamente, dall'autorità giudiziaria procedente (formula riferibile tanto al Giudice quanto al Pubblico Ministero) e dal Pubblico Ministero, e quindi prevede un ruolo attivo dell'autorità giudiziaria; ma gli ampi poteri riconosciuti al magistrato inquirente, fanno sì che, di norma, la misura preventiva sia adottata da un organo "non terzo" che non può garantire quel giudizio "imparziale" di cui si diceva. Non solo: l'aggiornamento dell'elenco dei siti utilizzati per le attività e le condotte di cui agli artt. 270 *bis* e 270 *sexies* c.p., pure espressamente subordinata all'esigenza di svolgere determinate attività investigative o preventive[20], è affidata a un'entità amministrativa (l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione[21]), che raccoglie le segnalazioni effettuate dagli organi di polizia giudiziaria. L'ordine, impartito ai fornitori di connettività, di inibire l'accesso ai siti inseriti nel suddetto elenco, quindi, proviene sì dall'autorità giudiziaria procedente, ma le scelte di quest'ultima sono condizionate da un'attività istruttoria condotta da organi non giurisdizionali. Non pare, infatti, prospettabile – alla luce della disciplina prevista dall'art. 2, co. II, d.l. 18 febbraio 2015, n. 7– alcun controllo prodromico all'inserimento nella *black list* circa l'attualità e la concretezza della pericolosità del sito *web*. Né può considerarsi sufficiente allo scopo quella forma di controllo *a posteriori* rappresentato dalla Relazione annuale che il Ministro dell'interno deve stilare ai sensi dell'art. 113 l. 1 aprile 1981, n. 121, al cui interno un'apposita sezione deve essere dedicata ai provvedimenti adottati ex art. 2, co. II, d.l. 18 febbraio 2015, n. 7.

Con riferimento alla rimozione dei contenuti illeciti, di cui al quarto comma, meritevole di apprezzamento risulta, invece, la limitazione ai soli contenuti illeciti accessibili al pubblico[22]. Si è quindi scelto di non seguire la strada di un invasivo monitoraggio delle comunicazioni private. Una scelta che sottende una logica di stretta funzionalità della limitazione della libertà rispetto all'azione di contrasto al terrorismo.

Volendo concludere sul punto, il raffronto tra le misure adottate in materia di pedopornografia e quelle introdotte nell'azione di contrasto al terrorismo lascia emergere alcune contraddizioni. Se la maggiore diffusività e pervasività del secondo fenomeno potrebbe far apparire tollerabile un qualche sacrificio delle garanzie a vantaggio della sicurezza, la maggiore difficoltà a determinare i confini tra condotte illecite e libertà di manifestazione del pensiero non può che esigere un elevato livello di garanzie, che si traduce anche nella necessità di affidare la gestione delle procedure ad organi "terzi".

---

[19] S. SIGNORATO, *Le misure*, cit., p. 63.

[20] Il riferimento è: a) alle operazioni sotto copertura che si traducano in attività illecite, ma coperte da causa di giustificazione (*ex* art. 9, co. I, lett. b. e co. II, l. 16 marzo 2006, n. 146), svolte nell'ambito di specifiche operazioni di polizia, esclusivamente al fine di acquisire elementi di prova circa i delitti commessi con finalità di terrorismo o di eversione; b) alle attività di prevenzione e di repressione delle attività terroristiche o di agevolazione del terrorismo condotte con mezzi informatici, previste dall'art. 7 bis, co. II, d.l. 27 luglio 2005, n. 144, convertito con l. 31 luglio 2005, n. 155.

[21] Si tratta di una formula che va intesa come riferibile al Servizio di polizia postale e delle telecomunicazioni. In argomento, anche per ulteriori riferimenti, S. SIGNORATO, *Le misure*, cit., p. 61 s.

[22] Per un esame critico S. SIGNORATO, *Le misure*, cit., p. 66.

4. *Il ruolo dell'*Internet service provider *e i suoi profili di responsabilità penale*

La rimozione dei contenuti illeciti dalla rete non può che vedere, con un ruolo da protagonista, il prestatore di servizi di connettività, il c.d. *Internet service provider* (*ISP*), essendo questi il soggetto materialmente in grado di portare a compimento questa attività. Non ci può essere efficace azione di contrasto che non passi da una qualche forma di coinvolgimento di questi soggetti.

Dal punto di vista penalistico – avuto particolare riguardo all'ordinamento interno – questo ruolo dell'*ISP* costringe a fare i conti con le problematiche tipiche delle forme di manifestazione del reato, rese ancora più complesse dalle peculiari caratteristiche di questo soggetto e dell'attività da lui svolte. Quest'ultime si svolgono, come detto, in una sorta di "non luogo"; sono realizzate da un soggetto non necessariamente "persona fisica" e involgono nel loro momento applicativo un difficile bilanciamento tra diritti fondamentali non compiutamente pre-imposto dal legislatore. Il rischio è quello di affidare questo bilanciamento ad un soggetto privato e non – come dovrebbe essere – ad un'autorità pubblica imparziale.

Non è certo questa la sede per affrontare le innumerevoli implicazioni tecnico-giuridiche e dommatiche poste da tale materia[23]. Basti qui evidenziare come le soluzioni da offrire ai problemi sin qui presi in esame – e le implicazioni tecnico-giuridiche che ne derivano – sono condizionate (anche) dal ruolo che si intende attribuire all'*ISP* e quindi al bilanciamento che si intende assicurare ai diritti fondamentali in conflitto:

a) se si ritiene che l'*ISP* debba essere considerato alla stregua degli altri comuni utenti di internet (senza particolari doveri nei confronti della collettività, né obblighi di controllo), esso risponderà solo dei reati di cui è autore o concorrente attivo;
b) se, invece, si ritiene che l'*ISP* debba assumere il ruolo sociale di "controllore", di "filtro" preventivo, esso risponderà come garante della tutela dei diritti dei terzi, secondo il paradigma del reato omissivo improprio.

Ora mi pare di poter affermare che entrambi questi approcci, nel loro estremismo, appaiono poco convincenti. In particolare, la prima impostazione sottovaluta il contributo che l'*internet provider* offre alla diffusione di contenuti digitali illeciti, non soltanto nella fase iniziale della loro immissione nella rete, quanto in quella, successiva, della loro permanenza *on line*. La seconda impostazione, d'altro canto, finisce col pretendere dal *provider* una condotta "censoria" che – stante la natura del *cyberspazio* – pare francamente inesigibile[24]. Senza

[23] Nella vasta letteratura in argomento, si segnalano, tra gli altri, S. SEMINARA, *La responsabilità penale degli operatori su internet*, in *Il diritto dell'informazione e dell'informatica*, 1998, p. 745 ss.; L. PICOTTI, *La responsabilità penale del* service provider *in internet*, in *Dir. pen. proc.*, 1999, p. 501 ss.; D. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, 2004, p. 121 ss.; R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet*, Milano, 2010, 2010, p. 417 ss.; D. DE NATALE, *Responsabilità penale dell'*internet service provider *per omesso impedimento e per concorso nel reato di pedopornografia*, in G. GRASSO-L. PICOTTI-R. SICURELLA (a cura di), L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona, Milano, 2011, p. 295 ss.; A. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., p. 1 ss.

[24] Significativo il c.d. caso *Google vs. Vivi Down*, relativo alla pubblicazione di un filmato sull'*host* Google Video, ritraente un ragazzo disabile umiliato da alcuni compagni all'interno di un edificio scolastico, con sottofondo anche di frasi ingiuriose nei confronti dell'associazione *Vivi Down*. In tutti e tre i gradi di giudizio, si è esclusa la responsabilità dei manager di Google per non aver impedito il delitto di diffamazione nei confronti del minore e dell'associazione (artt. 40 cpv. e 595 c.p.); esclusione fondata tanto su ragioni giuridiche (la direttiva sul commercio elettronico, attuata nel nostro ordinamento con il d.lgs. 9 aprile 2003, n. 70, esclude un

considerare che è quanto meno «inquietante l'idea di un privato che verrebbe incaricato di esercitare una sorta di censura per conto dell'ordinamento, avendone i mezzi tecnici, ma non quelli "culturali" per realizzarla»[25].

Il discorso, però, muta quando si discute di un'eventuale collaborazione dell'*ISP*, tanto nella forma della denuncia all'autorità giudiziaria, quanto in quella della rimozione dei contenuti illeciti e della inibizione all'accesso degli utenti a siti di contenuto illecito. Qui specifici obblighi a carico dell'*ISP* sono configurabili, e configurati da diverse fonti normative[26]. Alla base vi è l'idea che l'*ISP* sia una sorta di "tutore dell'ordine"; idea che, a sua volta, sottende la convinzione – del tutto condivisibile – che nel bilanciamento la libertà di espressione dell'utente e la tutela dei terzi de della società, la prima possa essere limitata solo parzialmente (vuoi riducendo o escludendo l'anonimato degli utenti, vuoi implementando strategie di repressione dei reati commessi che coinvolgano solo *ex post* l'*ISP*)

Semmai, è interessante riflettere su cosa succeda nel caso in cui, per esempio, l'*ISP* disattenda questo obbligo di collaborazione, violando le norme che gli impongono, su ri-

---

obbligo di vigilanza sul contenuto dei materiali diffusi dagli utenti), quanto su considerazioni di tipo fattuale (l'impossibilità in concreto di filtrare *ex ante* i contenuti degli *uploader*). La sentenza d'appello e quella della Corte di cassazione hanno altresì escluso una responsabilità dei *providers* per mancato impedimento del reato previsto dall'art. 167 d.lgs. 30 giugno 2003, n. 196. In particolare, la sentenza della Cassazione penale, Sez. III, del 17 dicembre 2013, n. 5107, ha stabilito che: a) non è possibile attribuire all'*host provider* un obbligo di impedire i reati commessi dagli utenti, mancando una norma che fondi l'obbligo giuridico; b) le attività compiute dall'*host provider* sui materiali caricati dagli utenti (che non importino un intervento sul contenuto degli stessi o la loro conoscenza) non fanno venir meno le limitazioni di responsabilità previste dagli artt. 16 e 17 d.lgs. 9 aprile 2003, n. 70; c) solo dal momento della conoscenza dell'illiceità dei contenuti pubblicati dagli utenti può ipotizzarsi una responsabilità del *provider* per illecito trattamento dei dati realizzata dagli *uploaders*.
Per una ricostruzione della vicenda, A. INGRASSIA, *La sentenza della Cassazione sul caso Google*, in *Diritto penale contemporaneo* (*www.penalecontemporaneo.it*), 6 febbraio 2014.

[25] G. FORNASARI, *Il ruolo della esigibilità nella definizione della responsabilità penale del provider*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica*, cit., p. 431.

[26] Oltre alle disposizioni, prese in considerazione nel testo, in materia di pedo-pornografia e contrasto al terrorismo, vengono in rilievo, per esempio, gli articoli 14, co. III; 15, co. II; e 16, co. III, d.lgs. 9 aprile 2003, n. 70 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico); questi attribuiscono all'autorità giudiziaria o a quella amministrativa avente funzioni di vigilanza il potere di esigere, anche in via d'urgenza, che il prestatore dei servizi informatici «impedisca o ponga fine alle violazioni commesse» nell'ambito delle attività, rispettivamente, di *mere conduit*, *caching* e *hosting*. Anche l'art. 163 l. 22 aprile 1941, n. 633 (*Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*), prevede la possibilità dell'autorità giudiziaria di inibire qualsiasi attività che costituisca violazione del diritto d'autore: un provvedimento che vede tra i possibili destinatari l'*ISP*. Ancora, l'art. 1, co. VI, d.l. 22 marzo 2004, n. 72 (convertito con l. 21 maggio 2004, n. 128), prevede un obbligo d'informazione (nei confronti del Dipartimento della pubblica sicurezza del Ministero dell'interno ovvero dell'autorità giudiziaria) a carico dei «fornitori di connettività e di servizi che abbiano avuto effettiva conoscenza della presenza di contenuti idonei a realizzare le fattispecie di cui all'articolo 171ter, co. II, lett. a bis), e all'articolo 174 ter, co. II bis e II ter, della legge 22 aprile 1941, n. 633, e successive modificazioni». Una parte della dottrina si spinge a fondare su tali disposizioni un generale obbligo d'impedimento di reati altrui. Così, L. PICOTTI, *La responsabilità penale*, cit., p. 504; ID., *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet (l. 6 febbraio 2006, n. 38) (parte seconda)*, in *Studium iuris*, 2007, p. 1207 ss. Aderisce a tale tesi, che traspone in relazione alla tutela del diritto d'autore e, più in generale, al d.lgs. 9 aprile 2003, n. 70, R. FLOR, *Tutela penale e autotutela tecnologica*, cit., p. 457 ss. Le norme richiamate da questi Autori, però, o si traducono in un obbligo di segnalazione del fatto illecito all'autorità privo di poteri impeditivi e perciò inidoneo a fondare una posizione di garanzia, oppure impongono un obbligo di attivarsi al fine di ridurre gli effetti disvoluti di reati già realizzati: in nessuno dei due casi siamo in presenza di un generalizzato obbligo di impedimento di reati altrui. Per questa conclusione, A. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., p. 33 ss.

chiesta dell'autorità competente, di rimuovere dai propri server il materiale illecito memorizzato e di inibire l'accesso a siti contenenti tali dati o informazioni.

In taluni casi, è lo stesso legislatore a predisporre le conseguenze sanzionatorie dell'inadempimento. Il citato art. 14 *quater* l. 3 agosto 1998, n. 269, per esempio, prevede una sanzione amministrativa pecuniaria da euro 50.000 a euro 250.000, irrogata dal Ministero delle comunicazioni. Analogamente dispone l'art. 1, co. VII, d.l. 22 marzo 2004, n. 72 (convertito con l. 21 maggio 2004, n. 128).

La questione è cosa succeda nel caso di "silenzio" del legislatore in merito ad eventuali conseguenze giuridiche per la mancata collaborazione.

Ipotesi che ricorre, per esempio, in relazione alle previsioni dell'art. 2 d.l. 18 febbraio 2015, n. 7[27]; fatta salva la sola sanzione dell'interdizione dell'accesso al dominio internet (da eseguirsi con le forme e le modalità stabilite per il sequestro preventivo *ex* art. 321 c.p.p.), per il caso di mancato adempimento all'ordine di rimozione dei contenuti illeciti disposto dal Pubblico Ministero[28].

Si potrebbe ipotizzare – almeno in taluni casi – un'applicazione del delitto di Inosservanza dolosa di un provvedimento del giudice (art. 388 c.p.)[29]; ovviamente limitatamente a quelle ipotesi in cui l'ordine di rimozione del contenuto illecito o di inibizione dell'accesso a determinati siti o contenuti provenga da un'autorità giudiziaria.

Sennonché, a parte che – come detto – tale soluzione non sarebbe percorribile laddove la "gestione" del procedimento sia affidata ad organi non giudiziari, a rendere non applicabile l'art. 388 c.p. è il difetto, nel caso di specie, di quella componente fraudolenta della condotta richiesta dalla norma incriminatrice (atti simulati o fraudolenti); componente, che secondo una giurisprudenza pressoché unanime, non può rinvenirsi nella mera violazione dell'obbligo imposto dal giudice[30].

---

[27] Sulla non applicabilità della disciplina sanzionatoria prevista dall'art. 14 *quater* l. 269 del 1998, G. AMATO, *Ampliati controllo e monitoraggio dei siti informatici*, in *Guida al diritto*, 2015, 19, p. 88.

[28] La norma in oggetto non chiariva se il sequestro fosse applicabile alle testate giornalistiche telematiche e ai loro siti *web*. Il tema è quello della possibilità di riconoscere alla stampa *on line* dello statuto giuridico garantito dall'art. 21, co. III, Cost., il quale prevede una riserva di legge e di giurisdizione come antidoto a forme arbitrarie di censura. Dopo alcune oscillazioni giurisprudenziali, la questione è stata affrontata e risolta dalle Sezioni Unite della Corte di Cassazione, che: da un lato, ha stabilito il principio secondo cui il sequestro preventivo di una pagina *web* può essere disposto anche imponendo al fornitore di servizi in rete di rendere inaccessibile la risorsa; dall'altro, ha precisato che il giornale *on line* registrato, al pari di quello cartaceo, non può essere sottoposto a sequestro preventivo, salvo nelle ipotesi specificatamente previste dall'art. 21 Cost. Così, Cass. pen., Sez. Un., 29 gennaio 2015, n. 31022, in *Diritto penale contemporaneo* (*www.penalecontemporaneo.it*), 9 marzo 2016, con nota di C. MELZI D'ERIL, *Contrordine compagni: le Sezioni unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate giornalistiche* on line *registrate*. In generale, sull'applicazione dello statuto sulla stampa a realtà giornalistiche telematiche, M. BASSINI, *La disciplina penale della stampa alla prova di Internet: avanzamenti e arresti nella dialettica giurisprudenziale da una prospettiva costituzionale*, in D. FALCINELLI, R. FLOR, S. MARCOLINI (a cura di), *La giustizia penale nella "rete"*, cit., p. 9 ss. A fronte di questo arresto giurisprudenziale e della mancata previsione di deroghe espresse da parte dell'art. 2 d.l. 18 febbraio 2015, n. 7 – deroghe che risulterebbero, peraltro, di dubbia legittimità costituzionale – si deve ritenere che la disciplina speciale in materia di prevenzione e repressione del terrorismo non è applicabile ai contenuti illeciti ospitati da testate giornalistiche alla *on line*. In argomento, S. SIGNORATO, *Le misure*, cit., p. 70.

[29] V. SPAGNOLETTI, *La responsabilità del provider per i contenuti illeciti in internet*, in *Giur. mer.*, 2004, p. 1929 s.

[30] Così, per tutte, la sentenza della Cassazione penale, sez. VI, del 13 febbraio 2006, n. 17543, in *Rivista penale*, 2007, p. 180; la sentenza della Cassazione penale, sez. VI, del 19 settembre 1989, Marino, in Cass. pen., 1991, p. 556. A. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., p. 38. In generale, sull'art. 388 c.p., tra gli altri, L. BISORI, *La mancata esecuzione dolosa di provvedimenti del giudice*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Trattato di diritto penale. Parte speciale*, III, Torino, 2008, p. 673 ss.; A. ABBAGNANO TRIONE,

Più adatta al caso di specie potrebbe risultare, semmai, la previsione dell'art. 650 c.p., che punisce, anche a titolo colposo, l'inosservanza di provvedimenti dell'autorità emessi, come nel caso di specie, per ragioni di giustizia o di sicurezza pubblica: in relazione a tale contravvenzione già il mancato adempimento dell'ordine dato dall'autorità ai sensi delle predette disposizioni integrerebbe il fatto tipico.

Sennonché l'accoglimento di una simile soluzione rischia di determinare delle discutibili (se non irrazionali) conseguenze sul piano sistematico. Non si comprende, infatti, perché l'*ISP* che, per esempio, non rimuova pagine dal contenuto diffamatorio debba essere sanzionato penalmente ex art. 650 c.p., mentre nel caso in cui l'omesso filtraggio a lui rimproverabile permetta agli utenti della rete di accedere e diffondere materiale pedopornografico la risposta dell'ordinamento si debba esaurire su un piano esclusivamente amministrativo (stante il carattere speciale delle norme extrapenali rispetto alla previsione codicistica qui considerata)[31].

L'auspicio non può che essere quello di un'armonizzazione della risposta dell'ordinamento alla mancata "collaborazione". La questione, semmai, è se tale armonizzazione debba necessariamente passare da un generalizzato ricorso alla sanzione penale, magari attraverso l'introduzione di una incriminazione *ad hoc*, con contestuale abrogazione degli illeciti amministrativi attualmente presenti nell'ordinamento. In realtà, il ricorso a un modello punitivo di natura amministrativa si lascia preferire: il ricorso a sanzioni amministrative pecuniarie (anche elevate) – eventualmente con l'aggiunta di sanzioni interdittive – appare adeguato in termini di proporzione della risposta repressiva e più in linea con il principio di sussidiarietà dell'intervento penale.

Anche su questo terreno, la predisposizione di un adeguato apparato sanzionatorio (a prescindere da quale esso sia) potrebbe, però, non dimostrarsi realmente efficace. La collaborazione comporta anche dei costi per la rimozione dei contenuti illeciti e per l'adeguamento della struttura informatica. Cosa succede nel caso in cui l'*ISP* non sia oggettivamente in grado di affrontarli? Il rischio è che all'irrogazione della sanzione non segua il perseguimento dell'obiettivo principale, che è quello di interrompere la permanenza a tempo indefinito nel mondo digitale di contenuti offensivi di beni giuridici meritevoli di tutela.

Al fine di scongiurare questo pericolo – evitando nel contempo di pretendere da parte dell'ISP una condotta inesigibile – si potrebbe pensare alla introduzione – secondo un modello già sperimentato, per esempio, in Francia[32] – di un sistema "premiale" di incentivi alla collaborazione o, quantomeno, prevedere un parziale rimborso delle spese sostenute dal *provider* per l'adeguamento tecnologico necessario ad ottemperare alle richieste di collaborazione.

Anche quest'ultima prospettiva, peraltro, non è priva di aspetti problematici. Risulta, infatti, contraddittorio irrogare ad un soggetto una misura afflittiva, il cui contenuto sarà di norma patrimoniale e, nello stesso tempo, riconoscere, al medesimo soggetto, la possibilità di accesso a contributi economici per coprire i costi necessari ad adempiere all'obbligo violato: l'effetto generalpreventivo insito nella minaccia della sanzione ne uscirebbe fortemente depotenziato.

La risposta penale all'elusione dei provvedimenti giurisdizionali, in A.A. V.V., *Scritti per la costituzione del dipartimento giuridico dell'Università del Molise*, Campobasso, 2012, p. 5 ss.

[31] A. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio,* cit., p. 38.

[32] L. V. BERRUTI, Black list, cit., p. 6.

5. *Considerazioni conclusive*

In conclusione, dal punto di vista del diritto penale, il tema delle condizioni normative atte a garantire efficienti prospettive di sviluppo del "mercato unico digitale" implica la necessità di individuare ragionevoli punti di equilibrio tra esigenze contrapposte: da una parte, l'obiettivo dell'accertamento dei reati, dell'assicurazione delle fonti di prova e di rimozione delle conseguenze lesive delle offese penalmente rilevanti; dall'altro, l'esigenza di garantire il rispetto dei diritti fondamentali dell'individuo, da quelli più tradizionali (libertà di manifestazione del pensiero, libertà di impresa, ecc..) a quelli di più recente emersione (integrità, sicurezza e riservatezza informatica; autodeterminazione informativa, *etc.*).

Tutto ciò presuppone l'individuazione di elevati *standard* comuni tra i diversi ordinamenti europei. Fino ad oggi, ad assumersi l'onere di bilanciare i diversi interessi in gioco sono state – in modo ovviamente episodico – le Corti Costituzionali nazionali, oltre alla Corte di Giustizia UE e alla Corte EDU[33].

Si pensi, per esempio, alla decisione della Corte di Giustizia UE che ha affermato il principio secondo cui l'ingiunzione diretta, da parte di un giudice ad un *service provider*, di adottare sistemi di filtro per impedire agli utenti di utilizzare sistemi di *file sharing* in violazione delle norme in materia di diritto d'autore, comprime in modo sproporzionato i diritti e le libertà tutelati dagli artt. 8 e 11 della Carta dei diritti fondamentali dell'Unione europea e dai corrispondenti artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, oltre che la libertà di impresa (ex art. 16 della Carta)[34]. Una pronuncia chiaramente ispirata all'idea – sopra esposta – secondo cui il grado di compressione della libertà di espressione e di fruizione della rete è legato al livello di offensività della condotta che si mira a reprimere (e a prevenire).

Un equilibrio più stabile, però, non può che essere realizzato a un livello normativo generale (*rectius*, sovranazionale). Centrale diventa allora il ruolo delle organizzazioni sovranazionale e la loro capacità di produzione di diritto positivo. Diversamente bisognerà fare i conti con un sistema – come quello attuale – frammentario e affidato alle oscillazioni sia dei singoli legislatori nazionali, sia della giurisprudenza delle Corti nazionali e sovranazionali.

---

[33] Sul punto, R. FLOR, *Lotta alla "criminalità informatica"*, cit., p. 5 ss.; O. POLLICINO, Copyright versus freedom, cit., p. 1971 ss.

[34] Sentenza della Corte di Giustizia dell'Unione Europea del 16 febbraio 2012, causa C-360/10, *SABAM c. Netlog NV*, in *Dir. comm. int.*, 2012, p. 1075 ss., con nota di A. MONTANARI, *Prime impressioni sul caso SABAM c. NETLOG NV: gli* internet service provider *e la tutela del diritto d'autore* on line.