UNIVERSITA' DEGLI STUDI DI VERONA

DIPARTIMENTO DI SCIENZE GIURIDICHE

SCUOLA DI DOTTORATO DI GIURISPRUDENZA

DOTTORATO DI RICERCA IN

Diritto ed Economia dell'impresa: Discipline interne ed internazionali - 28° ciclo

TESI DI DOTTORATO

INTERNET SERVICE PROVIDER DELINQUERE ET PUNIRI POTEST?

Coordinatore e Tutor: Prof. Lorenzo Picotti

Dottoranda: Dott.ssa Lisa Castellani

Anno Accademico: 2015-2016

Nessun impedimento giuridico all'uso di questo o di quel mezzo offerto dalla tecnica moderna sarà mai sufficiente garanzia per l'umana personalità fino a che regnerà la legge dell'odio in vece della legge dell'amore.

-Giuliano Vassalli-

INDICE

CAPITOLO PRIMO

CONSIDERAZIONI PRELIMINARI: LA RESPONSABILITA' PENALE "PERSONALE"

CAPITOLO SECONDO

CONTESTO DI RIFERIMENTO: IL *CYBERSPACE*

CAPITOLO TERZO

MODELLI DI REGOLAMENTAZIONE DELLA RESPONSABILITÀ DELL'*INTERNET SERVICE PROVIDER*

CAPITOLO QUARTO

RILIEVI PENALISTICI SULLA RESPONSABILITÀ *DELL'INTERNET SERVICE PROVIDER*

CAPITOLO PRIMO

CONSIDERAZIONI PRELIMINARI: LA RESPONSABILITA' PENALE "PERSONALE"

SOMMARIO: 1. Il concetto di responsabilità penale - 2. Il principio della responsabilità penale "personale" - 3. L'evoluzione interpretativa della Corte Costituzionale sulla personalità della responsabilità penale - 4. Profili di possibile contrasto con il principio di "personalità": a) L'art. 57 c.p.; b) La responsabilità da reato degli enti - 5. Prospettive *de iure condendo*: una nuova lettura della "personalità" della responsabilità penale.

1. IL CONCETTO DI RESPONSABILITA' PENALE

La locuzione "responsabilità penale" esprime il concetto di relazione sussistente tra un "fatto penalmente rilevante" e una "sanzione criminale"[1].

Essa indica l'ascrizione ovvero l'astratta attribuibilità della pena[2], e, quale giudizio di relazione, nasce nel momento in cui ci si interroga in ordine a chi

[1] Cfr. GROSSO C. F., voce *Responsabilità penale*, in *Novissimo Digesto Italiano*, 1968, p. 709. V. anche FIORELLA A., voce *Responsabilità penale,* in *Enciclopedia del diritto*, 1988, p. 1289 ss.; RICCIO G., voce *Responsabilità penale*, in *Enciclopedia giuridica Treccani*, 1993, p. 1 ss.; FIORELLA A., voce *Reato in generale,* in *Enciclopedia del diritto*, Milano, 1987, p. 771 ss.; DELITALA G., voce *Diritto penale,* in *Enciclopedia del diritto*, 1964, p. 1095 ss.

[2] Come evidenziato da NUVOLONE P., *Le leggi penali e la Costituzione*, Milano, 1953, p. 32: «responsabilità è termine che, nel linguaggio tecnico giuridico, sta a indicare l'assoggettamento al peso, alle conseguenze di un determinato fatto; nella specie, al carico della sanzione penale. Da certi fatti – in genere, si tratta propriamente di azioni – discende come conseguenza giuridico-penale, l'applicabilità di una sanzione: si dice allora che da quel fatto deriva una responsabilità penale. In genere, abbiamo detto, si tratta di azioni; ma talvolta abbiamo delle situazioni oggettive,

debba accollarsi un fatto penalmente rilevante ed ai motivi e meccanismi attraverso i quali si innesca e si sviluppa il processo di imputazione.

La responsabilità penale è il problema centrale dell'intero sistema penalistico, richiedendo riflessioni sulla determinazione di ciò che può essere definito penalmente rilevante, sul concetto di sanzione penale ed il fondamento/limite del ricorso ad essa.

Prima di procedere all'esame del principio cardine in materia, espresso dall'art. 27 Cost., è necessaria una breve premessa volta a chiarire, dal punto di vista sostanziale[3], i due elementi che intervengono nel giudizio di responsabilità: ovvero "il fatto penalmente rilevante" e la "sanzione criminale".

Parte della dottrina, adottando un criterio nominalistico, definisce come penalmente rilevante il fatto umano, descritto da un complesso di disposizioni dell'ordinamento giuridico, cui la legge ricollega una sanzione penale imputandola al suo autore[4].

Tale definizione è di natura formale poiché l'essenza dei fatti assunti a oggetto di disciplina non rileva. Indipendentemente dal contenuto delle singole fattispecie, il discrimine tra "fatti penalmente rilevanti" e "fatti non penalmente rilevanti" è esclusivamente basato sulle conseguenze giuridiche (pena criminale), che il legislatore designa in relazione agli stessi: se nei confronti di chi commette un determinato fatto è prevista l'applicazione di una pena ci troveremo di fronte ad una norma penale.

---

non ricollegabili se non indirettamente ad un'azione: per esempio l'essere colti in possesso di valori, di grimaldelli e chiavi false, ecc. ecc.»

[3] In genere la dottrina ha utilizzato due modalità per l'esame del reato dal punto di vista sostanziale: lo studio approfondito della singola fattispecie ovvero il raffronto tra il reato e gli altri illeciti dell'ordinamento. Cfr. BRICOLA F., voce *Teoria generale del reato,* in *Novissimo Digesto Italiano*, 1973, p. 12 ss.

[4] Cfr. GALLO M., *L'elemento oggettivo del reato*, Torino, 1969, p. 3 ss.

Questo criterio ha come diretta conseguenza la negazione dell'esistenza di un diritto penale naturale, essendo solo il legislatore ad "imprimere" ad alcuni atti illeciti il carattere di reato sanzionandoli penalmente[5].

La natura dei fatti è stata invece valorizzata, soprattutto nel corso dei primi anni del Novecento, da teorie volte all'individuazione di un concetto pre-giuridico di reato, svincolato dal modello legale.

Si consideri a titolo esemplificativo la definizione fornita da Maggiore, secondo il quale il fatto penalmente rilevante turba gravemente l'ordine etico[6], o il criterio identificativo del reato individuato da Ferri, ossia la violazione della moralità di un popolo in un determinato momento storico[7], o ancora da Grispigni, secondo il quale fatto penalmente rilevante è quello che mette in pericolo l'esistenza e la conservazione della società[8].

Tali ricostruzioni hanno suscitato numerose perplessità per la mutevolezza storica e non generalizzabilità dei criteri adottati, nonché per l'impossibilità della scienza giuridico-penale di prescindere dal dato normativo.

Le concezioni cd. "sostanziali" tratterebbero del reato in termini solo apparentemente sostanziali: nell'intento di trovare le "costanti" di un certo comportamento ribalterebbero il corretto approccio metodologico tra norma e reato in sé, partendo dalla valutazione dei motivi che hanno indotto il legislatore ad una certa normativa e cercando di spiegarli. Si confonderebbero quindi gli elementi sociologici con gli elementi formali, esprimendo, più o meno consapevolmente, semplici aspettative riguardo alla più idonea configurazione dell'illecito penale in una prospettiva *de iure condendo*[9].

Essenziale richiamare infine la teoria elaborata da Franco Bricola, volta a fondare una definizione pre-legislativa di reato, inteso quale fatto lesivo di un

---

[5] Cfr. DELITALA G., voce *Diritto penale*, cit., p. 1095 ss.

[6] Cfr. MAGGIORE G., *Diritto Penale*, Bologna, 1951.

[7] Cfr. FERRI E., *Principio di diritto criminale*, Torino, 1928.

[8] Cfr. GRISPIGNI F., *Diritto Penale Italiano*, Milano, 1947.

[9] Cfr. GALLO M., *L'elemento oggettivo del reato*, cit., p. 6 ss.; FIORELLA A., voce *Reato in generale*, cit., p. 775 ss.

valore costituzionalmente rilevante[10]. Tale tesi offre la possibilità di conciliare la definizione formale del reato con l'importanza di valorizzare un criterio "sostanziale" che possa limitare, nella fase pre-normativa, i margini di scelta del legislatore.

L'originale linea di pensiero elaborata da Bricola permette di individuare nella Costituzione non un mero limite, bensì il fondamento del diritto penale: la singola scelta incriminatrice viene legittimata positivamente grazie al tracciato costituzionale, che, pertanto, non rappresenta esclusivamente un semplice strumento di controllo dell'assenza di contrasti con i diritti di libertà in esso riconosciuti[11].

Anche riguardo al concetto di "sanzione criminale"[12] sono state elaborate definizioni basate sul criterio meramente nominalistico, in virtù del quale possono

[10] Secondo l'autore la rilevanza costituzionale del bene oggetto di tutela non va intesa in senso letterale, dovendo essere ricompresi in tale categoria anche gli interessi il cui riconoscimento costituzionale è "implicito" data la loro riconducibilità al novero dei valori del sistema sociale sotteso all'ordinamento costituzionale. Cfr. BRICOLA F., voce *Teoria generale del reato*, cit., p. 17 ss. In riferimento alle critiche mosse a tale teoria cfr. NUVOLONE P., *Il sistema del diritto penale,* Padova, 1982, p. 49 ss., in cui l'autore puntualizza come «non sembra possibile ritenere che una teoria del reato debba esaurirsi nella prospettiva costituzionale. Se è indubbio che i beni espressamente tutelati dalla Costituzione individuano interessi primari, è anche vero che essi non esauriscono, per loro natura, gli interessi suscettibili di tutela penale. Certamente, l'incriminazione della lesione di tali interessi sarà costituzionalmente legittima, ma non sarà illegittima l'incriminazione della lesione di altri interessi, purché non siano in contrasto con quelli garantiti dalla Costituzione. La Costituzione stessa, invero, nella sua struttura, lascia un largo ambito di operatività al legislatore ordinario, con due limiti: quello formale, della procedura di formulazione delle leggi, e quello, sostanziale, del contenuto non incompatibile con i principi costituzionale». V. inoltre DONINI M., voce *Teoria del reato*, in *Digesto delle discipline penalistiche*, 1999, p. 269 ss.

[11] Cfr. MANES V., *Il principio di offensività nel diritto penale*, Torino, 2005, p. 65.

[12] Per un'analisi completa cfr. NUVOLONE P., voce *Pena (diritto penale)*, in *Enciclopedia del diritto*, 1982, p. 787 ss., secondo il quale le note distintive della pena sarebbero le seguenti: è sanzione di un fatto-reato; la sua applicazione consegue all'accertamento di un fatto di reato; produce "effetti penali" ovvero è premessa di situazioni giuridiche qualificanti la persona dal punto di vista dell'applicazione della legge penale; si traduce generalmente nella creazione di uno status di condannato, afflittivo della personalità umana. «Ovviamente, possono mutare le forma ed

essere considerate pene solamente quelle che il legislatore chiama con questo lemma, rinviando alle tipologie enunciate dagli artt. 17 ss. c.p.[13].

Per parte della dottrina sarebbe invece possibile distinguere le pene da ogni altra specie di misura giuridica affidandosi al criterio offerto dalla tipologia del procedimento di applicazione previsto per le stesse[14]. Alla stregua di tale parametro sono ricondotte alla categoria delle "sanzioni criminali" sia le pene in senso stretto, che le misure di sicurezza, in quanto entrambe vengono irrogate dal giudice penale secondo modalità che ne determinato il carattere giurisdizionale penale, quale ad esempio l'iniziativa da parte del Pubblico Ministero[15]. Secondo tale impostazione, pertanto, lo stesso concetto di responsabilità penale viene ampliato, concernendo i fatti per i quali il legislatore ha previsto la pena o la misura di sicurezza, applicate poi alternativamente o congiuntamente in base alla capacità di intendere e di volere ed alla pericolosità del soggetto agente.

Ad avvalorare tale affermazione si consideri anche il fatto che, ove si escludessero le misure di sicurezza dalla categoria delle sanzioni penali, le stesse non risponderebbero più al principio di personalità della responsabilità penale ed alla finalità rieducativa della pena di cui all'art. 27 Cost., e potrebbero quindi

---

i contenuti delle pene in rapporto alle finalità che la coscienza sociale attribuisce di volta in volta alla loro esecuzione: intimidazione, prevenzione generale, prevenzione speciale. Ed è qui che sorgono le dispute dottrinarie, le contese ideologiche e le aporie pratiche: nella storia, non nella logica del pensiero. In questo quadro, ma anche solo in questi limiti, una crisi irrisolta domina ancora la tematica della pena». V. anche DELITALA G., voce *Diritto penale*, in *Enciclopedia del diritto*, 1964, p. 1095 ss. In modo particolare sui criteri di distinzione tra sanzione amministrativa e sanzione penale v. PALIERO C. E., TRAVI A., *La sanzione amministrativa. Profili sistematici*, Milano, 1988, p. 6 ss.; DE VERO G., *Corso di diritto penale*, Torino, 2012, p. 46 ss. Con riferimento ai problemi attuali della pena e della sua esecuzione alla luce delle indicazioni costituzionali v. PUGIOTTO A., *Il volto costituzionale della pena (e i suoi sfregi)*, in penalecontemporaneo.it, 10 Giugno 2014.

[13] Cfr. DELITALA G., voce *Diritto penale*, cit., p. 1095; FIORELLA A., voce *Responsabilità penale*, cit., p. 1289.

[14] V. MANZONI I., voce *Illecito amministrativo tributario*, in *Enciclopedia del diritto*, 2007, p. 717 ss.

[15] Cfr. GALLO M., voce *Capacità penale*, in *Novissimo Digesto Italiano*, 1958, p. 885 ss.

essere applicate a un soggetto per fatto altrui, con valenza prettamente punitiva, compromettendo ogni intento di riduzione della pericolosità.

La critica maggiore mossa nei confronti del tentativo di ricostruire il concetto di sanzione penale attraverso il criterio del procedimento riguarda l'inversione che si verificherebbe nel rapporto effettivo sussistente tra norma di diritto sostanziale e norma processuale. Si instaurerebbe, cioè, una sorta di "circolo vizioso", dato che la norma sostanziale qualificherebbe la norma processuale e viceversa[16].

Alcuni autori, respingendo il criterio del procedimento, si affidano a considerazioni teleologiche, individuando quale carattere essenziale delle sanzioni penali il fatto di essere conseguenze giuridiche volte alla prevenzione generale nonché alla funzione di emenda[17].

Le diverse teorie sin qui esposte sembrano ricomporsi nella definizione di "materia penale" offerta dalle Corti Supreme europee[18], le quali si affidano a tre criteri, elaborati a partire dalla celebre sentenza della Grande Camera della Corte EDU nel caso *Engel e altri c. Paesi Bassi* dell' 8 giungo 1976, ovvero:

---

[16] Cfr. PAGLIARO A., *Il fatto di reato*, Palermo, 1960, p. 75.

[17] *Ibidem*.

[18]Cfr. Corte EDU, sent. 8 giungo 1976, *Engel e altri c. Paesi Bassi*; Corte EDU, sent. 23 novembre 2006, *Jussila c. Finlandia*; Corte di Giustizia UE, sent. 5 giugno 2012, C-489/10, *Bonda*; Corte di Giustizia UE, sent. 26 febbraio 2013, *Aklagaren c. Hans Akerberg Franssonn*; Corte EDU, sent. 4 marzo 2014, *Grande Stevens c. Italia*, con commento *Relazione dell'Ufficio del Massimario della Cassazione sulle ricadute della sentenza della Corte EDU Grande Stevens c. Italia in tema di ne bis in idem*, in penalecontemporaneo.it, 29 Maggio 2014; VOZZA D., *I confini applicativi del principio del ne bis in idem interno in materia penale: un recente contributo della Corte di Giustizia dell'Unione europea*, in penalecontemporaneo.it, 15 Aprile 2013. Sulla definizione di "materia penale" v. PALIERO C. E., *"Materia penale" e illecito amministrativo secondo la Corte Europea dei Diritti dell'Uomo: una questione "classica" a una svolta radicale*, in *Rivista italiana di diritto e procedura penale*, 1985, p. 894 ss.; BERNARDI A., *Art. 7. "Nessuna pena senza legge"*, in BARTOLE S. CONFORTI B., RAIMONDI G., (a cura di), *Commentario della Convenzione europea dei diritti dell'uomo*, Padova, 2001, p. 249 ss.; NICOSIA E., *Convenzione europea dei diritti dell'uomo e diritto penale*, Torino, 2006; MANES V., ZAGREBELSKY V., (a cura di), *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011.

a) la qualificazione giuridica della violazione nell'ordinamento nazionale;

b) la natura effettiva della violazione;

c) il grado di severità della sanzione.

L'indicazione data dal sistema giuridico dello Stato rappresenta il primo *step* per la valutazione. Secondariamente, infatti, va considerata, mediante un'impostazione che ricorda molto l'analisi di Bricola, la natura sostanziale dell'illecito commesso, vale a dire se si è di fronte ad una condotta in violazione di una norma preposta alla tutela *erga omnes* di beni giuridici della collettività, anche alla luce del denominatore comune delle rispettive legislazioni dei diversi Stati contraenti.

Va infine considerato il grado di severità della pena che rischia la persona interessata poiché, secondo le Corti, in una società di diritto appartengono alla sfera "penale" le privazioni della libertà personale suscettibili di essere imposte quali punizioni.

2. IL PRINCIPIO DELLA RESPONSABILITA' PENALE "PERSONALE"

A seguito dell'individuazione, seppur sintetica, del significato dei concetti essenziali che contraddistinguono la responsabilità penale, l'indagine si deve necessariamente concentrare sul suo carattere "personale" fissato nella disposizione normativa di cui all'art. 27, 1° comma, Cost.

L'aggettivo "personale", nel linguaggio tecnico giuridico, indica il rapporto di connessione tra un soggetto ed un determinato oggetto. Responsabilità penale personale significa pertanto, in primo luogo, «una responsabilità legata indissolubilmente ad una persona: e, più precisamente, a quella persona che costituisce l'elemento soggettivo della fattispecie che l'ordinamento giuridico considera fonte di conseguenze penali»[19].

[19] Cfr. NUVOLONE P., *Le leggi penali e la Costituzione*, cit., p. 32.

In relazione al significato della formula contenuta nell'art. 27 Cost. in dottrina si sono sviluppati diversi orientamenti[20]. In quanto "principio" essa presenta le ambiguità tipiche della categoria[21] ed inoltre, né la lettera della disposizione né l'esame dei lavori preparatori offrono all'interprete una soluzione univoca[22].

Secondo la cosiddetta teoria oggettiva, alla locuzione "responsabilità penale personale" si dovrebbe attribuire l'accezione minima di responsabilità penale per fatto proprio.

La finalità della disposizione in esame sarebbe quella di vietare forme di responsabilità per fatto altrui, ovvero forme di responsabilità nelle quali il soggetto non ha posto in essere alcuna condotta, nonché di impedire sanzioni collettive. Alla base di tale ricostruzione la certezza che nella mente del Legislatore, al momento della stesura della norma, fossero ben vive le immagini delle rappresaglie, decimazioni e pene collettive dell'ultimo conflitto mondiale[23].

---

[20] Cfr. ALESSANDRI A., *Art. 27*, in BRANCA G., PIZZORUSSO A., *Commentario della Costituzione*, Bologna-Roma, 1991, p. 1 ss.; BRICOLA F., voce *Teoria generale del reato*, cit., p. 51 ss.; FIORELLA A., voce *Responsabilità penale*, cit., p. 1291 ss.

[21] In riferimento al concetto di "principio" ed alla distinzione rispetto al concetto di "norma" cfr. FIANDACA G., DI CHIARA G., *Introduzione al sistema penale per una lettura costituzionalmente orientata*, Napoli, 2003, p. 6 ss. L'autore definisce i principi come norme *sui generis*; le note distintive più significative tra i principi e le norme o regole giuridiche in senso stretto riguardano la portata, avendo i primi «portata – regolativa, orientativa o programmatica – tendenzialmente generale e contenuto relativamente indeterminato» nonché l'applicazione, dato che mentre «le norme in senso stretto sono applicabili nella forma del "o tutto o niente" […] i principi esulano dalla logica della contrapposizione antinomica ed ammettono, invece, applicazioni parziali o graduali nella forma del "più o meno": per cui, nel caso di reciproco conflitto, essi possono essere contemporaneamente applicati in base al peso rispettivo secondo la teoria del bilanciamento».

[22] In riferimento ai lavori preparatori e al fatto che gli stessi non offrono un "aiuto reale" per l'interpretazione della norma in esame cfr. GROSSO C. F., voce *Responsabilità penale*, cit., p. 712 ss.

[23] In merito a tal punto cfr. in senso critico ALESSANDRI A., *Art. 27*, cit., p. 57 ss., secondo il quale, l'accostamento delle pene collettive al problema della responsabilità penale è frutto «di un insidioso equivoco». Il divieto di rappresaglie, contemplato nel diritto internazionale, andrebbe riferito semmai agli artt. 10 e 11 Cost. e, come per le sanzioni collettive patrimoniali, la base

Il carattere "proprio" del fatto sarebbe quindi integrato dal nesso di causalità materiale che lega la condotta del soggetto agente all'evento: è sufficiente cioè che il soggetto realizzi il substrato materiale della fattispecie[24].

Nella sua accezione più ampia il principio viene interpretato, invece, come divieto di responsabilità per fatto incolpevole. Per aversi responsabilità personale, oltre al legame eziologico, sarebbe necessaria la valorizzazione della riferibilità anche psicologica del fatto commesso al soggetto, tale da far apparire il reato come frutto di una sua scelta volontaria (dolo) o comunque di un suo comportamento evitabile (colpa).

In effetti l'analisi delle altre disposizioni che, direttamente o indirettamente, determinano il volto costituzionale del sistema penale, induce a ritenere pienamente fondata l'opinione ora accennata.

In primo luogo, il 3° comma dell'art. 27 Cost., attribuendo funzione rieducativa alla pena, oltre a precludere già di per sé la possibilità di colpire un soggetto diverso dall'autore del reato, richiede una certa compenetrazione psicologica tra fatto e persona: «Solo là, infatti, dove l'agente si sia dimostrato ostile o indifferente ai valori della convivenza –tenendo una condotta che, per intrinseca pericolosità o perché riconoscibilmente proibita, poteva e doveva apparirgli asociale, illecita– solo allora il ristabilimento repressivo dei valori sociali dispregiati ed un'opera rieducativa (ammonitrice) sul reo avrebbero senso»[25].

I sostenitori di tale ricostruzione affermano inoltre che, aderendo alla lettura minimalistica dell'art. 27 Cost., si svuoterebbe di significato la disposizione di cui all'art. 25, 2° comma, Cost., la quale, prevedendo che nessuno può essere punito

---

sarebbe da rintracciarsi «nei valori primordiali del consorzio civile, tra i quali, in particolare, il diritto inviolabile al riconoscimento ed alla salvaguardia della dignità dell'uomo». Per un'analisi sintetica dell'istituto della rappresaglia e l'evoluzione dottrinale e giurisprudenziale in merito allo stesso v. RassegnaGM-HeinrichNordhorn in difesa.it.

[24] Cfr. NUVOLONE P., *Le leggi penali e la Costituzione*, cit., p. 33; VASSALLI G., *Sulla legittimità costituzionale della responsabilità penale obbiettiva per fatto proprio*, *e leggi penali e la Costituzione*, in *Giurisprudenza Costituzionale*, 1957, p. 1005 ss.

[25] Cfr. PULITANÒ D., voce *Ignoranza*, in *Enciclopedia del diritto*, 1970, p. 36 ss.

se non per un fatto *commesso*, già richiede necessariamente la sussistenza del nesso causale, altrimenti lo stesso fatto verrebbe meno[26].

Avvalorano infine la tesi della responsabilità penale per fatto proprio colpevole anche le direttive di cui agli artt. 2 e 3 cpv., Cost. Per garantire il libero sviluppo della persona umana ed il principio di certezza, la pena, infatti, non può prescindere da comportamenti umani colpevoli[27].

La Costituzione repubblicana nel suo complesso, ponendo l'uomo al vertice della scala dei valori, rende inammissibile la strumentalizzazione del reo. L'uomo "è fine in sé" pertanto il principio di personalità della pena comporta non solo il divieto di responsabilità per fatto altrui, ma anche l'illegittimità di sanzioni totalmente finalizzate alla general-prevenzione e determinate nel *quantum* sulla base di elementi non ancorati alla condotta o personalità del soggetto[28].

Proprio in virtù dei principi fondamentali di cui agli artt. 2 e 3 della Cost., i "fulmini" della legge penale non possono colpire «chi in ragionevole buona fede abbia ritenuto di agire (di estrinsecare la sua personalità) nei limiti del suo apparente diritto»[29]. Tutelare il libero sviluppo della persona, infatti, impone che contenuto e limiti della libertà, e dunque i confini fra il lecito e l'illecito, siano chiaramente segnati e soggettivamente riconoscibili. Lo stesso art. 25 Cost., esplicitando l'esigenza di tassatività ed irretroattività della legge penale, è finalizzato a garantirne la possibilità di conoscenza affinché il cittadino abbia un orientamento certo nell'uso della propria libertà personale[30].

Alla base di tali affermazioni ritroviamo una concezione di stampo liberal-contrattualistico dei doveri costituzionali gravanti rispettivamente sullo Stato e sul cittadino, dalla quale discende necessariamente che l'applicazione della sanzione penale non può essere sganciata dalla colpevolezza, né essere giustificata ove l'ignoranza o l'errore della legge penale siano inevitabili.

---

[26] Cfr. ALESSANDRI A., *Art. 27*, cit., p. 73.

[27] Cfr. BRICOLA F., voce *Teoria generale del reato*, cit., p. 51.

[28] Cfr. BRICOLA F., *La discrezionalità nel diritto penale*, Milano, 1965, p. 353 ss.

[29] Cfr. PULITANÒ D., voce *Ignoranza*, cit., p. 36 ss.

[30] Cfr. PULITANÒ D., *L'errore di diritto nella teoria del reato*, Milano, 1976, p. 457 ss.

Sembra pertanto doversi aderire alla parte della dottrina, la quale sostiene la sostanziale coincidenza tra l'imputazione ad un soggetto di un fatto altrui e quella di un evento che, ancorché frutto della sua condotta, si ponga al di fuori dei confini del dolo e della colpa: l'accadimento, anche in questo secondo caso, non essendo controllato dal soggetto né a lui rimproverabile, non può dirsi come "suo personale"[31].

In una prima fase storica la "colpevolezza", presupposto necessario per la rieducazione e per la personalità della pena, coincise con la sussistenza della colpa o del dolo (cd. concezione psicologica della colpevolezza). Già dagli inizi del Novecento però tale ricostruzione venne criticata dal punto di vista dogmatico per la sua incapacità di ricomprendere in un concetto unitario superiore il dolo e la colpa e, dal punto di vista funzionale, per il fatto di non consentire una graduazione della colpevolezza stessa.

Per superare tali aporie è stata elaborata una nuova concezione di colpevolezza cd. normativa: il rimprovero non è "per la volontà di ciò che non doveva essere" ma "per una volontà che non doveva essere", una volontà contraria alle aspettative del diritto[32]. La colpevolezza risulta pertanto un'entità complessa, che include l'insieme dei criteri dai quali dipende la possibilità di muovere all'agente un rimprovero giuridico per la commissione di un fatto conforme al tipo legale e non scriminato, quali l'imputabilità, il dolo o la colpa, la conoscenza o la conoscibilità della norma penale violata, la normalità del processo motivazionale.

Per concludere, quindi, secondo la prevalente dottrina, la formula *nulla poena sine culpa*, espressa dal principio di personalità della pena, non si esaurisce nell'accertamento del legame psicologico tra fatto ed autore, ma, alla luce dell'evoluzione della nozione di colpevolezza, richiede la rimproverabilità

---

[31] Cfr. GROSSO C. F., voce *Responsabilità penale*, cit., p. 713.

[32] Cfr. BETTIOL G., *Diritto penale*, Padova, 1969, p. 329 ss. Per un raffronto chiaro e sintetico della *concezione psicologica* e della *concezione normativa* della colpevolezza, anche per l'ampio richiamo alla bibliografia essenziale sul tema v. MANTOVANI F., *Diritto penale. Parte generale*, Ottava Edizione, Padova, 2013, p. 286 ss.; FIANDACA G., MUSCO E., *Diritto penale. Parte generale*, Sesta Edizione, Bologna, 2009, p. 318 ss.

dell'atteggiamento psicologico nonché l'adeguamento della sanzione alla gravità del fatto e alla personalità del reo[33].

3. L'EVOLUZIONE INTERPRETATIVA DELLA CORTE COSTITUZIONALE SULLA PERSONALITÀ DELLA RESPONSABILITÀ PENALE

Il principio fissato dall'art. 27, 1° comma, Cost., è stato oggetto di una profonda evoluzione nei tracciati della Corte Costituzionale. L'analisi diacronica dell'orientamento sviluppatosi in seno alla Corte permette di distinguere tre posizioni teoretiche[34].

Un primo filone è rappresentato dalle sentenze in cui la Corte ha inteso il principio in esame in senso stretto, come divieto di responsabilità per fatto altrui, affermando la sufficienza del nesso causale per tutelarne il rispetto. Trattasi di pronunce scarsamente argomentate nelle quali risulta ben percepibile lo sforzo della Corte di conservare fattispecie problematiche (quali la rissa aggravata, l'ubriachezza non accidentale o l'*error aetatis*) spostando l'attenzione dalla norma costituzionale a quella impugnata e dandone un'interpretazione che garantisse comunque un certo nesso psichico tra azione ed evento. In tal modo la Corte, in evidente contraddizione, affermava la legittimità di dette norme, offrendone però letture conformi a quell'accezione di responsabilità penale che la stessa dichiarava di rifiutare[35].

---

[33] Cfr. BRICOLA F., *La discrezionalità nel diritto penale*, cit., p. 354.

[34] Cfr. CANESTRARI S., voce *Responsabilità oggettiva*, in *Digesto delle discipline penalistiche*, 1997, p. 116 ss.

[35] Cfr. ex multis Corte Costituzionale, sent. n. 107/1957, in cui la Corte afferma che nella disposizione di cui all'art. 27 Cost. «la Costituzione - come si evince chiaramente dalla formulazione letterale del testo - non fa che enunciare il carattere personale della responsabilità penale e contiene perciò un tassativo divieto della responsabilità penale per fatto altrui, senza alcun riferimento al divieto della cosiddetta responsabilità oggettiva. Il limpido significato del testo della norma stessa è confermato, in modo da evitare ogni possibilità di dubbio, dai lavori preparatori, nei quali espressamente ed univocamente fu manifestato, come unico scopo della disposizione, quello di vietare tutte quelle forme di repressione penale che avevano avuto recenti esempi di triste esperienza, relativi a responsabilità estesa a persone o a gruppi di persone estranee al reato e

A fronte di tali pronunce, che, ricorrendo soprattutto all'esegesi dei lavori preparatori della Costituzione, offrivano un'interpretazione "oggettiva" del carattere della personalità, si rinviene un secondo filone di sentenze maggiormente aderenti alla teoria soggettiva, nelle quali la Corte, seppur con un atteggiamento molto cauto, ritiene soddisfatto il principio di personalità alla presenza, oltreché del nesso causale, di un certo nesso psichico, la cui definizione non è univoca ma intrinsecamente legata alla fattispecie penale oggetto di valutazione.

Le pronunce assunte in tale seconda categoria danno una lettura più ricca dell'art. 27 Cost. e manifestano dubbi circa la correttezza dell'inquadramento di talune fattispecie, in cui meno evidente è il collegamento con l'elemento del dolo e della colpa, nel paradigma della responsabilità oggettiva[36].

Il prudente atteggiamento della Corte Costituzionale non poteva far presagire la "svolta"[37] radicale segnata dalla sentenza n. 364 del 23 marzo 1988 che

---

diverse dal colpevole, ma che costituivano soltanto rappresaglia e vendetta contro gruppi familiari o etnici ai quali l'imputato apparteneva. La solenne riaffermazione della limitazione della responsabilità penale alle sole conseguenze del fatto proprio, assumeva perciò il significato della riaffermazione di un alto principio di civiltà giuridica. Così inteso, il contenuto della prima parte dell'art. 27 già citato richiede come requisito della responsabilità penale personale soltanto quel rapporto di causalità materiale tra azione ed evento che è enunciato nell'art. 40 del Codice penale e che è sufficiente a stabilire, tra il soggetto ed il fatto preveduto come reato, quel carattere di suità in cui consiste il requisito della personalità nella responsabilità penale». Cfr. anche Corte Costituzionale, sent. n. 79/1961; n. 54/1965; n. 33/1970; n. 20/1971; n. 21/1971; n. 190/1972.

[36] Cfr. *ex multis* Corte Costituzionale, sent. n. 3/1956, in materia di responsabilità penale dei direttori di periodico (unica sentenza interpretativa di rigetto provocata dal richiamo dell'art. 27 Cost.); n. 42/1965 in riferimento all'art. 116 c.p.; n. 259/1976 in merito alla legittimità dell'art 116 della legge doganale del 1940. In tali pronunce emerge un atteggiamento della Corte più attento all'analisi degli elementi soggettivi del fatto sulla premessa «che il principio di personalità della responsabilità penale trovi la sua massima espressione nella partecipazione psichica dell'agente al fatto». In numerose occasioni, inoltre, la Corte manifesta l'opportunità di interventi del Legislatore onde porre rimedio alla carenza di tipicità o mancata specificazione degli elementi soggettivi del reato.

[37] Alla luce degli orientamenti precedenti ben si può parlare di svolta in riferimento alla sent. n. 364/1988, anche se la Corte, preoccupata di convalidare un'idea di continuità del proprio indirizzo, nella stessa afferma che «va soltanto chiarito che quanto sostenuto è in pieno accordo

inaugura l'affermarsi di un terzo filone di pronunce in cui, secondo quanto già evidenziato dalla dottrina più sensibile, si accoglie il principio di colpevolezza specificando che per fatto "proprio" non s'intende tanto il fatto collegato al soggetto dal mero nesso di causalità quanto dal momento subiettivo, costituito, in presenza della prevedibilità ed evitabilità del risultato vietato, almeno dalla colpa in senso stretto[38].

---

con la tendenza mostrata dalle decisioni assunte da questa Corte allorché è stata chiamata a decidere sulla costituzionalità di ipotesi criminose che si assumeva non contenessero requisiti subiettivi sufficienti a realizzare il dettato dell'art. 27 Cost. Qui quella tendenza si completa e conclude. A parte un momento le affermazioni <di principio> contenute nelle citate decisioni, nessuno può disconoscere che, sempre, le sentenze, in materia, hanno cercato di ravvisare, nelle ipotesi concrete sottoposte all'esame della Corte, un qualche <requisito psichico> idoneo a renderle immuni da censure d'illegittimità costituzionale ex art. 27 Cost. Le stesse decisioni, pur muovendosi nell'ambito dell'alternativa tra fatto proprio ed altrui, non hanno mancato di ricercare spesso un qualche coefficiente soggettivo (anche se limitato) sul presupposto che il <fatto proprio> debba includere anche simile coefficiente per divenire <compiutamente proprio> dell'agente». Da notare infine che la dichiarazione della Corte in merito alla rilevanza scusante dell'ignoranza inevitabile della legge penale ha allineato il nostro ordinamento alle scelte giurisprudenziali e legislative già compiute in altri paesi europei: nella repubblica federale tedesca, ad esempio, tale principio era stato affermato dalla Bundesgerichtshof a partire dal 1952 e successivamente inserito nell'art. 17 StGB.

[38] In riferimento alla sent. n. 364/1988, con cui la Corte interviene sull'art. 5 c.p., concernente il principio *ignoratia legis non excusat,* dichiarandone l'illegittimità nella parte in cui non esclude dalla inescusabilità dell'ignoranza della legge penale l'ignoranza inevitabile, v. *ex multis* PALAZZO F. C., *Ignorantia legis*: *vecchi limiti ed orizzonti nuovi della colpevolezza*, in *Rivista italiana di diritto e procedura penale*, 1988, p. 920 ss.; PULITANÒ D., *Una sentenza storica che restaura il principio di colpevolezza*, in *Rivista italiana di diritto e procedura penale*, 1988, p. 686 ss.; PATRONO P., *Problematiche attuali dell'errore nel diritto penale dell'economia*, in *Rivista trimestrale di diritto penale dell'economia*, 1988, p. 87 ss., il quale in senso critico afferma la Corte Costituzionale con tale sentenza « – al di là di alcuni notevoli, indubbiamente importanti affermazioni di principio – ha detto troppo o troppo poco. Ha detto troppo con la pretesa riformulazione dell'art. 5 c.p. […] ha detto troppo poco nel suo non dichiarare in toto l'illegittimità costituzionale dell'art. 5 c.p. […] Ed ha detto troppo poco relativamente alla responsabilità oggettiva: ritenuta la costituzionalizzazione del principio di colpevolezza non ci si può poi trincerare dietro affermazioni quale quella secondo cui "va, di volta in volta, a proposito delle diverse ipotesi criminose, stabilito quali sono gli elementi *più significativi* della fattispecie che non possono non essere coperti almeno dalla colpa dell'agente" […] l'affermata costituzionalizzazione

Per la prima volta la Corte, recependo i frutti preparati dalla riflessione dottrinale[39], ha dichiarato l'illegittimità di una norma, l'art. 5 c.p.[40], proprio per contrasto con il carattere della personalità della responsabilità penale, esplicitamente concepito come contenente il principio di colpevolezza. Secondo l'impostazione seguita dalla dottrina più sensibile, la lettura dell'art. 27, 1° comma, Cost. viene collocata nel complesso dei principi di rilievo costituzionale: il suo significato, cioè, è determinato avendo particolare riguardo ai rapporti con il terzo comma dello stesso articolo e con gli artt. 2, 3, 25, secondo comma, 73, terzo comma, Cost. E' quindi l'interpretazione sistematica dell'art. 27 Cost. che ne svela l'ampia portata.

Nella pronuncia in esame viene inoltre valorizzata quella ricostruzione di stampo liberal-contrattualistico dei rapporti Stato-cittadino conforme, alle già indicate posizioni dottrinali. In modo particolare la Suprema Corte riconosce che l'obbligo statale di introdurre norme penali «non numerose, eccessive rispetto ai fini di tutela, chiaramente formulate, dirette alla tutela di valori almeno di <rilievo

---

del principio di colpevolezza, desunta da una lettura congiunta del 1° e 3° comma dell'art. 27 Cost., non serve poi alla Corte per dedurne quello che dovrebbe essere il più importante effetto: l'incostituzionalità della responsabilità oggettiva».

[39] Cfr. PALAZZO F. C., *Il problema dell'ignoranza della legge penale nelle prospettive di riforma*, in *Rivista italiana di diritto e procedura penale*, 1975, p. 777 ss. In modo particolare l'autore sostiene che «l'applicazione della pena a chi non conosce la legge o a chi neppure è in grado di conoscerla subordina e strumentalizza il valore della persona in sé al valore assolutistico e "statolatrico" della restaurazione dell'ordine giuridico violato o, al più, alla tutela obbiettiva – mediante intimidazione generale dei consociati – dei valori protetti dalla legge. La persona del reo, dunque, non costituisce più lo scopo, il fine della pena e del diritto penale, ma solo lo strumento, il mezzo col quale l'ordinamento realizza se stesso. In questa prospettiva, la responsabilità penale non ha più – per così dire – una dimensione sostanzialmente personale. L'art. 5 c.p., sotto questo primo profilo, dunque, rispecchia chiaramente un ordine di valori che è stato capovolto dalla Costituzione repubblicana, la quale ha posto al vertice della scala dei valori la persona umana con la dignità che la contraddistingue di "fine in sé": la sua incostituzionalità discende, perciò, prima ed oltre che dalla specifica violazione di norme costituzionali, dal contrasto con gli stessi principi informatori della carta fondamentale».

[40] In riferimento all'art. 5 c.p. cfr. ROMANO M., *Commentario sistematico del Codice penale*, Milano, 1995; per quanto attiene la problematica del rapporto tra art. 5 c.p. e gli artt. 59 e 47 c.p. cfr. GROSSO C. F., *L'errore sulle scriminanti*, Milano, 1961.

costituzionale> e tali da esser percepite anche in funzione di norme <extrapenali>, di civiltà, effettivamente vigenti nell'ambiente sociale nel quale le norme penali sono destinate ad operare» è speculare all'obbligo dei cittadini di adempire ai precetti nonché a «strumentali, specifici doveri d'informazione e conoscenza»[41]. Pertanto l'applicazione della sanzione penale non può essere giustificata ove l'ignoranza o l'errore della legge penale siano inevitabili: «far sorgere l'obbligo giuridico di non commettere il fatto penalmente sanzionato senza alcun riferimento alla consapevolezza dell'agente, considerare violato lo stesso obbligo senza dare alcun rilievo alla conoscenza od ignoranza della legge penale e dell'illiceità del fatto, sottoporre il soggetto agente alla sanzione più grave senza alcuna prova della sua consapevole ribellione od indifferenza all'ordinamento tutto, equivale a scardinare fondamentali garanzie che lo Stato democratico offre al cittadino ed a strumentalizzare la persona umana, facendola retrocedere dalla posizione prioritaria che essa occupa e deve occupare nella scala dei valori costituzionalmente tutelati»[42].

La Corte pone in primo piano la funzione di limite, di garanzia delle libere scelte d'azione che ha il principio di colpevolezza. Esso, in tal modo, costituisce il secondo aspetto del principio di legalità[43].

La disciplina dell'*ignorantia legis* risulta strettamente connessa alla necessità di sicurezza giuridica, ovvero all'esigenza di assicurare che il cittadino possa

---

[41] Cfr. Corte Costituzionale, sent. n. 364/1988, *Considerato in diritto 17-18.*

[42] Ivi, *Considerato in diritto 25.*

[43] Molto simile risulta l'impianto logico-deduttivo seguito dalla Corte europea dei diritti dell'uomo, sent. 20 gennaio 2009, *Sud Fondi s.r.l.*, §§ 116-117, in cui il principio di colpevolezza viene riconosciuto come conseguenza implicita del principio di legalità di cui all'art. 7 CEDU. La Corte EDU afferma infatti che, nonostante il silenzio della Convenzione EDU, «la logica della pena e della punizione così come la nozione di "guilty" (nella versione inglese) e la nozione di "personne coupable" (nella versione francese) vanno nel senso di una interpretazione dell'articolo 7 che esige, per punire, un legame di natura intellettuale (coscienza e volontà) che permetta di affermare un elemento di responsabilità nella condotta dell'autore materiale dell'infrazione. In mancanza, la pena non sarebbe giustificata. D'altronde, sarebbe incoerente, da una parte, esigere una base legale accessibile e prevedibile e, d'altra parte, permettere che si consideri una persona come "colpevole" e "punirla" ancorché non fosse in condizione di conoscere la legge penale, in ragione di un errore invincibile che non possa affatto essere imputato a chi ne è stato vittima».

preventivamente conoscere le conseguenze giuridiche e sanzionatorie della propria condotta onde regolarsi in conformità (cd. *choosing system*)[44].

I giudici della Consulta, pur non accogliendo apertamente la concezione normativa della colpevolezza, sulla base della relazione di corrispettività biunivoca tra principio della personalità e finalismo rieducativo, intendono il requisito della conoscibilità della legge quale presupposto necessario della garanzia del fatto proprio colpevole, corollario politico-criminale della funzione special-preventiva della pena.

Di lì a poco, nella sentenza n. 1085 del 13 dicembre 1988, la Corte Costituzionale ha specificato che, affinché la responsabilità sia autenticamente personale, «è indispensabile che tutti gli elementi che concorrono a contrassegnare il disvalore della fattispecie siano soggettivamente legati all'agente (siano, cioè, investiti dal dolo o dalla colpa) ed è altresì indispensabile che tutti e ciascun dei predetti elementi siano allo stesso agente rimproverabili e cioè anche soggettivamente disapprovati»[45].

Nel corso degli anni successivi si è consolidata una lettura estensiva del principio di cui all'art. 27, 1° comma, Cost. in termini di responsabilità per fatto proprio e colpevole, in virtù della quale ogni elemento significativo del fatto di reato deve necessariamente essere addebitato quanto meno a titolo di colpa ed il collegamento soggettivo tra soggetto e il nucleo fondante della fattispecie sia rimproverabile.

Il principio *nullum crimen sine culpa* rappresenta oggi innanzitutto un vincolo per il legislatore che, nell'ambito delle diverse forme di colpevolezza, può "graduare" il coefficiente psicologico di partecipazione dell'autore al fatto, ma in

---

[44] Cfr. FIANDACA G., DI CHIARA G., *Introduzione al sistema penale per una lettura costituzionalmente orientata*, cit., p. 168.

[45] La sentenza in esame interviene sull'art. 626, 1° comma, c.p., (c.d. furto d'uso) dichiarandone l'illegittimità nella parte in cui non contempla l'ipotesi di mancata restituzione dovuta a caso fortuito o a forza maggiore, non essendo tale eventualità, addebitabile all'agente per carenza di rimproverabilità soggettiva.

nessun caso può prescindere *in toto* da esso. Inoltre è un canone ermeneutico per il giudice nella lettura e nell'applicazione delle disposizioni vigenti[46].

4. PROFILI DI POSSIBILE CONTRASTO CON IL PRINCIPIO DI "PERSONALITÀ"

a) L'art. 57 c.p.

La disciplina dei delitti commessi a mezzo della stampa, che, come si approfondirà nel corso della trattazione, per parte della dottrina sarebbe suscettibile di applicazione in via analogica al *provider*, ha suscitato numerose critiche e problematiche sin dalla sua prima apparizione nell'Editto Albertino sulla stampa del 26 marzo 1848, che, all'art. 47, istituiva la figura del cd. "gerente responsabile", chiamato a rispondere in modo automatico di tutti i reati commessi per mezzo del giornale, indipendentemente dall'individuazione dell'autore dello scritto[47].

Ratio della previsione legislativa quella di garantire, senza eccezioni né scusanti, la repressione dei reati in questione.

La prassi, in realtà, mostrò come, a causa della comune estraneità del gerente dalla direzione dello stampato, l'esigenza di "giustizia" fosse totalmente frustrata sia per l'impunità degli effettivi autori che per la condanna di soggettivi prestanome retribuiti proprio in virtù dell'accollamento di responsabilità altrui[48].

---

[46] Cfr. Corte Costituzionale, sent. n. 322/2007, in riferimento al c.d. *error aetatis* di cui all'art. 609-sexies c.p., con la quale la Corte, pur dichiarando l'inammissibilità della questione, chiarisce come anche tale disposizione debba essere riletta in conformità al principio di colpevolezza. E' proprio dall'interpretazione adeguatrice che la Corte ricava la rilevanza scusante dell'errore inevitabile sull'età.

[47] Ex art. 47, r.e. n. 695/1848: «Tutte le disposizioni penali portate da questo capo sono applicabili ai gerenti dei giornali e agli autori che avranno sottoscritto gli articoli in essi giornali inseriti. La condanna pronunciata contro l'autore sarà pure estesa al gerente, che verrà sempre considerato come complice dei delitti e contravvenzioni commessi con pubblicazioni fatte nel suo giornale».

[48] Cfr. VASSALLI G., *Sulla illegittimità costituzionale dell'art. 57 n. 1 c.p.*, in *Giurisprudenza Costituzionale*, 1956, p. 222 ss.

Per tale motivo, con r.d.l. n. 3288/1923, venne introdotto l'obbligo di coincidenza tra il gerente ed il direttore o uno dei principali redattori ordinari e, successivamente, con legge n. 2307/1925, la figura del "direttore responsabile" (e del "redattore responsabile" qualora il primo fosse un deputato o senatore) sostituì completamente quella del "gerente".

Nel Codice Rocco, il testo originario dell'art. 57, comma 1, prevedeva che, salva la responsabilità dell'autore della pubblicazione, il direttore o redattore responsabile rispondesse "*per ciò solo"* del reato commesso.

Le perplessità avanzate in riferimento a tale diposizione si acuirono con l'entrata in vigore della Costituzione, in particolare per il contrasto con il principio di responsabilità personale, sia nella sua accezione più ampia che in quella minima di divieto di responsabilità per fatto altrui: essendo il direttore e il redattore responsabile chiamati a rispondere solamente in virtù della loro qualifica, arduo se non impossibile rintracciare non solo il legame psichico ma, ancor prima, il nesso causale tra condotta e reato[49].

Parte della dottrina, per sostenere la compatibilità della responsabilità del direttore con la Costituzione, ne fornì una lettura in termini di sanzione per *culpa in vigilando*[50]. Il direttore responsabile, cioè, sarebbe tenuto a vigilare per impedire pubblicazioni criminose e, qualora venga meno a tale obbligo di sorveglianza, troverebbe applicazione la disciplina dei reati commissivi per omissione ex art. 40 c.p.

Si tratta di una ricostruzione che richiede la presunzione dell'inosservanza od omissione volontaria, nonché la presunzione del dolo, dato che all'omissione di vigilanza non fa riscontro una responsabilità per colpa ma, invero, una

[49] Cfr. GALLI L., *L'art. 57, n. 1, c.p. e l'art. 27 della Costituzione*, in *Giustizia Penale*, 1950, p. 770 ss. L'autore, dopo un'analisi delle principali teorie diffuse in dottrina e la loro sapiente confutazione, conclude per una responsabilità in cui latita completamente sia il nesso di causalità materiale che quello psicologico.

[50] Cfr. CARNELUTTI F., *Teoria generale del reato*, Padova, 1933, p. 33 ss.; GUARNERI G., *La responsabilità anomala per i delitti commessi a mezzo della stampa e il principio costituzionale della personalità della responsabilità penale*, in *Giurisprudenza Italiana*, 1950, p. 12 ss.

responsabilità per il reato commesso dall'autore, che, nella maggior parte dei casi, è doloso.

Proprio tale aspetto è stato evidenziato per dimostrare l'inefficacia della posizione in esame diretta a sostenere la compatibilità dell'art. 57 c.p. con l'art. 27 Cost.

Come magistralmente denunciato da Vassalli «non par dubbio che lo stabilire, in relazione ad un fatto altrui, una presunzione assoluta di una condotta quanto meno omissiva e il sancire, come conseguenza di questa presunzione assoluta, una responsabilità penale per lo stesso titolo concretato dalla condotta attiva di un altro soggetto concreti una violazione evidente e completa del principio della personalità della responsabilità penale» che esclude ogni forma di responsabilità che «non sia autonomamente formulata sulla base di un fatto proprio del soggetto in questione»[51].

A sostegno della conformità dell'art 57 c.p. al dettato costituzionale va annoverato anche il tentativo di alcuni autori, quali il Nuvolone, di ravvisarvi una "responsabilità da posizione" legata alla funzione assunta liberamente dal soggetto nella piena consapevolezza dei rischi ad essa connessi[52].

La responsabilità sarebbe personale, anche se il fatto è commesso da altri, proprio in virtù dell'assunzione libera del ruolo rispetto a cui il rischio costituisce la stessa *ratio essendi*. Il maestro, detto ciò, puntualizzava come la responsabilità obbiettiva anomala del direttore del giornale non fosse pienamente in linea con il concetto di responsabilità personale per fatto proprio prospettata dalla dottrina più sensibile, invocando l'opportunità di una riforma che «pur senza muovere dall'erroneo presupposto di una inesistente incompatibilità, tenesse conto di questo concetto più moderno, nei limiti imposti dalle esigenze della materia»[53].

D'altro canto sembra condivisibile la posizione di quanti intravidero nella responsabilità per posizione una vanificazione non solo del nesso causale, ma anche della stessa rilevanza della condotta, la quale non può coincidere con

[51] Cfr. VASSALLI G., *Sulla illegittimità costituzionale dell'art. 57 n. 1 c.p.*, cit., p. 230.

[52] Cfr. NUVOLONE P., *I reati di stampa*, Milano, 1951, p. 177 ss.

[53] Cfr. NUVOLONE P., *Le leggi penali e la Costituzione*, cit., p. 40.

l'assunzione di un rischio totalmente integrato dalla condotta del terzo, senza che ciò comporti una allarmante assimilazione al paradigma della responsabilità oggettiva civile, lesiva non solo dell'art. 27 Cost. ma anche dell'art. 25, comma 2, Cost.[54].

La Corte Costituzionale, chiamata a pronunciarsi sulla legittimità dell'art. 57 c.p., con sentenza n. 3 del 15 giugno 1956 abbracciò un'interpretazione che attribuiva all'espressione "per ciò solo" funzione di distacco dal sistema dell'Editto Albertino[55]. La Suprema Corte dichiarò che «la responsabilità del direttore si fonda sulla circostanza, propria di lui, di non aver osservato gli obblighi di vigilanza e di controllo ai quali egli è tenuto per il fatto di essere direttore, obblighi che non è necessario rintracciare puntualmente espressi in un precetto legislativo, ma che ben possono desumersi dal sistema, come in questo caso del direttore del giornale: una figura della quale sono certi i lineamenti e quindi i diritti ed i doveri»[56].

Pur avvertendo la necessità di una riforma legislativa volta ad una revisione del contenuto dell'art. 57 c.p. onde renderlo «anche formalmente più adeguato alla norma costituzionale», la Corte ne escluse il contrasto con l'art. 27 Cost., in quanto il direttore risponderebbe per fatto proprio dato che la sua omissione risulterebbe legata all'evento non solo da un nesso materiale ma anche da «un certo nesso psichico (art. 40 Cod. pen.) sufficiente, come è opinione non contrastata, a conferire alla responsabilità il connotato della personalità»[57].

L'auspicata riforma, approvata con legge 4 marzo 1958 n. 127, ha previsto che, salva la responsabilità dell'autore della pubblicazione e fuori dei casi di concorso, qualora il direttore o il vice-direttore responsabile ometta di esercitare il

---

[54] Cfr. VASSALLI G., *Sulla illegittimità costituzionale dell'art. 57 n. 1 c.p.*, cit., p. 236; PISAPIA G. D., *La nuova disciplina della responsabilità per i reati commessi a mezzo stampa*, in *Rivista italiana di diritto e procedura penale*, 1958, p. 304 ss.; ALESSANDRI A., *Art. 27*, cit., p. 30.

[55] In riferimento alla sentenza della Corte Costituzionale n. 3/1956 cfr. PAGLIARO A., *Il fatto di reato*, cit., p. 413 ss.

[56] Cfr. Corte Costituzionale, sent. n. 3/1956, *Considerato in diritto 4*.

[57] Ivi, *Considerato in diritto 5.*

controllo necessario ad impedire la realizzazione di reati a mezzo stampa ed un reato sia commesso, egli sarà punito, a titolo di colpa, con la pena stabilita per tale reato, diminuita sino ad un terzo[58]. Con la modifiche apportate nel 1958, quindi,

l'obbligo di controllo sul contenuto del periodico «necessario ad impedire che col mezzo della pubblicazione siano commessi reati» è stato esplicitato ed è precipuamente sul fatto omissivo proprio che si fonda la responsabilità.

Nonostante gli sforzi prima ermeneutici, poi legislativi, la disciplina si presta, in realtà, ancora a numerose critiche.

Innanzitutto suscita perplessità il contenuto e l'estensione dell'«obbligo di controllo» nonché il significato del riferimento al «reato commesso», sorgendo il dubbio circa la necessità che lo stesso sia o meno perfetto in tutti i suoi elementi soggettivi ed oggettivi. Ma soprattutto risulta ambigua l'espressione «è punito a titolo di colpa»: il legislatore infatti non chiarisce quale sia l'elemento soggettivo del fatto omissivo, la natura ed il fondamento della responsabilità ma, con

[58] La legge n. 127/1958 ha rispettivamente introdotto e modificato anche i seguenti articoli: Art. 57 bis (Reati commessi col mezzo della stampa non periodica) «Nel caso di stampa non periodica, le disposizioni di cui al precedente articolo si applicano all'editore, se l'autore della pubblicazione è ignoto o non imputabile, ovvero allo stampatore, se l'editore non è indicato o non è imputabile». Art. 58 (Stampa clandestina) «Le disposizioni dell'articolo precedente si applicano anche se non sono state osservate le prescrizioni di legge sulla pubblicazione e diffusione della stampa periodica e non periodica». Art. 58 bis (Procedibilità per i reati commessi col mezzo della stampa) «Se il reato commesso col mezzo della stampa è punibile a querela, istanza o richiesta, anche per la punibilità dei reati preveduti dai tre articoli precedenti è necessaria querela, istanza o richiesta. La querela, la istanza o la richiesta presentata contro il direttore o vicedirettore responsabile, l'editore o lo stampatore, ha effetto anche nei confronti dell'autore della pubblicazione per il reato da questo commesso. Non si può procedere per i reati preveduti nei tre articoli precedenti se è necessaria un'autorizzazione di procedimento per il reato commesso dall'autore della pubblicazione, fino a quando l'autorizzazione non è concessa. Questa disposizione non si applica se l'autorizzazione è stabilita per le qualità o condizioni personali dell'autore della pubblicazione».

In riferimento agli artt. 57 ss. c.p. cfr. ROMANO M., *Commentario sistematico del Codice Penale*, Seconda Edizione, Milano, 1995, p. 579 ss.; MARINI G., DI LA MONICA M., MAZZA L., *Commentario al Codice Penale*, Torino, 2002, p. 517 ss.; MAMBRIANI A., *art. 57 c.p.,* in DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato*, Terza Edizione, Milano, 2011, p. 994 ss.

quell'inciso, sembra riferirsi solamente alla modalità o al "titolo" attraverso cui si il direttore o vice-direttore responsabile sono chiamati a rispondere di un determinato reato altrui.

A causa di tale ambiguità, parte della dottrina taccia anche la nuova disposizione di violazione del principio di personalità della responsabilità penale, ravvisando nella stessa una forma di responsabilità oggettiva[59].

Di contrario avviso si è mostrata la Corte di Cassazione, la quale ha più volte ribadito come la responsabilità del direttore responsabile che, con la sua condotta omissiva, abbia determinato una pubblicazione criminosa, non scaturisca oggettivamente bensì dall'inosservanza dell'obbligo giuridico di impedire che ciò avvenga. L'art. 57 c.p., secondo la Corte, costituirebbe un'autonoma ipotesi di reato colposo, strutturato in forma omissiva, nel quale l'evento è rappresentato dalla commissione di un reato tramite l'avvenuta pubblicazione criminosa. La prova della colpa si identificherebbe pertanto con la prova della omissione cosciente e volontaria del controllo sul periodico[60].

b) La responsabilità da reato degli enti

[59] Cfr. PISAPIA G. D., *La nuova disciplina della responsabilità per i reati commessi a mezzo stampa*, cit., p. 318 ss., il quale osserva criticamente come: «Da tale particolare configurazione della fattispecie legale deriva, anzi, la duplice conseguenza che viene trattata alla stessa stregua tanto l'omissione dolosa che quella colposa e, nel caso di omissione dolosa, si delinea l'anomalia di una punibilità a titolo di colpa per un fatto doloso. Il sistema adottato risente, in definitiva, della contraddizione d'aver creato, per il direttore responsabile della stampa periodica, una fattispecie legale autonoma e di averla poi inserita nella parte generale del codice, considerandola quasi come una forma di responsabilità *sui generis*, mentre più esattamente e coerentemente essa avrebbe dovuto essere collocata (una volta seguito quel sistema) nella parte speciale del codice. In tal modo si sarebbe evitata l'anomalia di applicare, anziché una pena autonoma, la pena stabilita per un reato diverso, eventualmente anche doloso, sia pure diminuita fino a un terzo».

[60] Cfr. *ex multis*, Corte di Cassazione, sent. n. 6787/1981; n. 10252/1981; n. 2840/1983; n. 9685/1997. In dottrina aderisce a tale interpretazione ANTOLISEI F., *Manuale di diritto penale. Parte generale*, Quindicesima Edizione integrata e aggiornata da L. Conti, Milano, 2000, p. 400.

L'art. 27, 1° comma, Cost., è stato a lungo considerato come una trasposizione a livello costituzionale dell'antico brocardo *societas delinquere non potest*[61]. Sia nell'accezione minima, che in quella più estesa, il principio della personalità osterebbe cioè alla risoluzione in termini positivi della *vexata quaestio* dell'ammissibilità di una responsabilità penale degli enti[62].

Due le argomentazioni poste a fondamento dell'idea delle società come *hortus clausus* impenetrabile dal diritto penale elaborate sulla base del dogma costituzionale in esame[63].

---

[61] Per un'analisi delle origini del brocardo *societas delinquere non potest* v. DE SIMONE G., *Persone giuridiche e responsabilità da reato. Profili storici, dogmatici e comparatistici*, Pisa, 2012, p. 40 ss.

[62] Cfr. ROMANO M., *Societas delinquere non potest (Nel ricordo di Franco Bricola)*, in *Rivista italiana di diritto e procedura penale*, 1995, p. 1036 ss., il quale, escludendo la configurabilità di una responsabilità propriamente penale delle persone giuridiche sulla base del dettato costituzionale, ammette, seppur cautamente, il superamento del *societas delinquere non potest* nel ristretto settore del diritto penale amministrativo.

[63] Da ricordare che, oltre all'argomento costituzionale, i sostenitori del brocardo in esame adducono quale motivazione del proprio convincimento, il pericolo della violazione del principio del *ne bis in idem*, data la possibilità, nel caso in cui si riconoscesse una responsabilità penale in capo agli enti, che la persona fisica risponda sia quale autore materiale dell'illecito sia quale parte dell'organo; nonché il rischio che vengano puniti anche i soci "innocenti", ovvero soggetti facenti parte dell'organismo sociale ma estranei allo specifico fatto di reato. In realtà tali asserti non sembrano condivisibili: il primo cade nel momento in cui si riconosce la soggettività autonoma dell'ente ed in riferimento alle piccole imprese, in cui la soggettività dell'ente molto spesso si confonde con quella della persona fisica, il pericolo "doppia punizione" potrebbe essere evitato attraverso specifiche cause di inapplicabilità o attenuazione della sanzione. Anche il secondo problema, relativo ai soci incolpevoli, pare facilmente superabile: le sanzioni che colpiscono l'ente si ripercuotono solo indirettamente sui soci, in favore dei quali potrebbero essere per lo più previste misure di salvaguardia quali forme particolari di recesso od indennizzi. La tesi del danno al socio innocente sembra per lo più confutabile nel momento in cui si riflette sulle sanzioni penali nel loro complesso: esse sono sempre ed inevitabilmente più o meno gravose anche per persone estranee al reato, si pensi ad esempio ai riflessi della pena detentiva nei confronti della famiglia del condannato. Cfr. PIERGALLINI C., *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 585 ss.; DOLCINI E., *Principi costituzionali e diritto penale alle soglie del nuovo millennio*, in *Rivista italiana di diritto*

In primo luogo, se la personalità della responsabilità penale ha come significato basilare il divieto di responsabilità per fatto altrui, l'ente non potrebbe mai essere chiamato a rispondere per il comportamento di un proprio dipendente o di un proprio organo, poiché sarebbe violata la necessaria coincidenza tra autore dell'illecito e destinatario della sanzione[64].

In secondo luogo, il filtro del principio di colpevolezza non farebbe che rafforzare la tesi dell'irresponsabilità penale delle *societas*, data l'incapacità di un loro atteggiamento volitivo colpevole che le pone per di più al di fuori dell'alveo del finalismo rieducativo proprio della pena[65].

Alla base di queste asserzioni vi è una lettura della persona giuridica e più in generale dell'ente in chiave finzionistica, sintetizzabile nell'affermazione kelseniana per cui le azioni ed omissioni possono essere soltanto azioni ed omissioni di un essere umano[66]. L'ente costituirebbe un mero "strumento di

---

e procedura penale, 1999, p. 22 ss.; PULITANÒ D., *La responsabilità da "reato" degli enti: i criteri di imputazione*, in *Rivista italiana di diritto e procedura penale*, 2002, p. 421 ss.

[64] Cfr. STORTONI L., *Profili penali delle società commerciali come imprenditori*, in *Rivista italiana di diritto e procedura penale*, 1971, p. 1165 ss., il quale critica le decisioni giurisprudenziali (in modo particolare la sentenza della Corte di Cassazione n. 610/1965) che ammettono la configurabilità del reato proprio dell'imprenditore o del datore di lavoro a carico dell'organo o dei soggetti appartenenti alla società.

[65] Cfr. PAGLIARO A., *Il fatto di reato*, cit., p. 366 ss. L'autore esclude categoricamente l'ammissibilità di una responsabilità penale delle persone giuridiche proprio per l'impossibilità di riferire alle stesse una pena o una misura di sicurezza senza dispenderne la specifica fisionomia. V. anche MAIELLO V., *La natura (formalmente amministrativa, ma sostanzialmente penale) della responsabilità degli enti nel D. Lgs. N. 231/2001: una truffa di etichette davvero innocua?*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 889 ss., il quale sostiene fermamente l'impraticabilità di una scelta di criminalizzazione dell'ente stante lo scopo della rieducazione che la Costituzione assegna alla pena. Secondo l'autore l'affermazione del principio *societas delinquere et puniri potest* comporterebbe la trasfigurazione del volto costituzionale del reato e della pena con conseguente deriva del diritto penale in una dimensione autoritaria ed arbitraria in cui anche il mero atteggiamento interiore potrebbe essere oggetto di incriminazione, giacché si costituirebbe una sorta di diritto penale parallelo foriero di effetti involutivi e pericoli per l'equilibrio dei rapporti soggetto-Stato.

[66] Con riguardo agli elementi essenziali della teoria della finzione ed alle intuizioni di Savigny, cfr. GALGANO F., *Delle persone giuridiche*, in *Commentario del Codice Civile Scialoja –*

tecnica legislativa" ed il principio *societas delinquere non potest* sarebbe pertanto strettamente connesso all'incapacità di azione, di colpevolezza e di rieducazione dell'ente[67].

In realtà in dottrina è stato ben presto evidenziato come, anche sulla scorta dell'analisi comparatistica dell'esperienza di numerosi paesi di *Civil* e *Common Law*[68], la cd. "teoria della *fictio*" ed i divieti da essa derivanti, lungi dal rappresentare dogmi precostituiti, impedimenti costituzionali ed ontologici,

---

Branca, Bologna, Roma, 2006, p. 3 ss.; DE SIMONE G., *Persone giuridiche e responsabilità da reato*, cit., p. 53 ss.

[67] Cfr. RIVERDITI M., *La responsabilità degli enti un crocevia tra repressione e specialprevenzione*, Napoli, 2009, p. 10.

[68] Sotto il profilo comparatistico numerosi i Paesi europei ed extraeuropei dotatisi di modelli di responsabilità penale degli enti. In modo particolare il superamento del principio *societas delinquere et puniri non potest* risale al 1882 nello Stato di New York, con l'introduzione della responsabilità penale delle persone giuridiche nel relativo Codice Penale; al 1948 in Gran Bretagna con il Criminal Justice Act. Più recente la svolta nei paesi di *Civil Law*: la Francia ha previsto la responsabilità penale delle *personnes morales* con il nuovo Codice Penale del 1994; mentre in Spagna, con la Ley Organica 5/2010, è stato inserito nel Codigo Penale il nuovo art. 31 *bis*, destinato a disciplinare le materia della responsabilità da reato delle persone giuridiche. Cfr. BRICOLA F., *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Rivista italiana di diritto e procedura penale*, 1983, p. 962 ss.; TIEDEMANN K., *La responsabilità penale delle persone giuridiche nel diritto comparato*, in *Rivista italiana di diritto e procedura penale*, 1995, p. 615 ss.; DE SIMONE G., *Persone giuridiche e responsabilità da reato*, cit., p. 24 ss.

Per quanto riguarda le scelte adottate a livello comunitario cfr. PALIERO C.E., *Le sanzioni comunitarie quale modello di disciplina per la responsabilità da reato delle persone giuridiche*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008, p. 173 ss.; MAUGERI A. M., *I principi fondamentali del sistema punitivo comunitario: la giurisprudenza della Corte di Giustizia e della Corte europea dei diritti dell'uomo*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo*, cit., p. 138 ss. V. inoltre MAUGERI A. M., *Il sistema sanzionatorio comunitario dopo la Carta europea dei diritti fondamentali*, in GRASSO G., SICURELLA R. (a cura di), *Lezioni di diritto penale europeo*, Milano, 2007, p. 99 ss.

costituiscono il frutto di scelte di politica criminale, e pertanto risultano contraddistinti dai caratteri della relatività e mutevolezza[69].

Il principio *societas delinquere non potest* sarebbe pertanto ampiamente superabile per raggiungere forme di controllo e prevenzione più efficaci della criminalità economica realizzata attraverso gli schemi societari.

Alla "teoria della *fictio*" si contrappone la "teoria della realtà" o "teoria organica" che considera la persona giuridica come "organismo naturale" al pari dell'uomo, la cui capacità non vivrebbe solo nel mondo delle norme ma avrebbe una base fisico-naturalistica, empirica, da porre a fondamento dell'imputazione del fatto dell'organo all'ente[70].

---

[69] Lo stesso Stortoni, pur riconoscendo l'esistenza di numerosi ostacoli all'applicabilità delle norme penali alle società, si sforza di dimostrare come gli stessi siano strettamente connessi a ragioni di ordine pratico, di opportunità ed efficienza. Cfr. STORTONI L., *Profili penali delle società commerciali come imprenditori*, cit., p. 1180. V. inoltre MARINUCCI G., *Il reato come "azione". Critica di un dogma*, Milano, 1971, p. 175, il quale magistralmente affermava come «basta volgere infatti lo sguardo agli ordinamenti penali contemporanei di popoli civilissimi, per notare che quel "non potest" viene colà largamente superato, senza che si avverta minimamente la ripugnanza che possono sentire solo coloro che scambiano per un limite logico, e per una verità eterna e intangibile, il mero prodotto concettuale estratto dalle norme del diritto positivo, vigente *hic et nunc*, con il quale e sul quale si sta lavorando». Il compianto maestro specificava quindi che a vietare l'introduzione in un dato ordinamento del principio *societas delinquere potest* non può essere un precostituito "concetto di azione".

[70] La relazione che intercorre tra le persone fisiche e l'ente rappresenterebbe una forma particolare di rappresentanza. Non si rinviene, infatti, né la duplice volontà (del rappresentante e del rappresentato), giacché non può naturalmente esistere una volontà propria che promani dall'ente, né la compenetrazione piena tra la persona fisica titolare dell'organo e la persona giuridica. Si tratterebbe di una sorta di coordinazione in virtù della quale la volontà di uno o più individui interviene necessariamente come elemento attivo di un'altra personalità che altrimenti non potrebbe esprimersi. Cfr. TRABUCCHI A., *Istituzioni di diritto civile*, Padova, 2004, p. 293 ss.; CASETTA E., *Manuale di diritto amministrativo*, Milano, 2012, p. 135 ss.; per un'analisi delle teorie degli autori tedeschi di riferimento, quali ad esempio quella elaborata da Gierkie, ed un richiamo alla letteratura in merito v. GALGANO F., *Delle persone giuridiche*, cit., p. 6; BRICOLA F., *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, cit., p. 956.

L'accoglimento della teoria organicistica, come evidenziato da Franco Bricola, permetterebbe di considerare come "propri" dell'ente i fatti realizzati dalle persone fisiche dell'organo, rendendo compatibile il dogma *societas delinquere potest* con il principio di personalità, per lo meno nel suo significato minimo di divieto di responsabilità per fatto altrui[71].

Anche tale ricostruzione si è prestata tuttavia a penetranti critiche: l'immedesimazione dell'ente nell'organo e quindi la riferibilità dell'azione del secondo direttamente al primo costituirebbe, nella sostanza, null'altro che una finzione legale comportante la lesione dello stesso principio di personalità: «poiché la regola secondo cui un soggetto non deve essere chiamato a rispondere per un'azione altrui ha come suo preciso rovescio che l'autore della medesima non possa venire esentato dalle sue responsabilità in nome dell'addebito delle stesse ad un soggetto diverso –nella specie la persona giuridica– che assorbirebbe sul piano del diritto positivo la sua personalità»[72].

---

[71] Viceversa, non sarebbe superabile il contrasto con la più ampia interpretazione dell'art. 27 Cost. che ravvisa in esso la costituzionalizzazione del principio di colpevolezza, non essendo possibile, nemmeno attraverso l'immedesimazione organica, "inventare" per la società i presupposti su cui si fonda il giudizio di rimproverabilità. Per tali ragioni il maestro Bricola prospetta l'applicabilità agli enti non delle pene bensì delle misure di sicurezza, nel cui ambito il principio di personalità sarebbe accolto nella sua portata minima (BRICOLA F., ult. op. cit., p. 1011). In senso critico v. ALESSANDRI A., *Art. 27*, cit., p. 159, il quale afferma che «una volta negata l'alterità tra organo ed ente riguardo al fatto materiale non si possono poi erigere barriere "logiche" allo scopo di negare l'immedesimazione anche per la volontà colpevole: è in gioco un meccanismo di imputazione normativa, non si intendono certo rintracciare le dinamiche psicologiche del "macroantropo"». Cfr. infine PECORELLA G., *Societas delinquere potest,* in *Rivista giuridica del lavoro*, 1977, p. 363, il quale sostiene invece che l'art. 27 Cost., non operando alcuna distinzione, equipara ai fini della personalità della responsabilità tutte le conseguenze *lato sensu* sanzionatorie che discendono dal reato, misure di sicurezza comprese: «Non si afferma che, si badi, l'art. 27 Cost. rappresenta un ostacolo all'applicazione di sanzioni penali alle società: come si dirà, siamo certi del contrario. Si vuole sostenere, piuttosto, che, dal punto di vista della Costituzione, o è consentita la responsabilità penale delle persone giuridiche, ed allora è ammissibile anche la pena nei loro confronti, o è vietata, perché si avrebbe sempre una responsabilità per fatto altrui, ed allora non sono legittime né le pene né le misure di sicurezza».

[72] Cfr. GROSSO C. F., voce *Responsabilità penale*, cit., p. 712. L'Autore, inoltre, mostra scetticismo anche per il fatto che, attraverso la teoria organicistica e quella finzionistica, la

Lo slancio verso un parziale superamento del dogma dell'irresponsabilità degli enti è stato supportato non solo dall'evoluzione interpretativa offerta dalla dottrina più sensibile[73] ma anche da ragioni eminentemente pratiche. D'altro canto il "costo" sociale dell'irraggiungibilità degli enti da parte dello strumento penale[74], le tendenze registrate nel contesto criminologico[75], le politiche

---

soluzione di un problema di interpretazione del diritto penale dipenderebbe dalla preventiva adesione ad uno modello extrapenale di rapporti intercorrenti tra i soggetti e l'ente.

[73] A tal proposito par d'uopo ricordare le parole di PULITANÒ D., *La responsabilità da "reato" degli enti: i criteri di imputazione*, cit., p. 422: «se la persona giuridica è costruita dall'ordinamento come soggetto capace d'agire, di esercitare diritti, di assumere obblighi, di svolgere attività da cui trarre profitto, ovviamente per il tramite di persone fisiche agenti per l'ente, è nella logica di un tale istituto che all'ente possa essere ascritto sia un agire lecito che un agire illecito, realizzato nella sfera di attività dell'ente stesso. […] La ragione sistematica conduce dunque a concludere che vi è contraddizione fra il riconoscere gli enti collettivi come 'soggetti protagonisti del sistema', ed il pretendere per essi, in nome di principi di garanzia pensati per le persone fisiche, 'una completa immunità nei confronti del sistema penale […] Lungi dal fungere da garanzia della certezza d'azione, come il "principio di colpevolezza" intende essere, la tesi che nega in radice la "capacità di colpevolezza" delle persone giuridiche è supporto ideologico di pretese di ingiustificato privilegio». La necessità di un intervento penale è ben evidenziata anche da FLICK M. G., *Problemi attuali e profili costituzionali del diritto penale d'impresa*, in *Rivista italiana di diritto e procedura penale*, 1983, p. 433 ss.

[74] Cfr. per tutti BRICOLA F., *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, cit., p. 951 ss. L'autore, nella sua lucida analisi, mostra gli elevati "costi" in termini di efficienza punitiva e di tutela dei beni giuridici che comporta il mantenimento del brocardo *societas delinquere et puniri non potest*.

[75] Cfr. PIERGALLINI C., *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, cit., p. 576 ss. L'autore individua, quali tratti caratterizzanti lo scenario politico-criminale a partire degli anni '60, l'incremento dei cd. *white collar crime*, espressivi di vere e proprie scelte aziendali, e dei cd. *reati del profitto*, quale il riciclaggio, spesso connessi alla criminalità organizzata; nonché l'aumento delle illiceità tipiche della *società del rischio* a "vittimizzazione di massa". Le costanti criminologiche strettamente concernerti la criminalità d'impresa sarebbero invece rappresentate dalla cd. *dominante collettiva*, ovvero la riferibilità degli illeciti di impresa a decisioni collegiali presupponenti una molteplicità variegata di fasi che coinvolgono una pluralità di soggetti; ed in secondo luogo dalla *capacità dell'ente di indurre la criminalità d'impresa.* Tramite quest'ultima espressione si vuole indicare l'idea di *societas* quale luogo in cui l'agire, sia lecito che illecito, viene organizzato: l'ente crea e sviluppa un proprio indirizzo strategico, una propria cultura della

dell'Unione europea e la necessità di adeguamento agli *standard* sopranazionali ed internazionali[76], hanno reso sempre più pressante l'esigenza di un intervento del legislatore.

E' con la legge delega n. 300/2000 ed il successivo decreto legislativo di attuazione n. 231/2001 che il nostro ordinamento si è dotato di un modello generale di responsabilità punitiva degli enti collettivi[77], che si affianca alla semplice responsabilità sussidiaria "collettiva" di cui all'art. 197 c.p.[78], e prevede la responsabilità cumulativa della persona giuridica e della persona fisica.

---

legalità o dell'illegalità. Solo in rarissimi casi, quindi, il reato è frutto di malfunzionamento episodico.

[76] In particolare v. Raccomandazione del Comitato dei Ministri del Consiglio d'Europa n. 88/1988; Convenzione OCSE sulla lotta alla corruzione dei funzionari stranieri del 17.12.1997; Convenzione sulla tutela finanziaria delle Comunità europee (PIF), Secondo Protocollo, del 19.06.1997.

[77] A commento v. DE SIMONE G., *Persone giuridiche e responsabilità da reato*, cit., p. 303 ss.; DE MAGLIE C., *Principi generali e criteri di attribuzione della responsabilità*, in *Diritto Penale e Processo*, n. 11/2001, p. 1348 ss.; PIERGALLINI C., *Sistema sanzionatorio e reati previsti dal codice penale,* in *Diritto Penale e Processo*, n. 11/2001, p. 1353 ss.; PATRONO P., *Verso la soggettività penale degli enti*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 183 ss.; PALIERO C.E., *La responsabilità delle persone giuridiche: profili generali e criteri di imputazioni*, in ALESSANDRI A. (a cura di), *Il nuovo diritto penale delle società*, Milano, 2002; RONCO M., *Responsabilità delle persone giuridiche*, in *Enciclopedia giuridica*, 2002, p. 1 ss.; ALESSANDRI A., *Note penalistiche sulla nuova responsabilità delle persone giuridiche*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 33 ss.; PIERGALLINI C., *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, cit., p. 571 ss.; MANNA A., *La c.d. responsabilità amministrativa delle persone giuridiche: un primo sguardo d'insieme*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 501 ss.; MAIELLO V., *La natura (formalmente amministrativa, ma sostanzialmente penale) della responsabilità degli enti nel D. Lgs. N. 231/2001*, cit., p. 879; DE SIMONE G., *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, in penalecontemporaneo.it, 28 Ottobre 2012.

[78] L'art. 197 c.p. prevede l'obbligazione civile delle persone giuridiche per il pagamento delle multe e delle ammende in caso di insolvibilità dell'autore materiale del reato. Quest'ultimo deve avere la rappresentanza o l'amministrazione dell'ente, oppure esservi legato da rapporto di dipendenza. L'illecito, infine, deve essere stato realizzato in violazione degli obblighi inerenti alla qualità del soggetto agente, ovvero, nell'interesse della persona giuridica.

«Forse per non aprire i delicati conflitti con i dogmi personalistici dell'imputazione criminale di rango costituzionale (art. 27 Cost.)»[79] la responsabilità introdotta è etichettata come "amministrativa", sebbene sia ancorata a presupposti e garanzie proprie del diritto penale che ne rendono molto controversa la natura[80].

Trattasi di responsabilità limitata in riferimento sia agli enti cui si rivolge – enti forniti di personalità giuridica nonchè società ed associazioni anche prive della personalità giuridica, con esclusione dello Stato, degli enti pubblici territoriali, degli enti non economici e degli altri enti che svolgono funzioni costituzionali – sia ai reati che fungono da presupposto per l'esistenza dell'illecito di cui l'ente è chiamato rispondere, circoscritti a quelli tassativamente elencati.

Quanto ai criteri di attribuzione della responsabilità il decreto, come chiarito nella relativa Relazione, propone il modello della teoria organica: per garantire l'identità tra autore del reato e destinatario della sanzione, ai sensi dell'art. 5, l'ente è responsabile dei reati commessi nel suo interesse e nel suo vantaggio da soggetti in "posizione apicale", cioè da persone con funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa con

---

[79] Cfr. Cassazione penale, sent. 20 dicembre 2005, n. 3615.

[80] Tratti che, a dispetto del *nomen juris*, farebbero propendere per una responsabilità sostanzialmente penale, sono ad esempio: il richiamo del principio di legalità e divieto di analogia sia in relazione al reato che alla sanzione (art. 2); il regime della successione delle leggi (art. 3); la disciplina concernente i reati commessi all'estero (art. 4); il criterio soggettivo di imputazione del reato all'ente sulla base della "colpa di organizzazione" (art. 6-7); la disciplina delle pene pecuniarie a quote e delle pene interdittive (artt. 9 ss.); la regolamentazione del procedimento di accertamento dinnanzi al giudice penale mediante le norme del codice di procedura penale (artt. 34 ss.). Viceversa aspetti dissonanti rispetto alla qualificazione in termini penalistici della responsabilità sono: il regime della prescrizione (art. 22); ed il trasferimento della responsabilità ai nuovi soggetti risultanti da vicende modificative dell'ente (artt. 29-39). Per un'analisi approfondita dei diversi aspetti v. DE VERO G., *La responsabilità penale delle persone giuridiche*, Milano, 2008.

La giurisprudenza, come la dottrina, ha mostrato posizioni contrastanti: cfr. Cass. civ., sez. un., sent. 30 settembre 2009, n. 20936; Cass. pen., sent. 29 dicembre 2005, n. 3615, in cui si propende per una lettura in termini penalistici; viceversa cfr. Cass. pen., sent. 9 luglio 2009, n. 360833 e sent. 16 luglio 2010, n. 27735, nelle quali si accoglie la tesi del *tertium genus* (così come si afferma nella *Relazione Ministeriale al d.lgs. 231/2001*).

autonomia finanziaria e funzionale, o persone che esercitano, anche di fatto, la gestione o il controllo dell'ente; oppure da soggetti sottoposti alla direzione vigilanza di uno dei soggetti in posizione apicale, sempre che i suddetti soggetti non abbiano agito nell'interesse esclusivo proprio o di terzi[81]. E' richiesta inoltre una "colpa d'organizzazione", cioè la mancata adozione o inefficacia attuazione di un modello di organizzazione e di gestione idoneo a prevenire reati della specie di quello verificatosi, ovvero il mancato affidamento del compito di vigilare sul funzionamento e sull'osservanza dei modelli all'organismo autonomo dell'ente. In alternativa è necessaria la sussistenza del cd. dolo dell'ente ovvero sia l'esistenza di una politica di impresa finalizzata alla commissione del reato: l'ente o uno sua unità organizzativa devono essere stabilmente utilizzati a scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la responsabilità (art. 16).

Per il principio dell'autonomia della responsabilità dell'ente (art. 8), questa sussiste anche quando l'autore dell'illecito non è identificato, non è imputabile o il reato si estingue per cause diverse dall'amnistia. Tale disposizione ha sicuramente il pregio di aver preso atto del processo di decentralizzazione tipico dell'imprese moderne, nelle quali è spesso complicato se non impossibile l'individuazione della persona fisica autore del reato presupposto, ma, evidentemente, mal si concilia con il criterio dell'immedesimazione organica

[81] Nel primo caso l'onere di provare l'assenza di una colpa d'organizzazione grava sull'ente, mentre, nel secondo l'onere della prova grava sull'accusa. V. Art. 6, 1° comma, d.lgs. n. 231/2001: «*Soggetti in posizione apicale e modelli di organizzazione dell'ente:* Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che: a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)». Per alcuni autori la presunzione di colpevolezza nel caso di reato realizzato dai soggetti in "posizione apicale" risulta talmente forte che i requisiti per superarla sono stati definiti come oggetto di *probatio diabolica.* In tal senso v. FERRUA P., *Le insanabili contraddizioni nella responsabilità dell'impresa*, in *Diritto e Giustizia*, n. 29/2001, p. 79 ss.

recepito nell'art. 5: come si potrebbe infatti escludere che il soggetto abbia perseguito il proprio esclusivo interesse quando non lo si identifica? Nonostante la previsione di criteri di imputazione soggettiva, la colpevolezza dell'ente risulta quindi per alcuni versi per lo più legata alla "condotta di vita", e non al fatto[82].

5. PROSPETTIVE *DE IURE CONDENDO:* UNA NUOVA LETTURA DELLA "PERSONALITÀ" DELLA RESPONSABILITÀ PENALE

Parte della dottrina ha evidenziato come le resistenze all'introduzione di una responsabilità diretta degli enti facenti leva sull'art. 27 Cost. siano ancorate ad una interpretazione eccessivamente "antropomorfica" del principio, che potrebbe invece essere oggetto di una lettura "evolutiva" onde permettere un riequilibrio del sistema[83].

Nella criminalità d'impresa la persona fisica è raramente autore esclusivo dell'illecito. Il reato d'impresa, nella maggior parte dei casi, richiede necessariamente una struttura organizzata per la sua realizzazione, che rende insufficiente la punizione del singolo.

Come sottolineato nella Relazione Ministeriale al d.lgs. 231/2001 proprio la mancata previsione di una forma di responsabilità della persona giuridica in relazione a comportamenti in linea o comunque discendenti dalla politica aziendale, insieme al costume di rinnovare frequentemente e sistematicamente i centri di imputazione formali all'interno della stessa, si risolvono paradossalmente nell'aggiramento di quel principio di responsabilità personale che ha rappresentato la remora più sensibile all'adozione da parte dell'Italia di questo nuovo modello sanzionatorio. Non solo, oltre all'aggiramento del principio di

[82] Cfr. PATRONO P., *Problematiche attuali dell'errore nel diritto penale dell'economia*, cit., p. 190 ss.

[83] Cfr. MANNA A., *La c.d. responsabilità amministrativa delle persone giuridiche: un primo sguardo d'insieme*, cit., p. 504 ss. In senso critico cfr. CASTELLANA A. M., *Diritto penale dell'Unione europea e principio «societas delinquere non potest»*, in *Rivista trimestrale di diritto penale dell'economia*, 1996, p. 793 ss.

personalità, punendo solo la persona fisica non si tutelano efficacemente i beni giuridici coinvolti nella moderna attività d'impresa[84].

Responsabilità "personale" non deve essere quindi confusa con responsabilità "individuale". Alcuni autori hanno perfino sostenuto, proprio sulla base di questo ragionamento, che se il Costituente nel momento della redazione dell'art. 27 Cost. sicuramente aveva come riferimento la persona fisica, il principio in esso contenuto dovrebbe essere applicato in modo circoscritto solamente a quest'ultima.

Pur non estremizzando l'*iter* logico in tali termini, sembra potersi aderire all'idea secondo la quale, se è evidente che il paradigma fondante la cultura penalistica fin dalle sue origini è quello del criminale e della vittima considerati in termini individualistici, e che la persona fisica è l'unica ad essere considerata nel diritto penale tradizionale, ciò non significa necessariamente che il Costituente abbia voluto totalmente escludere la responsabilità penale dei soggetti che non siano persone fisiche[85].

Indipendentemente dall'adesione alla teoria della finzione o a quella organicistica, superando la concezione delle categorie penalistiche lette in una dimensione solo "individualistica", le costanti criminologiche che spingono in direzione di una criminalizzazione della *societas* potrebbero trovare un'adeguata formalizzazione penalistica ricorrendo a categorie che permettano di tipizzare sia i criteri di imputazione, oggettiva e soggettiva, dell'illecito all'ente, sia le sanzioni funzionali agli obiettivi di prevenzione e "rieducazione".

In primo luogo, per quanto riguarda l'azione, se la persona giuridica può stipulare contratti vincolandosi agli obblighi civilistici ad essi connessi, la conclusione secondo la quale l'ente può rendersi anche autore di violazioni sembra più che scontata. La *societas* può agire illecitamente: con tale ammissione non si fa nulla di più che permettere al diritto di esprimere lo stesso giudizio sugli

[84] Cfr. ALESSANDRI A., *Note penalistiche sulla nuova responsabilità delle persone giuridiche*, cit., p. 33 ss.

[85] Cfr. PECORELLA G., *Societas delinquere potest*, cit., p. 366 ss.

enti formulato dalla realtà sociale, superando la concezione naturalistica di azione [86].

In riferimento alla colpevolezza, solo continuando ad attribuirle connotati psicologici, etici e morali modellati sulla persona umana si può concludere per una impossibilità di responsabilità colpevole dell'ente[87]. In modo particolare, l'abbandono della concezione psicologica in favore dell'accoglimento della cd. concezione normativa, permetterebbe di eliminare il "sostrato antropomorfico" quale presupposto necessario ed ineludibile della punibilità[88].

Non sembrano insuperabili nemmeno le pretese di impossibilità di "rieducazione" dell'ente. Meccanismi quali i *compliance programs*, volti a prevenire il rischio di commissione di reati, e la valorizzazione ad esempio delle condotte *post factum*, non possono che dimostrare, infatti, come la finalità special-preventiva di rieducazione dell'ente sia senz'altro perseguibile, per lo più in una forma particolarmente penetrante, permettendo di promuovere una politica aziendale volta alla legalità[89].

Alla luce di una lettura evolutiva del principio costituzionale di cui all'art. 27 Cost. e del contenuto delle categorie del diritto penale l'adesione al dogma *societas delinquere non potest* non pare niente affatto necessitata. Si tratta di una scelta che il legislatore, senza timori di una violazione della lettera e dello spirito del principio costituzionale, deve operare sulla base di valutazioni politiche,

---

[86] Cfr. TIEDEMANN K., *La responsabilità penale delle persone giuridiche nel diritto comparato*, cit., p. 626.

[87] Cfr. BRICOLA F., *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, cit., p. 956.

[88] Questo viene sottolineato anche nella Relazione Ministeriale al d.lgs. 231/2001. Cfr. PIERGALLINI C., *Societas delinquere non potest: la fine tardiva di un dogma*, cit., p. 583. In senso contrario v. MAIELLO V., *La natura (formalmente amministrativa, ma sostanzialmente penale) della responsabilità degli enti nel D. Lgs. N. 231/2001*, cit., p. 884 ss., il quale critica fortemente questa posizione sostenendo che la vigente disciplina costituzionale continua a rappresentare un ostacolo insormontabile all'introduzione di una forma di responsabilità penale dell'ente e che quindi l'unica via percorribile è quella della innovazione costituzionale.

[89] Cfr. DOLCINI E., *Principi costituzionali e diritto penale alle soglie del nuovo millennio*, p. 24.

rispettose degli impulsi sovranazionali e dei dati empirici. A tal riguardo i recenti scandali di grosse imprese e società multinazionali (quali Parmalat, Monte dei Paschi di Siena, Siemens, Volkswagen, ecc.) non fanno che confermare l'insufficienza dei tradizionali strumenti di prevenzione e contrasto alla grande criminalità economica ancorati al paradigma tradizionale della responsabilità penale delle singole persone fisiche e ad un sistema di prevenzione sostanzialmente interno o settoriale. La struttura organizzata delle imprese e delle società commerciali, anche multinazionali, ed il loro *modus operandi* presentano spesso similitudini rispetto a quelli della criminalità organizzata. Anche in virtù di tali convergenze forse si potrebbe riflettere, a partire dalle fonti sovranazionali[90],

[90] A livello sovranazionali numerose sono le fonti che interessano entrambe le tipologie di criminalità in settori specifici: quali la corruzione, le frodi in sovvenzioni, il riciclaggio, il finanziamento del terrorismo, gli illeciti nei mercati finanziari, i delitti contro l'ambiente ed in specie il traffico di rifiuti, il traffico d'organi, la tratta degli esseri, la responsabilità di imprese ed enti per i crimini internazionali (che seppur non prevista normativamente è oggetto di ampia discussione e di recente giurisprudenza). V. Convenzione ONU contro la criminalità organizzata transnazionale, siglata a Palermo nel 2000, che già prevede – con i relativi protocolli addizionali - reati transnazionali riconducibili (anche) alla criminalità d'impresa, per cui è stabilita la responsabilità degli enti, come nel caso emblematico del riciclaggio, mentre in ambito europeo si considerino i diversi strumenti, dalla decisione quadro 2008/841/GAI contro la criminalità organizzata fino all'ultima direttiva 2014/42/UE in materia di confisca di proventi illeciti. V. inoltre Convenzione per la protezione degli interessi finanziari europei del 26 luglio 1995 con i due protocolli addizionali del 1996 e 1997, che interessano le frodi, la corruzione, il riciclaggio, nonché la responsabilità delle persone giuridiche per questi reati. Più in specifico in materia di corruzione v. la Convenzione ONU di Merida 14 dicembre 2005, con misure repressive e preventive volte a prevenire anche il riciclaggio di denaro, e le Convenzioni del Consiglio d'Europa del 27 gennaio 1999 e dell'Unione europea del 26 maggio 1997, oltre alla decisione quadro 2003/568/GAI relativa alla lotta contro la corruzione nel settore privato; in materia di finanziamento del terrorismo v. la Convenzione ONU del 1999 e le risoluzioni del Consiglio di sicurezza del 2001, la Convenzione di Varsavia del Consiglio d'Europa sulla prevenzione del terrorismo del 16 maggio 2005 e le decisioni quadro 2002/474/GAI e 2008/919/GAI in materia di lotta al terrorismo, che dovrebbero a breve essere sostituite da una direttiva specifica. In materia di riciclaggio le direttive europee 91/308/CEE, 2001/97/CE, 2005/60/CE sono state sostituite dall'ultima "quarta" direttiva 2015/849 del 20 maggio 2015, che si estende a misure contro il finanziamento del terrorismo; la direttiva 2014/57/UE stabilisce ora sanzioni penali contro gli abusi di mercato mentre il coevo regolamento n. 596/2014 prevede la disciplina extrapenale e le

sull'introduzione di un diritto penale dell'impresa imperniato specificamente su "delitti di organizzazione". Sembrerebbe infatti profilarsi sempre più una responsabilità non da "mancata organizzazione", così come delineata del d.lgs. 231/200, ma "da organizzazione" dell'ente.

Anche le caratteristiche del *cyberspace*, che si analizzeranno nel capitolo successivo, non fanno che confermare la necessità del superamento del dogma della personalità intesa come responsabilità "dell'individuo" e della creazione di un vero e proprio terzo genere di responsabilità autonoma dell'ente che, prescindendo consapevolmente dal soggetto persona-fisica, si sostanzi in fattispecie specifiche di parte speciale.

---

sanzioni amministrative; in materia di protezione penale dell'ambiente si considerino le direttive 2009/123/CE e 2008/99/CE, conseguenti all'annullamento della decisione-quadro 2003/80/GAI (Corte di Giustizia Europea 13 settembre 2005 C-176/03), nonché la Convenzione del Consiglio d'Europa sulla protezione dell'ambiente attraverso il diritto penale del 4 novembre 1998; infine in materia di traffico d'organi v. la Convenzione del Consiglio d'Europa contro il traffico di organi umani del 25 marzo 2015 e la Direttiva 2011/36/UE contro la tratta di persone. Cfr. inoltre il Piano d'azione UE per il periodo 2014-2020 volto a reprimere la criminalità organizzata, approvato dalla Commissione speciale sulla criminalità organizzata, la corruzione e il riciclaggio di denaro, istituita nel marzo 2012, ed i vari *reports* degli organismi internazionali sull'attuazione di detti strumenti.

CAPITOLO SECONDO

CONTESTO DI RIFERIMENTO: IL *CYBERSPACE*

SOMMARIO: 1. *Internet service provision* - 2. L'impatto di Internet sulla criminalità - 3. La "criminalità informatica" ed i "*cybercrimes*" - 4. Impulsi sovranazionali nella lotta ai *cybercrimes* - 5. La normativa penale italiana in materia di criminalità informatica - 6. (segue) Il decreto Cyber-Sicurezza (DPCM 24.01.2013).

1. *INTERNET SERVICE PROVISION*

La questione inerente all'*an* e al *quomodo* della responsabilità penale degli *Internet Service Providers* (ISPs) richiede una preliminare analisi di alcuni aspetti tecnici concernenti la struttura di Internet.

La prima definizione ufficiale del termine "Internet", contrazione della locuzione «*interconnected networks*», venne fornita dal Federal Networking Council (FNC) statunitense, comitato costituito dallo U.S. National Science and Technology Council's Committee on Computing, Information and Communications (CCIC)[1] nel 1995, al fine di coordinare lo sviluppo dell'utilizzo delle tecnologie telematiche da e tra le agenzie federali.

Nella risoluzione del 24 ottobre 1995 l'FNC statuì che Internet «*refers to the global information system that – (i) is logically linked together by a globally*

[1] Vi partecipano tra gli altri il Department of Defense, il Department of Energy, la DARPA (Defense Advanced Research Projects Agency), l'NSF (National Science Foundation) e la NASA (National Aeronautics and Space Administration).

unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein»[2].

Si tratta di un'interconnessione globale tra reti informatiche di diversa natura ed estensione, resa possibile da una *suite* di protocolli (TCP/IP)[3], che costituiscono la "lingua" comune con cui i *computer* connessi ad Internet (gli *host*) comunicano tra loro ad un livello superiore, indipendentemente dalla loro sottostante architettura *hardware* e *software*, garantendo così l'interoperabilità tra sistemi e sotto-reti fisiche diverse[4].

---

[2] La risoluzione in esame è consultabile in nitrd.gov.

[3] Insieme delle regole che permettono il processo di comunicazione in rete tra terminali e apparati diversi (*host*, *computer* clienti, s*martphone*, *personal digital assistant*, *monitor*, stampanti, etc.).

La struttura della *suite* di protocolli internet è stata schematizzata a livelli *(layer)*.

Lo standard *de iure* nell'ambito delle reti dati è rappresentato dal modello ISO-OSI (*Open Systems Interconnection***)**, composto da sette livelli (1. Livello fisico 2. Livello di collegamento 3. Livello di rete 4. Livello di trasporto 5. Livello di sessione 6. Livello di presentazione 7. Livello di applicazione). Ogni livello esegue una specifica serie di operazioni in un crescendo dall'interfaccia di rete a quella dell'utente.

Lo standard *de facto* è invece rappresentato dalla *suite* di protocolli TCP/IP, chiamata così per sineddoche in funzione dei due più importanti protocolli in essa definiti: il *Transmission Control Protocol* (TCP) e l'*Internet Protocol* (IP), che, a differenza del modello ISO/OSI, presenta quattro livelli (1. Livello di accesso alla rete 2. Livello di rete 3. Livello di trasporto 4. Livello di applicazione).

Cfr. CANNON R., *The Legacy* of *the Federal Communications Commission's Computer Inquiries*, in *Federal Communication Law Journal*, n. 55/2003, p. 194 ss.

[4] Cfr. COMER D. E., *Internetworking con TCP/IP. Principles, Protocols and Architecture*, New York, 2006, p. 37. A livello fisico, la rete Internet può essere vista come una complessa interconnessione di nodi con funzionalità di ricetrasmissione, appoggiata a collegamenti trasmissivi di vario tipo, sia cablati che *wireless* (fibre ottiche, cavi coassiali, doppini telefonici, cavi elettrici in posa anche in strutture idrauliche, collegamenti sottomarini, collegamenti satellitari, collegamenti a radiofrequenza (*Wi-Fi*) e su ponti radio). Attraverso un *modem* o un *router*, si collega innanzitutto il proprio *computer* con l'ISP, che, a seguito della stipulazione di un

La "rete delle reti" assume così una struttura che viene definita "anarchica", non registrandosi alcuna gestione centralizzata ed essendo basata sostanzialmente sulla volontaria adesione all'accordo internazionale relativo ai protocolli di rete. Ciò è dovuto alla finalità per la quale Internet fece la sua comparsa alla fine degli anni sessanta, ovvero assicurare la connettività tra diversi *computer* e l'operatività della stessa anche in caso di attacco atomico[5].

Attualmente Internet rappresenta il principale mezzo di comunicazione di massa[6] e la tipologia delle funzioni offerte è ormai molto variegata[7], comprendendo il servizio *World Wide Web*, che permette di navigare e usufruire di un insieme vastissimo di contenuti (multimediali e non) collegati tra loro attraverso legami (*link*) ed organizzati nei cosiddetti siti *web*, a loro volta strutturati in pagine *web*, le quali si presentano come composizioni di testo e/o grafica visualizzate sullo schermo di ogni *computer* dal *browser web*[8]; il servizio

---

contratto di servizio, fornisce accesso alla rete per il tramite di una linea di telecomunicazione dedicata cablata o *wireless* ovvero di una linea telefonica, rendendo possibile la sessione di navigazione attraverso l'utilizzo di un *web browser*.

[5] Le origini di Internet si trovano in ARPANET, una rete di *computer* costituita nel 1969 negli USA dal Dipartimento della Difesa. Solamente negli anni novanta Internet, fino a quel momento rete di *computer* mondiale di proprietà statale e destinata al mondo scientifico, iniziò a divenire una realtà pubblica. Con il "*High performance computing act"* del 1991, infatti, venne prevista la possibilità di un suo ampliamento per opera dell'iniziativa privata e con finalità di sfruttamento commerciale. Per un'analisi dell'evoluzione di Internet cfr. VANBERG M., *Competition and cooperation among Internet Service Providers*, Baden, 2009, p. 34 ss.

[6] Basti considerare che per l'anno 2014 la stima della popolazione mondiale è di 7.181.858.619 e quella degli utenti di Internet 2.802.478.934. La crescita percentuale degli internauti registrata dal 2000 al 2014 è pari 676,3%. Per statistiche dettagliate in riferimento ai diversi Paesi cfr. internetworldstats.com.

[7] Per un sintetico riferimento ai principali servizi Internet cfr. AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Matelica, 2006, p. 25 ss.; sotto il profilo civilistico cfr. RISTUCCIA R., TUFFARELLI L., *La natura giuridica di Internet e le responsabilità del provider*, in interlex.it, 19 Giugno 1997.

[8] Tutti i siti *web* sono identificati da un "indirizzo", ovvero una sequenza di caratteri univoca chiamata URL che ne permette la rintracciabilità. Tramite il sistema d'indirizzamento DNS (*Domain name system*) avviene la conversione da nome a indirizzo IP e viceversa. Non è previsto

di Posta Elettronica (*e-mail*), grazie al quale ogni utente abilitato può inviare e ricevere dei messaggi utilizzando un *computer* o altro dispositivo elettronico connesso in rete attraverso un proprio *account* di posta registrato presso un fornitore del servizio[9]; il servizio di *Newsgroup*, che, a mo' di bacheca, offre la possibilità di postare o leggere messaggi; il servizio di *File sharing*[10], ovvero condivisione di *file* sia attraverso una rete con architettura *client-server* (cliente-servente) sia attraverso sistemi *peer-to-peer* (pari a pari)[11]; il servizio di *Cloud computing*, che permette la memorizzazione, archiviazione o elaborazioni dati tramite la delocalizzazione di risorse e servizi informatici[12]; e molteplici ancora.

Già nella nota sentenza *Reno v American Civil Liberties Union* del 26 giugno 1997, che rappresenta il primo intervento della Corte Suprema Federale relativamente ai contenuti presenti in rete, Internet viene qualificato come «*a unique and wholly new medium of worldwide human communication […] Individuals can obtain access to the Internet from many different sources,*

---

un indice aggiornato in tempo reale dei contenuti del *web*, quindi, nel corso degli anni, sono nati ed hanno riscosso notevole successo i cosiddetti "motori di ricerca", ovvero siti *web* da cui è possibile ricercare contenuti in modo automatico sulla base di parole chiave inserite dall'utente.

[9] In riferimento al servizio di posta elettronica v. POMANTE G., *Internet e criminalità*, Torino, 1999, p. 90 ss.

[10] Per un'analisi delle problematiche relative alla responsabilità per violazione del *copyright* in caso di *file sharing*, in chiave comparata e con approfonditi richiami alla giurisprudenza americana di riferimento v. STROWEL A. (ed.), *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham-Northampton, 2009.

[11] Merita di essere ricordato l'ormai defunto Napster, chiuso per ripetuta violazione di *copyright*. Fondato nel 1999 dallo studente Shawn Fanning, fu il primo sistema *peer-to-peer* di massa a permettere agli utenti lo scambio di file audio compressi cd. Mp3, prodotti in casa da dischi originali. A differenza del sistema Napster, che utilizzava anche server centrali per mantenere la lista dei sistemi connessi e dei file condivisi, gli odierni sistemi P2P risultano totalmente decentrati, pertanto ogni singolo utente che condivide un file appare come vero e proprio *server*.

[12] In riferimento alla nozione di *cloud computing* cfr. FLICK C., AMBRIOLA V., *Dati nelle nuvole: aspetti giuridici del Cloud computing e applicazione alle amministrazioni pubbliche*, in federalismi.it, 20 marzo 2013; BIANCHI D., *Cloud computing e big data: vantaggi e rischi*, in personaedanno.it, 25 Marzo 2013.

generally hosts themselves or entities with a host affiliation […] Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services ("mail exploders" sometimes referred to as "listservs"), "newsgroups", "chat rooms", and the "World Wide Web". All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium-known to its users as ***"cyberspace"*** *– located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet*»[13].

Nell'ambito dell'*Internet service provision* si suole distinguere tra *"Internet core services"*, ovvero servizi utilizzati ed utilizzabili esclusivamente in relazione alla rete, e *"Internet periphery services"* che conoscono un impiego anche separato[14].

Tra le prime vengono annoverate, in modo particolare, tutte quelle attività offerte dagli ISPs entrate a far parte della quotidianità degli utenti, (servizi *e-mail*, *homepage services*, etc.), nonché gli elementi e le attività infrastrutturali che permettono l'accesso e la navigazione in rete, quale ad esempio l'assegnazione di indirizzi IP[15] (cd. servizi di *Internet Access*, di connessione locale tra *client* e ISP

[13] Decisione *Reno v American Civil Liberties Union*, 521 U.S. 844, consultabile alla pagina supreme.justia.com.

[14] Cfr. KNIEPS G., *Competition in Telecommunication and the Internet Services. A Dynamic Perspective*, in BARFIELD C. E., HEIDUK G., WELFENS P.J.J. (eds.), *Internet, Economic Growth and Globalization – Perspectives on the New Economy in Europe, Japan and the US*, Berlin et al., 2003, p. 217.

[15] L'IP *address* è una sequenza numerica che permette l'identificazione dei *computer* di rete. Mentre le macchine di proprietà del *provider* posseggono un IP statico, quelle degli utenti, nel momento della connessione, ne ricevono uno temporaneo dal ISP stesso che conserveranno solo sino al termine della sessione di navigazione. Cfr. AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, cit., p. 23 ss.

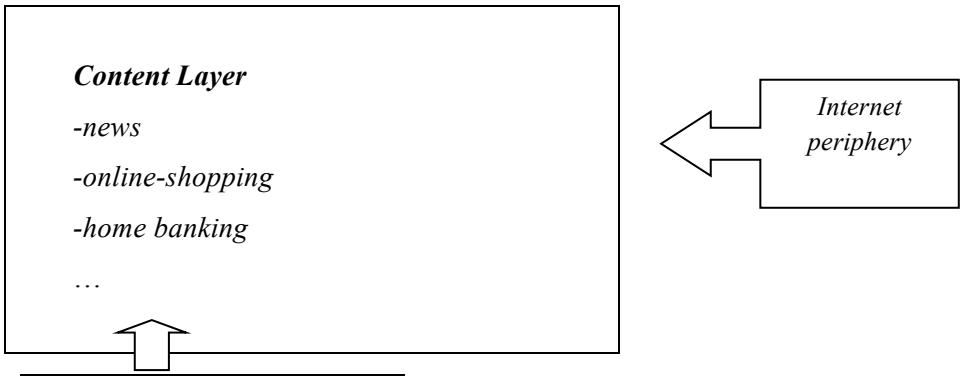
point of presence/POP; e servizi *Internet Backbone*, concernenti le comunicazioni a lunga distanza all'interno e tra ISPs).

Nella cd. *Internet periphery* vengono invece ricomprese le *Communications Infrastracture* sia locali che a lunga distanza ed i *Terminal Equipment* (PCs, *Notebooks*, *phones* etc.), dato che si prestano ad usi alternativi quali la trasmissione della tv via cavo o delle comunicazioni vocali. Rientra in questa categoria anche l'insieme dei contenuti e delle informazioni (*Content*) trasmessi in rete, che ovviamente possono circolare anche in sua assenza.

Proprio sulla base della distinzione tra *Internet core* e *periphery* si può delineare una prima definizione di ISP quale fornitore di servizi appartenenti all'*Internet core*. L'integrazione delle attività dell'ISP con servizi appartenenti all'alveo della *periphery* è possibile, ma non necessaria, ai fini della sua identificazione[16].

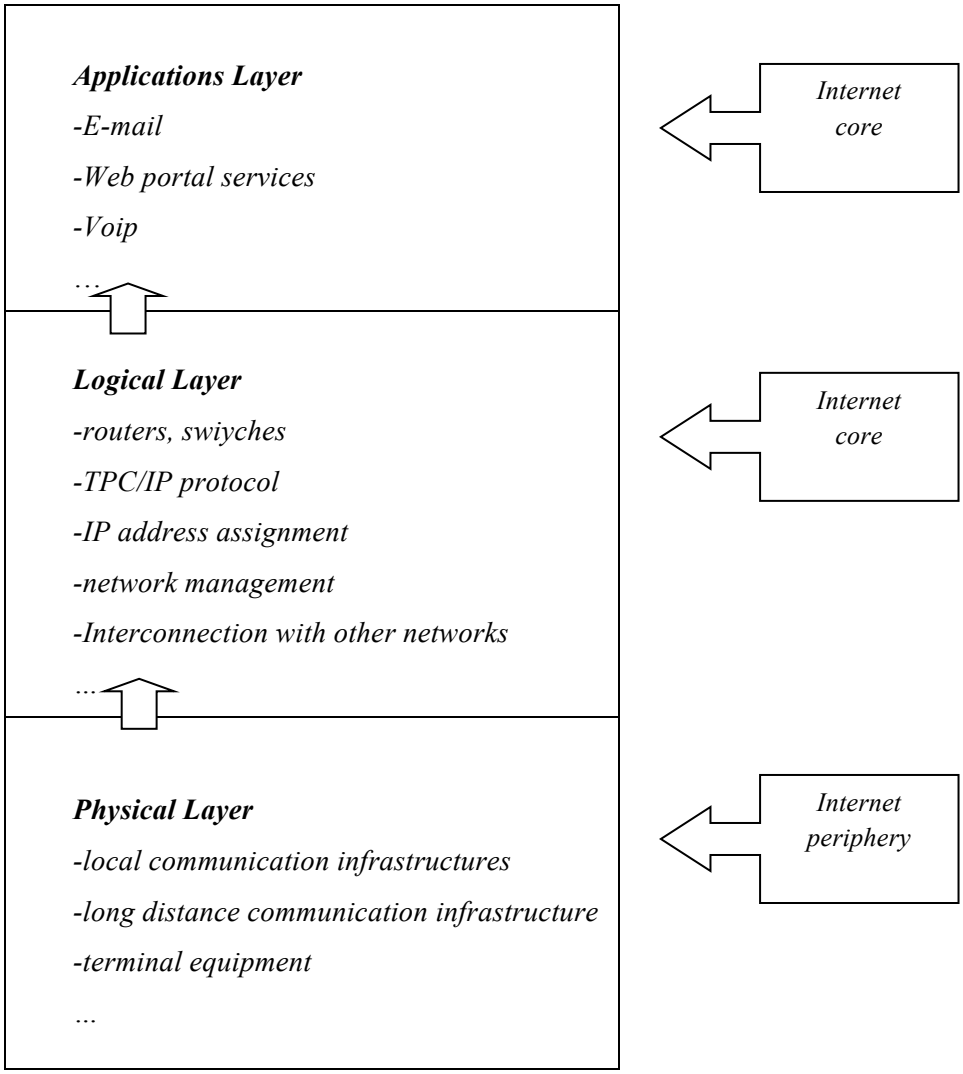
Da ultimo molto efficace risulta un'ulteriore distinzione all'interno dell'ampia categoria dell'*Internet service provision*, che sarà essenziale nel prosieguo della trattazione per formulare ipotesi di responsabilità penale degli ISPs.

Come suggerito da Vanberg, la fornitura di servizi Internet potrebbe essere rappresentata dalla seguente struttura a strati[17].



[16] Cfr. VANBERG M., *Competition and cooperation among Internet Service Providers*, cit., p. 27.

[17] *Ivi*, p. 32.



2. L'IMPATTO DI INTERNET SULLA CRIMINALITA'

Il *cyberspace*[18], inteso «*as any space of communication conducted with the aid of ICT networks*»[19], proprio per la sua caratteristica specifica di "non luogo",

[18] Il termine *cyberspace* venne utilizzato per la prima volta dallo scrittore William Gibson, che, nel suo romanzo *Neuromancer* del 1984, lo definì come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici. Una rappresentazione grafica di dati ricavati dai banchi di ogni *computer* del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano». E' interessante puntualizzare che il termine *cyber* deriva dal greco *κυβερνήτης (kybernētēs)* che significa *timoniere, nocchiere, pilota.* Nell'era della meccanica il termine venne mutuato dal

privo di confini e distanze[20], ha comportato la nascita di nuove problematiche giuridiche nel campo del diritto penale.

Internet costituisce uno spazio sociale-politico-economico che permette nuove forme di rappresentazione del sé, incide sulle identità, consente nuove forme di espressione e di esperienza artistica[21], ma allo stesso tempo, le sue enormi potenzialità diffusive ed i nuovi strumenti informatici hanno agevolato il proliferare di attività criminose inedite, nonché la realizzazione di fatti già costituenti reato ma attraverso modalità insolite, che richiedono molto spesso un difficoltoso ripensamento dei concetti tradizionali di azione, di evento, di *locus* e *tempus commissi delicti* [22].

---

mondo tecnico per indicare lo studio dei meccanismi con cui un sistema automatico può autoregolarsi. Fu Norbert Wiener ad introdurre il termine *cybernetics* per indicare lo studio dei meccanismi teleologici (rapporti di causa-effetto) nei sistemi automatici biologici e non, rendendo popolare il termine con la sua opera del 1948 *"Cybernetics, or Control and Communication in the Animal and Machine"*.

[19] Cfr. Associazione Internazionale di Diritto Penale, *Draft Resolution Verona 2012*, in aidpitalia.org.

[20] Cfr. INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, in LUPARIA L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, p. 18 ss.

[21] Cfr. RODOTÀ S., *Relazione introduttiva: Libertà, opportunità, democrazia, informazione*, Convegno *Internet e privacy – Quali regole?*, Roma, 8 Maggio 1998, in privacy.it.

[22] Cfr. PICOTTI L., voce *Reati informatici,* in *Enciclopedia Giuridica Treccani*, Roma, 2000, p. 30; ID., *Internet e responsabilità penali*, in PASCUZZI G. (a cura di), *Diritto e informatica*, Milano, 2002, p. 115 ss.; ID., *Profili penali delle comunicazioni illecite via Internet*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 2/1999, p. 283 ss. A fronte del superamento della dimensione spazio-temporale la rete impone ovviamente ed inevitabilmente un adattamento delle regole concernenti la giurisdizione e la competenza del giudice; sul punto cfr. SARGENTI B., *Giurisdizione e competenza territoriale in materia penale*, in *Giurisprudenza di merito*, n. 12/2012, p. 2642 ss.; CORRIAS LUCENTE. G., *In tema di competenza territoriale per la pubblicazione su Facebook, in violazione del diritto alla privacy*, in medialaws.eu, 4 Maggio 2015. Con riguardo all'orientamento espresso dalla Corte di Giustizia dell'Unione europea e dalla Corte europea dei diritti dell'uomo in materia di individuazione della giurisdizione applicabile alle controversie originate dall'utilizzo su vasta scala del *web* v. POLLICINO O., *Internet nella*

Si assiste inoltre ad una sorta di "democratizzazione" del crimine: la rete ha dato all'agente, anche di medie competenze informatiche, il potere di organizzare "attacchi" ed illeciti fino a qualche anno fa totalmente esclusi dalla portata del singolo. Più voci in dottrina hanno denunciato questa emergenza dell'*empowered single agent*[23].

La lotta alla criminalità nel cyberspazio è dunque alquanto problematica data la peculiarità della cd. *Internet Trinity*: una trinità fatta dalla tecnologia del mezzo, dalla distribuzione geografica dei suoi utenti, dalla natura dei suoi contenuti[24].

La rete delle reti, in quanto sistema sostanzialmente anarchico, risulta spesso un «*neighborhood without a police department*»[25], incontrollato e forse incontrollabile a fronte della possibilità di anonimato consentita agli utenti e della rapidità di trasmissione dei dati a distanze «talmente immense da rendere spesso vano ogni tentativo di delimitazione spazio-temporale degli illeciti commessi»[26].

L'impatto di Internet sulle possibilità di commettere illeciti e sulle fattispecie criminose risulta dunque molto eterogeneo.

In primo luogo la rete favorisce il proliferare di alcuni fenomeni illegali già esistenti attraverso la circolazione d'informazioni. *On line*, infatti, è possibile reperire facilmente spiegazioni per realizzare diverse attività illecite, quali a titolo esemplificativo il cd. *chipping*, cioè il *bypass* dei dispositivi di sicurezza negli

---

giurisprudenza delle Corti europee: prove di dialogo?, in forumcostituzionale.it, 31 Dicembre 2013.

[23] WALL D. S., *The Internet as a Conduit for Criminal Activity (Revised March 2010)*, in PATTINAVIA A. (ed.), *Information Technology and the Criminal Justice System*, Thousand Oaks, Califronia, 1995, p. 77 ss., *paper* consultabile anche in ssrn.com.

[24] Cfr. RODOTÀ S., *Relazione introduttiva: Libertà, opportunità, democrazia, informazione*, cit. V. inoltre PICA G., *Diritto penale delle tecnologie informatiche: computer's crimes e reati telematici, internet, banche dati e privacy*, Torino, 1999, p. 231 ss.

[25] Cfr. SUSSMAN V., *Policing Cyberspace*, in *U.S. News & World Report*, 23 Gennaio 1995, citato da WALL D. S., *The Internet as a Conduit for Criminal Activity (Revised March 2010)*, cit., in ssrn.com, p. 12.

[26] Cfr. PECORELLA C., *Diritto penale dell'informatica*, Padova, 2006, p. 33.

apparecchi telefonici o nei *decoders* televisivi per captarne il segnale, o il cd. *phreaking*, cioè l'uso di frequenze per manipolare un sistema telefonico.

In secondo luogo la rete, superando la tradizionale dimensione spazio temporale e creando un ambiente transnazionale, fornisce l'opportunità di estendere a livello globale alcuni illeciti e di realizzare condotte già penalmente sanzionate attraverso nuove modalità. Basti a tal riguardo considerare le fattispecie della diffusione di opere dell'ingegno coperte dal diritto d'autore[27] o ancora le ripercussioni registrate in materia di terrorismo[28].

Infine, come detto, nel *cyberspace* si sono sviluppate forme di criminalità fino a pochi anni fa del tutto sconosciute, quali gli attacchi cd. Dos, *(Denial of Service)*, che rendono inoperativi i servizi presi di mira[29], o ancora i cd. *phishing*

---

[27] In riferimento cfr. SEMINARA S., *La pirateria su Internet e il diritto penale*, in *Rivista trimestrale di diritto penale dell'economia*, 1997, p. 71 ss.; ID., *Tutela penale del diritto d'autore tra normativa vigente e prospettive di riforma*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 312 ss.

V. inoltre FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale,* Padova, 2010.

[28] Eloquente, a tal proposito, l'affermazione del Segretario Generale delle Nazioni Unite, Ban Ki-moon: «*The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner*». Cfr. UNODC, *The use of the Internet for terrorist purposes*, in unodc.org, New York, Settembre 2012.

[29] Cfr. DPCM 27 gennaio 2014, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, Glossario, p. 41: «Dos: Attacco volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi server».

Sempre più crescente negli ultimi anni il numero dei cd. DDoS, *Distributed Denial of Service*, che prendono di mira soprattutto istituzioni e servizi finanziari, sferrando contemporaneamente attacchi da più fonti così da rendere difficile rintracciare l'attaccante originario.

Noti alla cronaca gli attacchi del gruppo autoproclamatosi di "*hacktivisti* musulmani" chiamato Qassam Cyber Fighters (QCF) contro decine di banche con sede negli Stati Uniti che ha avuto per le stesse un costo approssimativo di $ 30.000 per ogni minuto di attacco. Cfr. voce *Operation Ababil* in wikipedia.org.

attacks, che, attraverso l'invio di messaggi di posta elettronica che imitano la grafica di siti bancari o postali, cercano di carpire i dati sensibili dell'utente[30].

Si delineano così anche esigenze di tutela di interessi e beni giuridici inediti: si pensi, ad esempio, alla riservatezza e alla sicurezza dei dati in rete[31].

---

[30] In riferimento al fenomeno in questione cfr. FLOR R., *Phishing, identity theft* e *identity abuse*: *le prospettive applicative del diritto penale vigente*, in *Rivista italiana di diritto e procedura penale*, 2007, p. 899 ss.

Data l'importanza assunta dai dispositivi mobili nella vita quotidiana degli utenti, sempre più diffuse risultano forme particolare di *phishing*, quali il *Vishing* (*phishing* tramite telefono) e il *Smishing* (*phishing* tramite messaggi di testo o SMS). Si registrano inoltre sempre più casi di *phishing attacks* che sfruttano il download di *app* solo apparentemente legittime.

Cfr. il Rapporto "Stato corrente della criminalità informatica nel 2013, uno sguardo attento al panorama delle minacce in costante evoluzione", in italy.emc.com.

[31] In relazione alla riservatezza dei dati informatici in dottrina si parla spesso di *"electronic panopticon"*, ovvero del potere offerto dalla rete di controllare in modo invisibile, nonché della problematica della cd. *"disappearance of disappearance"*, che favorisce e crea nuove opportunità per i furti di identità informatiche. Con riguardo ai concetti appena menzionati ed ai relativi risvolti social-culturali cfr. l'interessante articolo di HAGGERTY R. K., ERICSON V. R., *The surveillant assemblage*, in *British Journal of Sociology*, n. 51/2000, p. 605 ss., consultabile anche in englweb.umd.edu. V. inoltre CIPOLLA P., *Social network, furto di identità e reati contro il patrimonio*, in *Giurisprudenza di merito*, n. 12/2012, p. 2672 ss.; GALDIERI P., *Il trattamento illecito del dato nei social network*, in *Giurisprudenza di merito*, n. 12/2012, p. 2697 ss.; SICA S., CODIGLIONE G., *Social network sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, n. 12/2012, p. 2714 ss.

Sul concetto di "riservatezza informatica", anche per la bibliografia di riferimento, v. VENEZIANI P., *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, cit., p. 184 ss.

In riferimento alla problematica sottesa al bilanciamento tra esigenze di accertamento e ricerca della prova ed il rispetto del diritto di disporre delle proprie "aree informatiche" e di determinarne il "destino", quali nuove "manifestazioni" dei diritti inviolabili dei cittadini cfr. FLOR R., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, in penalecontemporaneo.it, 20 Settembre 2012; ID., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Rivista trimestrale di diritto penale dell'economia*, n. 3/2009, p. 695 ss., ID., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del*

Per comprendere le ripercussioni della diffusione globale di Internet sulla criminalità è interessante non solo la distinzione tra le fattispecie contraddistinte da inediti mezzi o modalità di aggressione a beni giuridici tradizionali e i fenomeni criminosi che, al contrario, ledono nuovi beni giuridici o interessi meritevoli di tutela, ma anche la valorizzazione dell'oggetto materiale, inteso in termini di oggetto passivo, su cui ricadono la condotta o l'evento[32].

Molto efficace, a tal riguardo, risulta *"The matrix of cybercrimes: level of opportunity by type of crime (with selected examples)"*[33], elaborata dal prof. Wall già nel 2003 e di seguito riportata.

Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention, in *Ciberspazio e diritto*, 2010, p. 359 ss.; ID., *Le recenti sentenze del Bundesverfassungsgericht e della Curtea Constituţională sul data retention*, in unicam.it, *Atti del Convegno- Ascoli Piceno*, 5-7 Marzo 2010.

[32] Sull'insufficienza, nell'ambito della categoria dei reati informatici, della bipartizione tra illeciti che prevedono nuovi mezzi e modalità d'aggressione a beni giuridici tradizionali e attività criminose offensive di beni giuridici del tutto nuovi, e sull'importanza dell'individuazione quantomeno di una terza categoria "intermedia" attraverso il parametro dell'oggetto materiale v. PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati* in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, cit., p. 21 ss.

[33] Cfr. WALL D. S., *Mapping out cybercrimes in a cyberspatial surveillant assemblage*, in WEBSTER F., BALL K. (eds.), *The intensification of surveillance: Crime, terrorism, and warfare in the information age*, London, 2003, p. 115 ss.

IMPACTS OF THE INTERNET
ON CRIMINAL OPPORTUNITIES AND BEHAVIOR

Crime Types ►	***Crime against machines/*** *Integrity-related*	***Crime using machines/*** *Computer-related*	***Crimes in the machine/*** *Content - related*	***Crimes in the machine/*** *Content - related*
Opportunities ▼	*/ Harmful /Trespass*	*Acquisition/ (Theft /Deception)*	*Obscenity*	*Violence*
Traditional crime using computers *More opportunities for traditional crime*	*Phreaking *Chipping	*Frauds	*Trading sexual materials	*Stalking *Harassment (personal)
Hybrid cybercrime *New opportunities for traditional crime* (e.g., organisation across boundaries)	* Cracking/ Hacking *Viruses *Hactivism	*Multiple large-scale frauds *Trade secret theft *ID Theft	*Online Sex trade *Camgirl sites	*General Hate speech *Organised paedophile rings (Child abuse)
True Cybercrime *New opportunities for new types of crime (Sui Generis)*	*Spams (list constuction and content) *Denial of Service *Information Warfare *Parasitic Computing	*Intellectual Property Piracy *Online Gambling *E-auction scams *Phishing	* Cyber-sex *Cyber-pimping	*Online Grooming * Organised Bomb talk /Drug talk *Targeted hate speech

La matrice presenta sull'asse Y le predette opportunità offerte da Internet allo sviluppo ed all'innovazione dei comportamenti lesivi degli interessi e

diritti altrui, mentre sull'asse delle X distingue gli illeciti a seconda che gli stessi si realizzino in danno all'integrità del pc/rete, vengano eseguiti tramite l'utilizzo del *computer* o la loro illeceità sia strettamente connessa ai contenuti trasmessi[34].

Analizzando i diversi settori individuati dall'intersezione delle righe e colonne della matrice risulta lampante come la fenomenologia criminosa nel *cyberspace* sia estremamente composita.

Questa varietà sta mettendo a dura prova la capacità delle legislazioni nazionali ed internazionali di identificare strategie adeguate per proteggere non solo le loro infrastrutture ma anche la sicurezza ed i diritti fondamentali dei cittadini[35], generando, come dimostra un recente sondaggio Eurobarometro sull'impatto della criminalità informatica[36], crescenti preoccupazioni nel popolo degli internauti.

---

[34] In riferimento ai più ricorrenti abusi di rilevanza penale nelle comunicazioni telematiche via Internet ed alle relative problematiche sia "di parte speciale" che "di parte generale" cfr. PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, in *Il Diritto dell'Informazione e dell'Informatica*, 1999, p. 283 ss.

V. inoltre SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer. Le nuove sfide di internet*, trad. it. a cura di Sforzi, in *Rivista trimestrale di diritto penale dell'economia*, 1997, p. 743 ss. – p. 1193 ss.

[35] Quanto mai attuali appaiono le considerazioni pronunciate a metà degli anni novanta da SEMINARA S., *La pirateria su Internet e il diritto penale*, cit., p. 112: «In realtà, l'inesistenza di soluzioni adeguate rappresenta null'altro che la conseguenza dell'incapacità degli ordinamenti giuridici nazionali, "chiusi" per loro natura, di fronteggiare la "società aperta creata da *Internet*, tetragona ad ogni tentativo di una sua comprensione giuridica in ambiti territorialmente definiti. Non risulta dunque eccessiva l'affermazione che la rete delle reti spinge verso un'unificazione internazionale dei diritti punitivi con una forza mai raggiunta in passato; è però evidentemente eccessiva l'opinione che i tempi siano maturi –o comunque prossimi– per un siffatto mutamento».

[36] Cfr. European Commission - IP/13/1130, pubblicato il 22 novembre 2013, in europa.eu.

Il sondaggio Eurobarometro, che ha interessato oltre 27.000 persone in tutti gli Stati membri, evidenzia innanzitutto come una percentuale elevatissima di internauti (circa il 76% degli intervistati) ritenga che il rischio di cadere vittima della criminalità cibernetica sia aumentato nell'ultimo anno. Interessante inoltre notare come, anche se il 70% degli internauti dell'UE si reputa in grado di usare Internet per effettuare operazioni bancarie o acquisti *on line*, solo il 50% circa scelga effettivamente di farlo. Questo notevole divario mostra l'impatto negativo della

3. LA "CRIMINALITÀ INFORMATICA" ED I "CYBERCRIMES"

Nonostante l'esplosione a livello internazionale del fenomeno, non si riviene, in alcuna disposizione giuridica sovranazionale una definizione specifica di *cybercrime*[37].

Il temine *cybercrime* da molto tempo viene utilizzato, soprattutto dai media, per raggruppare l'eterogenea gamma dei pericoli e degli illeciti che infettano il *cyberspace*.

Questo vuoto normativo ha fatto si che in dottrina ci si interroghi circa il rapporto intercorrente tra la nozione di "crimini cibernetici" e la nozione di "criminalità informatica", altrettanto priva di una specificazione giuridica internazionalmente riconosciuta, nonostante il suo utilizzo in numerose fonti interne e sovranazionali e la recente menzione tra i crimini che, ai sensi dell'art. 83, par. 1, del Trattato sul funzionamento dell'Unione (TFUE), rientrano nella competenza penale diretta dell'Unione europea[38].

Pur in assenza di una enunciazione specifica si può affermare con certezza che un crimine per poter rientrare nella categoria dei "reati informatici" deve

---

criminalità informatica sul mercato unico digitale, sull'economia digitale e sulle attività *on line*. Molti soggetti decidono di non sfruttare appieno tutte le possibilità offerte da Internet per timore della *cyber* criminalità: le due principali preoccupazioni riguardano l'abuso dei dati personali e la sicurezza dei pagamenti *on line* (rispettivamente secondo il 37% e il 35% degli intervistati).

[37] I *cybercrimes* sono i crimini che vengono realizzati nel *cyberspace*: per questo forse sarebbe più appropriato parlare di *cyberspace crimes*. Cfr. WALL D. S., *Cybercrime: The transformation of crime in the information age*, Cambridge, 2007, p. 10 ss.

[38] Per un'approfondita analisi dell'impatto della competenza penale riconosciuta all'Unione europea a seguito delle modifiche apportate al TFUE dal Trattato di Lisbona, adottato nel 2007 ed entrato in vigore nel 2009, che, oltre ad aver consolidato le basi del cd. diritto penale europeo, ha abolito la divisione in "pilastri" che in precedenza contraddistingueva la struttura istituzionale europea e riconosciuto il valore giuridicamente vincolante della Carta di Nizza, v. GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

presentare una connessione con l'informatica ovvero con il trattamento e/o trasmissione dell'informazione mediante procedure automatizzate[39].

La genericità di tale requisito, pur presentando il pregio di attagliarsi perfettamente alla fluente mutevolezza delle forme criminose nell'informatica, non permette all'espressione in esame di assumere un preciso significato tecnico-giuridico ai fini esegetici e sistematici.

Focalizzando l'attenzione sulla "tipicità" del fatto costitutivo dei reati informatici nel diritto positivo vigente, in dottrina si è evidenziato come essa includa sempre un "elemento tecnico" tra i requisiti indispensabili per produrre l'offesa ai beni giuridici tutelati[40].

Sulla base di tale acquisizione è possibile tracciare una distinzione tra *reati informatici in senso stretto* e *reati informatici in senso lato*, a seconda che la tecnologia informatica rappresenti il tratto distintivo o solamente eventuale del mezzo tipico, della modalità di realizzazione della condotta o dell'oggetto passivo offeso[41].

---

[39] Cfr. La definizione di *computer crimes* in OECD (ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT), *Computer-related Criminality: Analysis of legal Policy in the OECD Area* (a cura di Briat U., Sieber U.), PIIC n. 10, Parigi, 1986. In relazione alle prime definizioni di "criminalità informatica" cfr., con ampi richiami alla bibliografia nazionale ed internazionale di riferimento, PICOTTI L., *Studi di diritto penale dell'informatica*, Verona, 1992, p. 13 ss. V. inoltre ZICCARDI G., *International Encyclopaedia of Laws – Cyber Law. Italy*, The Netherlands, 2012, p. 303 ss.

[40] Cfr. PICOTTI L., *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Rivista trimestrale di diritto penale dell'economia*, n. 4/2011, p. 845 ss.

[41] Già agli inizi degli anni ottanta Sarzana suggeriva la distinzione tra un *diritto penale dell'informatica in senso ampio*, concernente quegli illeciti penali «comunque connessi all'uso del computer», ed un *diritto penale dell'informatica in senso stretto*, definibile come «quel gruppo di norme giuridiche con le quali lo Stato proibisce mediante la minaccia di una pena, determinati specifici comportamenti umani nel campo dell'informatica». Cfr. SARZANA C., *Note sul diritto penale dell'informatica*, in *La Giustizia Penale*, n. 1/1984, p. 21 ss.

Si ascrive alla prima tipologia, ad esempio, il reato di accesso abusivo ad un sistema informatico previsto dall'art. 615 ter c.p.[42].

Tra i reati informatici in senso lato vanno invece annoverati tutti quei reati che presentano una formulazione "elastica" passibile di applicazione nel caso di connessione del fatto con l'informatica. Basti a tal riguardo considerare la fattispecie di cui all'art. 171 *ter* lett. b) della Legge 22 aprile 1941, n. 633[43]: anche se il legislatore non ha espressamente previsto elementi di tipizzazione connessi alla tecnologia informatica, non vi sono dubbi circa la possibilità di commettere tale reato per via informatica, riproducendo ad esempio l'opera cartacea protetta in formato elettronico.

A seguito di questa prima distinzione chiarificatrice è necessario tornare al quesito di partenza, ovvero valutare se la relazione che intercorre tra l'ampia categoria dei reati informatici e quella dei reati cibernetici sia di inclusione stretta o si possano solamente individuare aree di intersezione tra le due.

---

[42] L'art. 615 *ter* c.p. sanzione fatto di chi «abusivamente si introduce in un sistema informatico telematico protetto da misure di sicurezza ovvero che si mantiene contro la volontà espressa tacita dici al diritto di escluderlo». Per un'analisi della fattispecie v. SALVADORI I., *L' accesso abusivo ad un sistema informatico telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti del diritto penale dell'informatica*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 125 ss.

[43] L'art. 171 *ter* lett. b) della legge n. 633/1941 sulla "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" (l.d.a.) punisce, con la reclusione da sei mesi a tre anni e con la multa da cinque a trenta milioni di lire, chiunque a fini di lucro e per uso non personale «abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati». Per uno sguardo sintetico e complessivo alla tutela penale dei diritti d'autore cfr. FLOR R., *Concezione dualistica dei diritti d'autore e tutela penale: quali prospettive per la rivalutazione della componente personalistico?*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, cit., p. 77 ss.

Il tratto distintivo dei reati cibernetici è da scorgere nella loro realizzazione e proiezione nel *cyberspace*.

In modo particolare si parla di *reati cibernetici in senso stretto (o proprio)* in relazione ai reati informatici in senso stretto contraddistinti dal riferimento alla rete nella formulazione normativa.

Ne è un esempio la messa a disposizione del pubblico di un'opera dell'ingegno protetta tramite immissione in un sistema di reti telematiche di cui all'art. 171 lett. a) *bis* della legge n. 633/1941[44].

Con l'espressione *reati cibernetici in senso lato (o impropri)* si indentificano, invece, i reati realizzabili solo *eventualmente* in rete, per la presenza di elementi costitutivi suscettibili di applicazione, in via interpretativa, alla specifica modalità o sede di commissione nel *cyberspace*.

A tal riguardo si considerino ad esempio i reati di ingiuria o di diffamazione di cui agli artt. 594, 595 c.p.[45], o ancora al reato di sostituzione di persona ex art. 494 c.p.[46].

In questa categoria potrebbero anche essere annoverati tutti quei reati tradizionali non informatici (né in senso ampio, né in senso stretto), quali ad

---

[44] In materia, molto interessante il caso "sky-calcio libero", affrontato dalla Corte di Cassazione nella sent. 10 ottobre 2006, n. 33945, con nota di FLOR R., *La rilevanza penale dell'immissione abusiva in un sistema di reti telematiche di un'opera dell'ingegno protetta: bene iudicat qui beni distinguit?*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 3/2007, p. 557 ss. In riferimento al reato di cui alla legge n. 633/1941, art. 171 lett. a) bis, ed ai problemi inerenti al sequestro preventivo di siti web cfr. FLOR R., *Sequestro preventivo di siti web e abusiva trasmissione telematica di programmi televisivi. Nota a G.i.p. Trib. Milano (ord.), 07.1.2013, Giud. Ghinetti*, in penalecontemporaneo.it, 15 Marzo 2013.

[45] Cfr. PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, cit., p. 283 ss.; PIOLETTI U., *Ingiuria, diffamazione e reti sociali*, in *Giurisprudenza di merito*, n. 12/2012, p. 2652 ss.; TABARELLI DE FATIS S., *Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione on-line*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, cit., p. 193 ss.

[46] In argomento cfr. la recente sentenza della Corte di Cassazione, 23 aprile 2014, n. 25774, con commento di SANSOBRINO F., *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in penalecontemporaneo.it, 30 Settembre 2014.

esempio quelli associativi, in cui l'utilizzo della rete diviene elemento contraddistintivo della fase preparatoria e quindi non influenza in alcun modo la tipicità della fattispecie. In questi casi il coinvolgimento di Internet ha delle ripercussioni importanti soprattutto dal punto di vista processuale, condizionando *in primis* la sfera investigativa e probatoria nel suo complesso.

Riprendendo la matrice di Wall (riportata nel precedente paragrafo) ritroveremo le stesse distinzioni: i *"traditional crimes using computer"* non sono altro che i reati cibernetici in cui l'utilizzo della reta ha risvolti non sul piano della tipicità ma su quello processuale; gli *"hybrid' cybercrimes"* coincidono con i reati cibernetici impropri, mentre i *"true cybercrimes"* sono i reati cibernetici in senso stretto.

Per valutare quali nuove fenomenologie criminose rientrino in quest'ultima categoria, a fronte del fatto che la maggior parte dei *"true cybercrimes"* non sono stati ancora disciplinati e tipizzati dal legislatore, il Prof. Wall suggerisce un semplice *"transformation test"*, consistente nel considerare che effetto avrebbe l'eliminazione dell'elemento della rete[47].

Schematizzando il ragionamento si potrebbe affermare che:

1. Se eliminando la rete il comportamento criminoso rimane inalterato, ci troviamo dinnanzi ad un *traditional crime using computer*;
2. Se eliminando la rete il comportamento criminoso continua ad esistere, ma non su così ampia scala e con la stessa diffusione, si tratta di un *hybrid cybercrime*;
3. Se eliminando la rete anche il comportamento criminoso scompare, allora è un *true cybercrime*.

Ma, se a causa della mancata traduzione di questi nuovi fenomeni in fattispecie legislative *ad hoc*, la maggior parte dei *true cybercrimes* costituiscono

[47] Cfr. WALL D. S., *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace*, in *Police Practice & Research: An International Journal*, 8(2), p. 183 ss., consultabile on line in ssm.com.

"new wines in no bottles!"[48], essenziale risulta stabilire quali rientrino nella più ampia categoria della cd. criminalità informatica, vista la competenza attribuita all'Unione europea di dettare «norme minime relative alla definizione dei reati e delle sanzioni»[49] anche in questa particolare sfera di criminalità.

Dato il carattere transnazionale del *cyberspace* sembra più che mai opportuno, onde garantire una risposta efficace contro i nuovi fenomeni criminosi, che la sfera della criminalità informatica accolga in primo luogo i *cybercrimes* in senso stretto. E' proprio in assenza delle *"bottles"* che il potere riconosciuto all'Unione europea acquista il suo pieno significato[50].

L'effetto che il test *"Take away the Internet"* ha mostrato in relazione ai reati cibernetici in senso lato, invece, non può che far propendere per una loro esclusione dal settore di competenza delineato dalla nozione di "criminalità informatica", potendo quegli stessi fenomeni eventualmente rientrare, in caso di particolar gravità, dimensione transnazionale e necessità di risposte su basi comuni, in una delle altre sfere di cui all'art. 83, par. 1, TFUE (ad es. si pensi al fenomeno del cyber-terrorismo); ovvero, nell'ambito della competenza penale cd. "accessoria" prevista dall'art. 83, par. 2, TFUE, qualora il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si riveli indispensabile per garantire l'attuazione efficace di una politica dell'Unione in un settore che è stato oggetto di misure di armonizzazione, (ad es. si pensi alla materia della tutela della proprietà intellettuale).

4. IMPULSI SOVRANAZIONALI NELLA LOTTA AI *CYBERCRIMES*

Come più volte ricordato, per contrastare le moderne forme di criminalità connesse alla rete, travalicanti i limiti nazionali, quantomeno in potenza, la

[48] *Ivi*

[49] Art. 83, par. 1, del Trattato sul funzionamento dell'Unione (TFUE).

[50] Cfr. PICOTTI L., *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, cit., p. 861 ss.

prospettiva di un'azione coordinata a livello sovranazionale o addirittura globale sembra senz'altro preferibile[51].

Nell'ambito delle iniziative contro i *cybercrimes* promosse dagli organismi con una competenza che interessa l'area territoriale più ampia, doveroso risulta innanzitutto il richiamo all'impegno del gruppo dei Paesi industriali (cd. G8), che, durante l'incontro svoltosi a Lione nel 1995, ha istituito un comitato di esperti chiamato ad approfondire la materia del *cybercrime* a livello internazionale e successivamente, nel 1997, ha creato un sottocomitato *ad hoc* competente per le questioni connesse alle indagini ed al contrasto dei crimini ad "alta tecnologia"[52].

Fondamentale per una cooperazione tendenzialmente globale anche l'opera delle Nazioni Unite, ed in modo particolare del suo Ufficio per il controllo della droga e la prevenzione del crimine (UNODC), fondato nel 1997[53], nonché dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE/OECD)[54] e del suo Comitato per Informazione, Informatica e Comunicazione (ICCP).

---

[51] In riferimento al problema dell'armonizzazione normativa fra i diversi sistemi penale nazionali e agli importanti interrogativi che l'attuale scenario multilivello pone alla scienza penale cfr. MILITELLO V., *L'identità della scienza giuridica penale nell'ordinamento multilivello*, in *Rivista italiana di diritto e procedura penale*, n. 1/2014, p. 106 ss.

[52] In argomento cfr. MILITELLO V., *Iniziative sovranazionali di lotta alla criminalità organizzata ed al riciclaggio nell'ambito delle nuove tecnologie*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, cit., p. 95 ss.

[53] Nel 2012 l'Agenzia delle Nazioni Unite contro la droga e la criminalità ha pubblicato un rapporto che si pone l'obiettivo di aiutare a comprendere le modalità con cui i terroristi usano Internet e di accrescere la cooperazione internazionale per assicurare la messa in atto di risposte efficaci di fronte a questa sfida. V. UNODC, *The use of the Internet for terrorist purposes*, in unodc.org.

[54] L'OCSE, come ben noto, ha contribuito in modo essenziale al dibattito internazionale sul tema *privacy* fin dal 1980, quando furono pubblicate le *"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"*. Per la loro consultazione e anche per comprendere il funzionamento del Comitato ICCP v. oecd.org. V. inoltre BRIAT M., SIEBER U., (eds.) *Computer Related Criminality: Analysis of Legal Policy in the OECD- Area*, Parigi, 1986.

Dal punto di vista legislativo una prima tappa fondamentale è rappresentata dalla Raccomandazione sulla Criminalità Informatica n. R. (89) 9, adottata il 18 gennaio 1989 dal Consiglio d'Europa, nella quale le diverse forme di criminalità informatica vengono ripartite in due gruppi - cd. "lista minima" e "lista facoltativa"- a seconda della necessità di provvedere alla loro repressione con strumenti penali oppure con sanzioni diverse scelte autonomamente dai singoli Stati[55].

Anche la successiva Raccomandazione n. (95) 13 approvata dal Consiglio d'Europa l'11 settembre 1995, pur concentrandosi sui profili di procedura penale collegati alle tecnologie dell'informazione, fornisce indicazioni essenziali in materia di *cybercrimes*, suggerendo tra l'alto agli Stati membri di predisporre specifici obblighi per gli ISPs di fornire le misure tecniche necessarie per permettere l'intercettazione delle telecomunicazioni e l'identificazione gli utenti da parte delle competenti autorità investigative.

Tra i progetti "globali" più importanti portati a termine, deve essere sicuramente menzionata la Convenzione *Cyber-crime* del Consiglio d'Europa, firmata a Budapest il 23 novembre 2001 ed entrata in vigore nel luglio 2004[56]. Ad oggi essa rappresenta l'unico trattato internazionale vincolante esistente in materia di criminalità informatica e traccia le linee guida per tutti gli Stati che vogliano sviluppare una legislazione nazionale completa in tale settore[57].

---

[55] Nel primo gruppo rientrano: frode informatica, falso informatico, accesso non autorizzato a sistemi informatici, sabotaggio informatico, danneggiamento di dati e di programmi informatici, intercettazione di dati non autorizzata, riproduzione non autorizzata di programmi protetti; mentre nel secondo: alterazione non autorizzata di dati o programmi (ma senza loro danneggiamento), divulgazione di informazioni legate al segreto industriale o commerciale (una tipologia riconducibile alla fattispecie dello spionaggio informatico), l'utilizzazione non autorizzata di un elaboratore elettronico o di un programma informatico protetto.

[56] Per la consultazione del testo integrale della Convenzione e del Protocollo addizionale relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici, nonché per l'analisi dello stato delle firme e ratifiche v. coe.int.

[57] Interessante ricordare che la Convezione *Cyber-crime* è stata aperta alla firma anche di Paesi "terzi" quali Stati Uniti, Canada, Australia e Giappone. Essa è articolata in 4 capitoli: definizioni, misure da adottare a livello nazionale in tema di diritto sostanziale e processuale,

A livello "regionale" europeo, in seguito al superamento della struttura a pilastri operato dal Trattato di Lisbona, la cooperazione giudiziaria e di polizia in materia penale, prima essenzialmente affidata al metodo intergovernativo, risulta attualmente pienamente integrata nel sistema dell'Unione. Ad essa sono dedicati gli articoli 82-89 del Trattato sul funzionamento dell'Unione europea[58].

In particolare, l'articolo 83 TFUE, come anzidetto, prevede che il Parlamento europeo e il Consiglio possano stabilire, secondo la procedura legislativa ordinaria, norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale[59], tra le quali è espressamente menzionata la criminalità informatica[60].

---

cooperazione internazionale, clausole finali. Tra le fattispecie in relazione alle quali gli Stati sottoscriventi sono chiamati «ad adottare le misure legislative ed di altra natura» necessarie affinché costituiscano «reato in base alla propria legge nazionale» vengono ricompresi reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici quali l'accesso illegale ad un sistema informatico (art. 2), l'intercettazione abusiva (art. 3), l'attentato all'integrità dei dati (art. 4), l'attentato all'integrità di in un sistema (art. 5), l'abuso di apparecchiature (art. 6); reati informatici quali la falsificazione e la frode informatica (artt. 7, 8); reati relativi ai contenuti quali quelli relativi alla pornografia infantile (art. 9); ed infine reati contro la proprietà intellettuale e diritti collegati (art. 10).

In argomento cfr. MORALES G. O., *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul Cybercrime*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, cit., p. 123 ss.

[58] Cfr. in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*: GRASSO G., *La «competenza penale» dell'Unione Europea nel quadro del Trattato di Lisbona*, p. 683 ss.; PICOTTI L., *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, p. 207 ss.; MAUGERI A. M., *Il principio di proporzione nelle scelte punitive del legislatore europeo. L'alternativa delle sanzioni amministrative comunitarie*, p. 68 ss. In riferimento alle tensioni sussistenti tra riconoscimento di una competenza dell'Unione in materia penale e principio di legalità v. SICURELLA R., *«Prove tecniche» per una metodologia dell'esercizio delle nuove competenze concorrenti dell'Unione Europea in materia penale*, *Ivi*, p. 3 ss.; BERNARDI A., *All'indomani di Lisbona: note sul principio europeo di legalità penale*, in *Quaderni Costituzionali*, n. 1/2009, p. 37 ss.

[59] L'armonizzazione sanzionatoria a livello europeo, prima delle innovazioni apportate dal Trattato di Lisbona, è avvenuta in modo spontaneo con riferimento agli "illeciti a carattere

In questo quadro, e secondo le priorità stabilite Consiglio europeo nel Programma di Stoccolma per lo spazio di libertà sicurezza e giustizia per il periodo 2010-2014[61], il 3 settembre 2013 è entrata in vigore la Direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione 2013/40[62], che sostituisce la decisione quadro 2005/222/GAI e prevede obblighi di incriminazione in riferimento all'accesso abusivo ad un sistema di informazione[63], all'interferenza illecita relativamente ai sistemi ed ai

---

meramente interno"; attraverso il metodo intergovernativo, grazie anche all'impulso del Consiglio d'Europa, per gli "illeciti di rilievo transnazionale; in modo coatto legislativo o giurisprudenziale per gli "illeciti comunitari" (v. in modo particolare le famose sentenza dalla Corte di Giustizia del 13 settembre 2005 e del 23 ottobre 2007). Cfr. in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo*, cit.,: BERNARDI A., *L'armonizzazione delle sanzioni in Europa: linee ricostruttive*, p. 381 ss.; SICURELLA R., *"Eppur si muove!": alla ricerca di un nuovo equilibrio nella dialettica tra legislatore comunitario e legislatore nazionale per la tutela degli interessi dell'Unione europea*, p. 263 ss.; PICOTTI L., *Superamento della c.d. tecnica del "doppio testo" e tutela penale degli interessi europei*, p. 323 ss. V. inoltre SIEBER U., *The future of European Criminal Law: a new approach to the aims and models of the European Criminal Law system, Ivi*, p. 689 ss.

[60] Le sfere di criminalità menzionate nell'art. 83 TFUE sono le seguenti: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata.

[61] Cfr. Programma di Stoccolma – Un'Europa aperta e sicura al servizio e a tutela dei cittadini [Gazzetta ufficiale C 115 del 4.5.2010], adottato dal Consiglio europe nel dicembre 2009 e consultabile nella sezione Sintesi della legislazione dell'UE > Diritti umani > Diritti fondamentali nell'ambito dell'Unione europea in europa.eu. Esso delinea gli orientamenti strategici della programmazione legislativa ed operativa nello spazio di libertà, sicurezza e giustizia, in conformità all'art. 68 TFUE. I nuovi orientamenti per periodo 2015-2020 sono espressi nelle Conclusioni del Consiglio europeo del 26-27 giugno 2014, in consilium.europa.eu, v. nota 67.

[62] Cfr. CONIGLIARO S. C., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della nuova direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in penalecontemporaneo.it, 30 Ottobre 2013. Per il testo integrale della direttive v. eur-lex.europa.eu.

[63] Ai sensi dell'art. 3 della direttiva 2013/40/UE del 12 agosto 2013, l'accesso senza diritto ad un sistema di informazione o a una parte dello stesso andrebbe punito solo quando effettuato in violazione di una misura di sicurezza, condizione prima non richiesta dalla decisione quadro né dalla Convenzione di Budapest.

dati informatici, all'intercettazione illecita, alla fabbricazione di *malware* ed alla diffusione di *password*, ma anche obblighi per gli Stati membri di adottare le misure necessarie ad assicurare che le persone giuridiche possano essere ritenute responsabili di tali reati se commessi a loro vantaggio da un soggetto che, in seno all'ente, detiene una "posizione dominante", ovvero da parte di una persona "subordinata", qualora la mancata sorveglianza o il mancato controllo da parte del superiore abbia permesso la commissione del reato stesso.

Anche la direttiva 2011/93, concernente la lotta contro l'abuso e lo sfruttamento sessuale dei minori[64], tratta aspetti di diritto penale sostanziale e processuale significativi nell'ambito della prevenzione e repressione dei crimini informatici. Basti a tal proposito ricordare l'obbligo di incriminazione delle nuove forme di abuso e sfruttamento sessuale favorite dall'uso di strumenti informatici, quale l'adescamento dei minori *on-line* ai fini di abuso[65], o ancora l'obbligo per gli Stati di adottare le misure necessarie per assicurare la tempestiva rimozione

[64] La direttiva 2011/93/UE del 13 dicembre 2011, la cui numerazione è il risultato di una rettifica, in quanto l'originaria era 2011/92/UE, sostituisce la decisione quadro 2004/68/GAI del Consiglio relativa alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile, adottata il 22 dicembre 2003, a cui l'Italia aveva dato attuazione con la legge 6 febbraio 2006, n. 38. Nelle intenzioni del legislatore europeo (v. *Considerando 7*), poiché spesso le vittime di reati di abuso o sfruttamento sessuale sono anche vittime della tratta di esseri umani, la direttiva in esame fungerebbe da completamento alla direttiva 2011/36/UE sulla prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime, sostitutiva della decisione quadro del Consiglio 2002/629/GAI. Cfr. VERRI A., *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE*, in penalecontemporaneo.it, 28 Marzo 2012.

In riferimento alla direttiva 2011/36/UE del 5 aprile 2011, a cui l'Italia ha dato attuazione con d.lgs. 4 marzo 2014, n. 24, cfr. SICURELLA R., *Prosegue l'azione dell'Unione europea nella lotta alla tratta di esseri umani*, in penalecontemporaneo.it, 25 Luglio 2011; MONTARI M., *L'attuazione italiana della direttiva 2011/36/UE: una nuova mini-riforma dei delitti di riduzione in schiavitù e di tratta di persone*, in penalecontemporaneo.it, 20 Marzo 2014.

[65] V. art. 6 direttiva 2011/93/UE. In riferimento al cd. fenomeno del "*grooming*" cfr. VIZZARDI M., *Sull'"adescamento" di minore tramite social network e il tentativo di atti sessuali con minorenne, Nota a Tribunale di Milano, Uff. Gup, 25 ottobre 2011, Giud. Domanico*, in penalecontemporaneo.it, 9 Febbraio 2012.

delle pagine *web* contenenti immagini pedopornografiche che abbiano *host* nel proprio territorio, con la possibilità di richiedere la stessa misura anche al di fuori dei limiti territoriali[66]. La direttiva 2011/93 prevede inoltre, in materie di responsabilità delle persone giuridiche, norme analoghe a quelle della direttiva 2013/40 citate poc'anzi.

Nell'ambito delle risposte dell'Unione europea alla criminalità informatica, la finalità di prevenire e perseguire efficacemente gli attacchi su vasta scala contro i sistemi informatici, è stata attuata anche mediante l'istituzione del Centro europeo per la lotta alla criminalità informatica (EC3), operativo dal gennaio 2013.

L'attività dell'EC3 è principalmente volta a favorire la cooperazione tra le autorità di contrasto degli Stati membri e di paesi terzi e la loro assistenza[67]. Si tratta di una scelta totalmente in linea con gli obbiettivi di promozione della cooperazione transfrontaliera tra sistemi giudiziari e forze di polizia degli Stati membri dell'UE, richiamati anche nella direttiva relativa agli attacchi contro i sistemi di informazione 2013/40[68].

Da ultimo, nelle Conclusioni adottate dal recente Consiglio europeo dei Capi di Stato e di Governo riunitosi a Ypres il 26 e 27 giugno 2014[69], la cyber-sicurezza è menzionata tra le priorità principali dell'Unione europea.

---

[66] V. art. 25 direttiva 2011/93/UE.

[67] Cfr. European Commission - IP/13/13, 09/01/2013, in europa.eu.

[68] V. *Considerando 28* della direttiva 2013/40/UE: «Una migliore cooperazione tra competenti organismi preposti all'applicazione della legge e autorità giudiziarie in tutta l'Unione è essenziale ai fini di una lotta efficace contro la criminalità informatica. In tale contesto, si dovrebbe incoraggiare l'intensificazione degli sforzi, intesi a fornire una formazione adeguata alle pertinenti autorità, al fine di aumentare la comprensione della criminalità informatica e del suo impatto e promuovere la cooperazione e lo scambio di migliori pratiche, ad esempio attraverso le competenti agenzie e organismi specializzati dell'Unione. Tale formazione dovrebbe mirare, tra l'altro, ad aumentare il grado di conoscenza dei diversi ordinamenti giuridici nazionali, delle possibili sfide giuridiche e tecniche da affrontare nelle indagini penali e della ripartizione delle competenze tra le competenti autorità nazionali».

[69] Le Conclusioni del Consiglio europeo dei Capi di Stato e di Governo delineano i nuovi orientamenti strategici per lo spazio europeo di libertà, sicurezza e giustizia e guideranno l'azione

Viene quindi confermata la tendenza espressa, in modo maggiormente dettagliato, nel Piano di sicurezza informatica dell'UE *"Uno spazio informatico aperto e sicuro"* per tutelare la rete aperta, la libertà e le opportunità da essa offerta, elaborato dalla Commissione in collaborazione con l'Alta rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza, pubblicato il 7 febbraio 2013 contestualmente alla proposta di direttiva della Commissione in materia di sicurezza delle reti e dell'informazione[70].

Gli obbiettivi in cui è articolata tale strategia, con l'intento di promuovere i valori europei di libertà e democrazia e garantire che l'economia digitale possa svilupparsi in modo sicuro, sono essenzialmente questi:

1. Conseguire la resilienza informatica;
2. Ridurre drasticamente la criminalità informatica;
3. Sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune;
4. Sviluppare le risorse industriali e tecnologiche per la sicurezza informatica;
5. Istituire una coerente politica internazionale del ciberspazio per l'Unione europea e sostenere i valori fondamentali dell'UE.

5. LA NORMATIVA PENALE ITALIANA IN MATERIA DI CRIMINALITÀ INFORMATICA

La stratificazione normativa che si è progressivamente sviluppata nel nostro ordinamento per contrastare fenomeni criminosi legati all'utilizzo delle nuove

---

dell'Unione europea in quest'ambito durante il quinquennio 2015-2020. Esse subentrano al Programma di Stoccolma. La programmazione pluriennale nel campo della giustizia e degli affari interni era stata avviata sin dal programma di Tampere (1999-2004) e proseguita con il programma dell'Aia (2005-2009). Cfr. COTTU E., *Il Consiglio europeo adotta i nuovi orientamenti strategici per lo spazio di libertà, sicurezza e giustizia per il quinquennio 2015-2020*, in penalecontemporaneo.it, 22 Luglio 2014.

[70] Cfr. European Commission - IP/13/94, 07/02/2013, in europa.eu.

tecnologie e per uniformarsi alle indicazioni sovranazionali appare molto disorganica[71].

Non si rinviene un *corpus* unitario di disposizioni e la congerie normativa relativa ai "crimini informatici", nelle loro diverse accezioni, è disseminata in diverse parti del codice penale ed in differenti leggi speciali, quali il Codice *privacy* (T.U. n. 196/2003 in materia di protezione dei dati personali) e la Legge sul diritto d'autore (legge n. 633/1941)[72].

Il primo passo verso la creazione di un diritto penale dell'informatica risale alla fine degli anni settanta, quando, con legge 18 maggio 1978, n. 191, venne reintrodotto nel codice penale l'art. 420, in cui si incluse espressamente anche la tutela della integrità e funzionalità degli impianti di ricerca o di elaborazione dei dati[73].

In quegli stessi anni si registrano anche i primi dibattiti in merito alle truffe realizzate attraverso gli elaboratori, in assenza di controllo umano dell'*output*,

[71] Per uno sguardo alle tappe fondamentali della produzione, in Italia, delle fattispecie riconducibili alla categoria dei reati informatici cfr. PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, cit., p. 26 ss. Secondo l'autore i modelli ispiratori delle diverse disposizioni nazionali in materia di criminalità informatica sarebbero essenzialmente quattro ovvero: 1. le raccomandazioni del Consiglio d'Europa; 2. le esperienze legislative di altri ordinamenti o singoli casi giurisprudenziali; 3. le norme del codice penale sulla riservatezza domiciliare e nelle comunicazioni personali introdotte con legge 8 aprile 1974, n. 98; 4. i precetti extra-penali rilevanti in ambito informatico e bisognosi di tutela penale in attuazione a direttive comunitarie.

[72] Per un'analisi complessiva dei retai informatici previsti sia nel codice penale che nella legislazione penale complementare cfr. PICOTTI L., voce *Reati informatici*, cit., p. 1 ss.; PICA G., voce *Reati informatici e telematici*, in *Digesto* delle *Discipline Penalistiche*, 2000, p. 521 ss.

[73] Alla base dell'intervento la necessità di far fronte ai numerosi casi di danneggiamento di sistemi registratesi negli anni settanta. La norma venne applicata dalla giurisprudenza non solo qualora l'oggetto passivo fosse l'*hardware*, ma anche quando fossero compromessi dati o programmi in grado di rendere inservibile il sistema di elaborazione. Cfr. AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, cit., p. 55 ss.

difficilmente sanzionabili ai sensi dell'art. 640 c.p. per la mancanza di artifici e raggiri volti ad ingannare una persona fisica[74].

A fronte delle difficoltà incontrate dalla giurisprudenza nell'applicazione delle disposizioni esistenti alle nuove realtà della delinquenza informatica ed alle numerose sollecitazioni sovranazionali, il legislatore degli anni novanta si è adoperato, su diversi fronti, in progetti di modiche e innovazioni dell'impianto legislativo penale.

Con decreto legislativo n. 518/1992 è stata innanzitutto data attuazione alla direttiva CEE n. 250/1991, inserendo nel *corpus* della legge sul diritto d'autore sanzioni penali a tutela del *software*[75].

---

[74] Cfr. SARZANA C., *Note sul diritto penale dell'informatica*, cit. p. 28 ss.

[75] Il d.lgs. n. 518/92 ha equiparato il "programma per elaboratore" alle opere dell'ingegno apprestandogli quindi tutela attraverso la disciplina del diritto d'autore. L'articolo 10 del decreto, in particolare, prevedeva: «Dopo l'art. 171 della legge 22 aprile 1941, n. 633, è inserito: Art. 171 *bis*. - 1. Chiunque abusivamente duplica a fini di lucro, programmi per elaboratore, o, ai medesimi fini e sapendo o avendo motivo di sapere che si tratta di copie non autorizzate, importa, distribuisce, vende, detiene a scopo commerciale, o concede in locazione i medesimi programmi, è soggetto alla pena della reclusione da tre mesi a tre anni e della multa da L. 500.000 a L. 6.000.000. Si applica la stessa pena se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione di un programma per elaboratore. La pena non è inferiore nel minimo a sei mesi di reclusione e la multa a L. 1.000.000 se il fatto è di rilevante gravità ovvero se il programma oggetto dell'abusiva duplicazione, importazione, distribuzione, vendita, detenzione a scopo commerciale o locazione sia stato precedentemente distribuito, venduto o concesso in locazione su supporti contrassegnati dalla Società italiana degli autori ed editori ai sensi della presente legge e del relativo regolamento di esecuzione approvato con regio decreto 18 maggio 1942, n. 1369. 2. La condanna per i reati previsti al comma 1 comporta la pubblicazione della sentenza in uno o più quotidiani e in uno o più periodici specializzati». Cfr. PICA G., voce *Reati informatici e telematici*, cit., p. 548 ss.

In riferimento alle successive modifiche apportate alla legge sul diritto d'autore v. FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet*, cit., p. 159 ss. Con riguardo alla disciplina specifica dell'autotutela tecnologica dei diritti d'autore, anche in prospettiva comparatistica ed euopea, v. FLOR R., *Misure tecnologiche di protezione ed anticipazione della punibilità nel sistema di tutela penale dei diritti d'autore e connessi in Europa*,

La legge 23 dicembre 1993, n. 547[76], si è proposta invece come organica riforma del codice penale e, anche sulla base della Raccomandazione del Consiglio d'Europa n. R (89) 9, ha introdotto i reati di cui agli artt. 615 *ter* (Accesso abusivo ad un sistema informatico o telematico), 615 *quater* (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici), 615 *quinquies* (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico), 617 *quater* (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche), 617 *quinquies* (Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche), 617 *sexies* (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche), 635 *bis* (Danneggiamento di informazioni, dati e programmi informatici) e 640 *ter* (Frode informatica).

La novella in esame ha inoltre integrato l'art. 392 c.p. (includendo i "sistemi informatici" tra le "cose" su cui può essere esercitata la violenza), l'art. 616 c.p. (estendendo la nozione di "corrispondenza" anche a quella "informatica o telematica"), e l'art. 621 c.p. (annoverando tra i "documenti" anche "qualunque supporto informatico contenete dati, informazioni o programmi").

Il legislatore del 1993 ha previsto all'art. 491 *bis* c.p., un "rinvio" alle fattispecie penali di falso già esistenti per i casi di falsificazioni di documenti informatici ed ha infine esplicitato l'applicazione dell'art. 420 c.p. anche al danneggiamento dei "dati, informazioni o programmi" pertinenti o contenuti nei sistemi informatici o telematici di pubblica utilità.

---

in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, cit., p. 233 ss.

[76] In riferimento alla legge n. 547/1993 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica") e per un analisi completa dei reati informatici introdotti nel nostro ordinamento cfr. PICOTTI L., voce *Reati informatici*, cit., p. 5 ss. V. inoltre PICA G., voce *Reati informatici e telematici*, cit., p. 521 ss.

Proseguendo in questo rapido *excursus* cronologico, nel 1996, con legge n. 675, sono state introdotte, in attuazione della direttiva CE 95/46, specifiche fattispecie di illeciti relativi al trattamento ed alla diffusione dei dati personali[77].

Il problema relativo al rapporto tra pedopornografia di ed informatica ha rappresentato invece il cuore dell'iniziativa legislativa culminata nella legge n. 269/1998, che, in attuazione della Convenzione sui diritti del fanciullo di New York del 1989 ed a quanto sancito dalla dichiarazione finale della Conferenza mondiale di Stoccolma del 16 agosto 1996, ha introdotto nuove ipotesi di reato, tra le quali la diffusione di materiale pedopornografico anche per via telematica di cui all'art. 600 *ter* c.p.[78], successivamente modificati con legge 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[79].

Venendo quindi alle riforme più importanti in materia di criminalità informatica del ventunesimo secolo, con legge 18 marzo 2008, n. 48[80] l'Italia ha

---

[77] La legge n. 675/1996 è stata abrogata ai sensi dell'art. 183, comma 1, lettera a), del Codice in materia dei dati personali, che ha a sua volta dato attuazione alla direttiva CE 2002/58. Per un rapido sguardo alla situazione attuale v. TIBERI G., *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, p. 515 ss.

[78] In argomento cfr. PICOTTI L., *Pornografia minorile: evoluzione della disciplina penale e beni giuridici tutelati*, in FIORAVANTI L. (a cura di), *La tutela penale della persona: nuove frontiere, difficili equilibr*i, Milano, 2001, p. 295 ss.

[79] In tema v. PICOTTI L., *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet (l. 6 febbraio 2006, n. 38) (parte prima),* in *Studium iuris*, 2007, p. 1059 ss.; PICOTTI L, *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. 1196 ss.

[80] Per un commento alla legge 48/2008 cfr. PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Diritto penale e processo*, n. 6/2008, p. 700 ss.; LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processuali*; in *Diritto penale e processo*, n. 6/2008, p. 717 ss.; BELLUTA H., *Cybercrime e responsabilità degli enti*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l.18 marzo 2008, n.48)*, Milano, 2009, p. 83 ss.

ratificato ed attuato la Convenzione *Cyber-crime* sopracitata, apportando modifiche al codice penale e di procedura penale, al Codice *privacy* e al d. lgs. 231/2001, estendendo la responsabilità degli enti a tutti i reati informatici[81].

In modo particolare il legislatore ha provveduto ad abrogare i commi 2 e 3 dell'art. 420 c.p., ed a sopprimere la definizione di "documento informatico" di cui all'art. 491 *bis* c.p., risultando ormai inidoneo a rappresentare la realtà quel richiamo al "supporto informatico" operato dalla legge n. 547/1993[82].

Sono state poi introdotte due nuove fattispecie criminose in materia di firme elettroniche, ovvero l'art. 495 *bis* c.p. *(*Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri) e l'art. 640 *quinquies* c.p. (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica), e tre in materia di danneggiamento informatico, ovvero l'art. 635 *ter* c.p. (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità); l'art. 635 *quater* c.p. (Danneggiamento di sistemi informatici o telematici); e l'art. 635 *quinquies* c.p. (Danneggiamento di sistemi informatici o telematici di pubblica utilità).

---

[81] Inspiegabilmente sono stati esclusi dall'estensione l'art. 495 *bis* c.p. ed il reato di cui all'art. 640 *ter* c.p. qualora non sia commesso in danno allo Stato o ad ente pubblico.

[82] Soprattutto dopo l'avvento di Internet i contenuti informatici possono essere trattati totalmente in modo indipendente dai "supporti" che eventualmente possono contenerli. Abbandonata quindi l'idea di una definizione di "documento informatico" ad *hoc*, oggi, anche ai fini penalistici, il rinvio è al Codice dell'amministrazione digitale (d.lgs. 82/2005). Ai sensi dell'art. 1, comma 1, lett. p) per documento informatico si intende «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».

Nella prima parte dell'art. 491 *bis* la legge n. 48/2008 ha inserito le parole «avente efficacia probatoria». Come evidenziato dal prof. Picotti non si tratta di un requisito superfluo e, inteso in senso non strettamente processuale, svolge l'importante funzione di «guidare l'interprete nella spesso sottile distinzione fra la molteplicità di dati e trattamenti informatici, che pur possono venire in rilievo anche a specifici fini giuridici, ma senza godere di una siffatta tutela, perché privi di una fuzione o rilevanza probatoria». Cfr. PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, cit., p. 704.

Il legislatore del 2008 ha inoltre modificato la disposizione di cui all'art. 615 *quinquies* c.p., estendendo in modo peraltro criticabile le condotte punibili[83], e quella dell'art. 635 *bis* c.p., rendendola procedibile a querela della persona offesa.

Tra le riforme dell'ultimo quinquennio, è particolarmente significativa nel settore quella attuata tramite legge 15 febbraio 2012, n. 12[84] che, nel disciplinare nuove misure per il contrasto ai fenomeni di criminalità informatica, ha introdotto il sequestro dei beni informatici o telematici utilizzati in tutto o in parte per la commissione di reati previsti dalle leggi n. 547/1993 e n. 48/2008 (cui può far seguito il loro affidamento in custodia giudiziale con facoltà d'uso agli organi di polizia o ad altri organi dello Stato) e la confisca dei medesimi beni *ex* art. 240 c.p. (con successiva definitiva assegnazione alle amministrazioni o, a seconda dei casi, agli organi di polizia, di polizia giudiziaria, o altri organi dello Stato).

Dello stesso anno anche la legge di ratifica della Convenzione per la protezione dei minori dall'abuso e dallo sfruttamento sessuale del Consiglio d'Europa[85] che, tra le diverse modifiche apportate, ha introdotto nel codice penale

---

[83] In riferimento al problema relativo alla trasformazione del requisito della dannosità delle apparecchiature, dispositivi e programmi in mero oggetto del dolo specifico cfr. PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, cit., p. 708 ss.

[84] In argomento v. PISTORELLI L., *Legge 15 febbraio 2012, n. 12, recante "Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica" – Disposizioni rilevanti per il settore penale. Relazione a cura dell'Ufficio del Massimario della Corte di Cassazione*, in penalecontemporaneo.it, 28 Febbraio 2012.

[85] La cd. "Convenzione di Lanzarote", è stata adottata dal Comitato dei Ministri del Consiglio d'Europa il 12 luglio 2007 ed aperta alla firma il 25 ottobre 2007 a Lanzarote, dopo un'intensa attività di negoziato avviata nel 2006. L'Italia ha sottoscritto il testo il 7 novembre 2007 ed ha provveduto alla ratifica con legge 172/2012. In tema cfr. PISTORELLI L., ANDREAZZA G., *Legge 1 ottobre 2012, n. 172 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007)*, in penalecontemporaneo.it, 22 Ottobre 2012; GATTA G. L., *Protezione dei minori contro lo sfruttamento e l'abuso sessuale: ratificata la Convenzione di Lanzarote del 2007 (e attuata una mini-riforma nell'ambito dei delitti contro la persona),* in penalecontemporaneo.it, 20 Settembre 2012; PICOTTI L., *La Convenzione di Lanzarote per la tutela penale dei minori dagli abusi sessuali e la sua attuazione in Italia*, in AIAF, n. 3/2013, p. 49 ss.

il nuovo reato di "adescamento di minorenni" (art. 609 *undecies*), che consiste in qualsiasi atto volto a carpire la fiducia di un minore di anni sedici attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete Internet (cd. *grooming*) o di altre reti o mezzi di comunicazione per commettere i reati connessi all'abuso ed allo sfruttamento sessuale dei minori.

Ultime in ordine temporale le modifiche apportate alla frode informatica grazie al più ampio progetto di revisione del codice penale "in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province" attuato con decreto legge 14 agosto 2013, n. 93[86] e successiva legge di conversione 15 ottobre 2013, n. 119[87].

Ravvisata «la necessità di introdurre disposizioni urgenti in materia di ordine e sicurezza pubblica a tutela di attività di particolare rilievo strategico, nonché per garantire soggetti deboli, quali anziani e minori, e in particolare questi ultimi per quanto attiene all'accesso agli strumenti informatici e telematici, in modo che ne possano usufruire in condizione di maggiore sicurezza e senza pregiudizio della loro integrità psico-fisica»[88], è stata introdotta, nel comma 3 dell'art. 640 *ter* c.p., una nuova aggravante ad effetto speciale per il caso in cui il fatto sia commesso

[86] Per un'analisi del d.l. 93/2013 cfr. PISTORELLI L., *Prima lettura del decreto-legge 14 agosto 2013, n. 93 (Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province). Relazione a cura dell'Ufficio del Massimario della Corte di Cassazione*, in penalecontemporaneo.it, 28 Agosto 2013. In argomento, seppur in dettaglio sulla questione del contrasto alla violenza di genere, cfr. RECCHIONE S., *Il decreto legge sul contrasto alla violenza di genere: una prima lettura*, in penalecontemporaneo.it, 15 Settembre 2013; PAVICH G., *Le novità del decreto legge sulla violenza di genere: cosa cambia per i reati con vittime vulnerabili*, in penalecontemporaneo.it, 24 Settembre 2013; per i profili processualistici v. DE MARTINO P., *Le innovazioni introdotte nel codice di rito dal decreto legge sulla violenza di genere, alla luce della Direttiva 2012/29/UE*, , in penalecontemporaneo.it, 8 Ottobre 2013.

[87] Cfr. PISTORELLI L., P*rime note sulla legge di conversione, con modificazioni, del d.l. n. 93 del 2013, in materia tra l'altro di «violenza di genere» e di reati che coinvolgano minori. Relazione a cura dell'Ufficio del Massimario della Corte di Cassazione*, in penalecontemporaneo.it, 18 Ottobre 2013.

[88] Cfr. d.l. 4 agosto 2013, n. 93.

con «furto o indebito utilizzo» dell'identità digitale in danno di uno o più soggetti[89].

Scopo della disposizione è combattere il crescente fenomeno delle frodi realizzate mediante l'accesso abusivo al sistema informatico grazie all'indebito utilizzo dell'identità digitale, intesa, ai sensi del Codice dell'amministrazione digitale, come «l'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi»[90].

La legge di conversione non ha però recepito la disposizione del decreto inerente all'estensione della responsabilità degli enti per la frode informatica aggravata sopracitata, per l'utilizzo indebito di carte di credito o pagamento di cui all'art. 55, comma 9, del d.lgs. 231/2007 e per i reati in materia di violazione della *privacy* di cui agli artt. 167, 168, 169 d.lgs. n. 196/2003.

6. (SEGUE) IL DECRETO CYBER-SICUREZZA (DPCM 24.01.2013)

A pochi giorni dall'identificazione dell'ennesima sofisticata rete di *cyber* spionaggio mondiale denominata "Ottobre Rosso"[91], con Decreto del Presidente

[89] Nell'originaria previsione contenuta nel decreto legge n. 93/2013, al posto di «furto o indebito utilizzo», compariva il termine «sostituzione». Il legislatore quindi, in sede di conversione, ha preferito definire in modo più dettagliato la condotta oggetto dell'aggravante. La specificazione in realtà non sembra soddisfacente dal momento che non viene offerta alcuna definizione di *furto di identità digitale* e dei caratteri che lo contraddistinguono dall'*utilizzo indebito*.

[90] Cfr. art. 1 lett. u-*ter*) del d.lgs. n. 82/2005 così come modificato dal d.lgs. n. 235/2010.

[91] Il 13 gennaio 2013 *Kaspersky Lab*, società russa *leader* nel settore *anti-virus*, ha lanciato l'allarme su un'operazione di hackeraggio di enorme portata contro le principali istituzioni pubbliche di sessantanove paesi diversi. Gli attacchi hanno colpito principalmente Russia ed altre repubbliche ex sovietiche, ma sono stati infettati anche molti *computer* in India, Afghanistan e in particolare in Belgio, dove hanno sede l'Unione europea e la NATO. Meno infezioni sono state registrate negli Stati Uniti, in Iran, Svizzera e Italia. Ribattezzata "Ottobre Rosso", in onore del celebre sottomarino comandato da Sean Connery nel film del 1990, l'operazione di *cyber-crime*, per cinque anni, attraverso una serie di attacchi di spear phishing con email molto personalizzate per target specifici contenenti allegati malevoli sotto forma di file Microsoft Office, avrebbe

del Consiglio dei Ministri del 24 gennaio 2013[92] l'Italia si è dotata di una strategia nazionale in materia di sicurezza informatica, avente l'obiettivo di accrescere le capacità del nostro paese di confrontarsi con le minacce provenienti dallo spazio cibernetico anche attraverso la riorganizzazione dell'architettura istituzionale del settore, considerata disorganica ed inefficiente.

Per la prima volta si è proceduto alla definizione normativa di concetti chiave del settore, quali quelli di spazio, sicurezza, minaccia, evento cibernetico e, nel contempo, di allarme e di situazione di crisi[93].

Ai sensi dell'art. 2 del decreto lo "spazio cibernetico" viene qualificato come «l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi»[94].

Nella definizione in esame, quindi, è ricostruita la complessità della struttura del *cyberspace* contraddistinta da tre dimensioni: fisica, logica e sociale[95].

La "minaccia cibernetica", invece, viene definita come «complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia in

---

permesso di collezionare una mole impressionante di dati, copiando e leggendo mail personali, sms, documenti secretati e tutto il materiale registrato all'interno dei pc infettati.

Non sono stati ancora identificati i creatori ed i mandanti dell'operazione, anche se i sospetti si concentrano sui servizi segreti della Corea del Nord. Per una analisi completa v. *Research report of Red October by Kaspersky Lab's experts* in kaspersky.com.

[92] DPCM 24 gennaio 2013, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", pubblicato in G.U. 19 marzo 2013, n. 66.

[93] Le definizioni riprendono quelle contenute nel "Glossario Intelligence" pubblicato dal Dipartimento Informazioni per la Sicurezza nel giugno 2013.

[94] Cfr. art. 2 comma 1, lett. h) DPCM 24.01.13.

[95] Nel linguaggio comune spesso i termini *Internet* e *Cyberspace* vengono utilizzati come sinonimi. In realtà il primo rappresenta solamente uno degli elementi che sottendono allo spazio cibernetico. Da precisare inoltre che, sempre nel linguaggio comune, le reti di reti (*networks of networks*) sono denominate internet (con la i minuscola), mentre le reti tra *computer* sono denominate *intranet*. I rischi connessi ad Internet rappresentano solamente una parte delle problematiche relative al *cyberspace*.

particolare, nelle azioni di singoli individui o organizzazioni, statuali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi»[96].

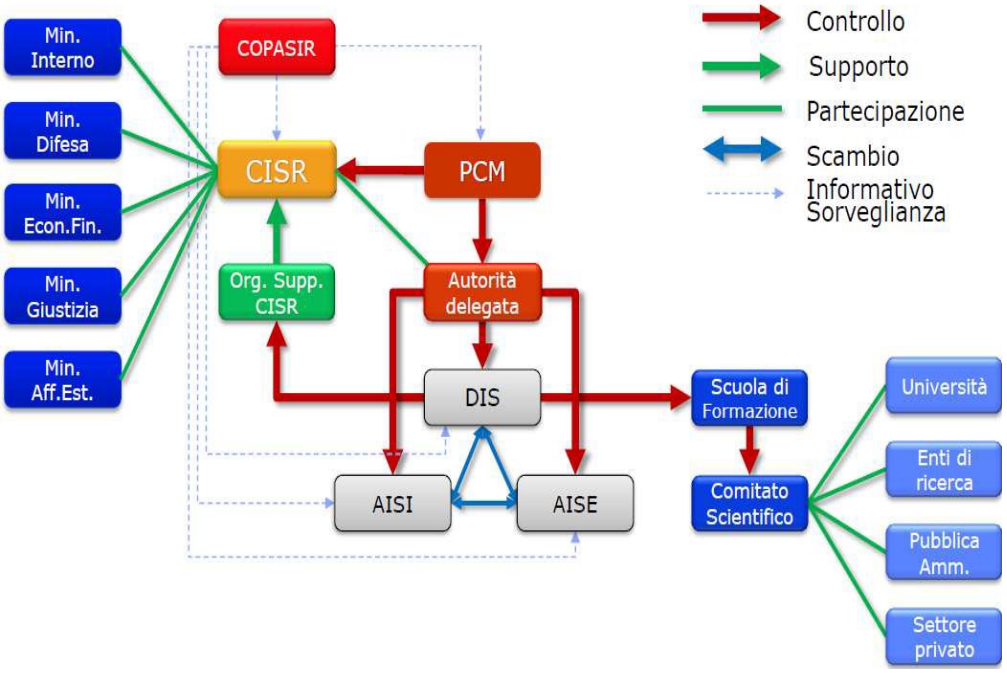
Il decreto delinea quindi i punti chiave dell'architettura della sicurezza cibernetica nazionale, ponendo le basi di un sistema di interventi a tre livelli:

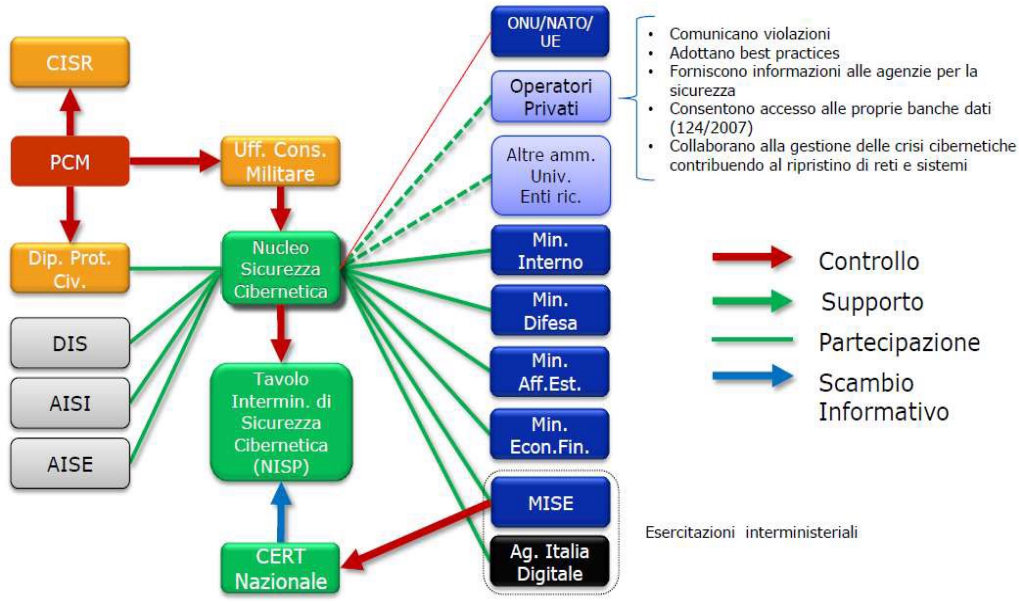
- il livello di indirizzo politico e coordinamento strategico, affidato al Comitato interministeriale per la sicurezza (CISR);

- il livello di supporto e raccordo nei confronti di tutte le amministrazioni, la cui competenza spetta ad un organismo collegiale di coordinamento, presieduto dal Direttore generale del Dipartimento Informazioni per la Sicurezza (DIS);

- il livello di gestione operativa della crisi, per il quale è stato istituito il Nucleo per la sicurezza cibernetica, costituito in via permanente presso l'Ufficio del Consigliere militare e da questo presieduto.

[96] Cfr. art. 2 comma 1, lett. l) DPCM 24.01.13.





* Grafici riassuntivi in ZORZINO G., *Isaca Roma Chapter: Cybersecurity e le strategie nazionali*, in isacaroma.it, 21 maggio 2013.

Al vertice della struttura si trovano quindi il Presidente del Consiglio ed i Ministri che vanno a formare il CISR.

Il Nucleo per la sicurezza informatica è composto invece dai rappresentanti

degli organismi di Intelligence[97] (Dipartimento delle informazioni per la sicurezza DIS, Agenzie informazioni e sicurezza esterna ed interna AISE ed AISI), del Ministero dell'interno, del Ministero degli affari esteri, del Ministero della difesa, del Ministero dello sviluppo economico, del Ministero dell'economia, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale. Esso ha la funzione di sviluppare attività di prevenzione, allertamento e approntamento, in caso di eventuali situazioni di crisi, anche attraverso una propria unità operativa permanente e costantemente attiva, nonché di svolgere le opportune azioni di risposta e ripristino rispetto a queste situazioni, provvedendo ad «attivare il Tavolo interministeriale di crisi cibernetica»[98], nell'ipotesi in cui un c.d. evento cibernetico (attacco, incidente, furto/spionaggio) assuma «dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale» o non possa «essere fronteggiato dalle singole amministrazioni competenti in via ordinaria»,

Ai sensi dell'art. 3 comma 1 lett. a), b) del DPCM 24.01.13, il Presidente del Consiglio dei Ministri ha poi adottato, con Decreto 27 gennaio 2014, il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", che individua gli "indirizzi strategici" da perseguire per un accrescimento delle capacità del paese di prevenire e rispondere alle sfide poste dallo spazio cibernetico, ed il relativo "Piano nazionale per la protezione cibernetica" contenente in specifico gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare le indicazioni del Quadro Strategico[99].

---

[97] Per comprendere il funzionamento dei diversi organi e delle autorità del Sistema di informazione per la sicurezza della Repubblica istituito in seguito al varo della legge n. 124/2007 v. sicurezzanazionale.gov.it.

[98] Cfr. art. 9 comma 3, lett. b) DPCM 24.01.13.

[99] DPCM 27 gennaio 2014, "Strategia nazionale per la sicurezza cibernetica", pubblicato in G.U. 19 febbraio 2014, n. 41. Il Quadro Strategico ed il Piano Nazionale sono stati elaborati dal Tavolo Tecnico Cyber (TTC) che – istituito il 3 aprile 2013 in seno all'organismo collegiale permanente (c.d. CISR "tecnico") dopo l'entrata in vigore del DPCM 24 gennaio 2013 – opera presso il Dipartimento Informazioni per la Sicurezza. Ai lavori del TTC partecipano i punti di contatto *cyber* dei Dicasteri CISR (Affari Esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo Economico) dell'Agenzia per l'Italia Digitale e del Nucleo per la Sicurezza Cibernetica.

Gli indirizzi identificati nel Quadro Strategico sono:

1. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;

2. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese;

3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali;

4. Promozione e diffusione della cultura della sicurezza cibernetica;

5. Rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali *on-line*;

6. Rafforzamento della cooperazione internazionale.

Al fine di dare concreta attuazione agli indirizzi operativi del Piano Nazionale, viene dettagliata una *roadmap* così composta:

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare;

2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati;

3. Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento;

4. Cooperazione internazionale ed esercitazioni;

5. Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteriali;

6. Interventi legislativi e *compliance* con obblighi internazionali;

7. *Compliance* a *standard* e protocolli di sicurezza;

8. Supporto allo sviluppo industriale e tecnologico;

9. Comunicazione strategica;

10. Risorse;

11. Implementazione di un sistema di Information Risk Management nazionale.

Interessante notare come nel Quadro Strategico, a proposito dello "spazio cibernetico", si affermi che esso costituisce un «dominio virtuale di importanza

strategica per lo sviluppo economico, sociale e culturale delle nazioni»[100]. E' proprio questa sua caratteristica a rendere necessaria la ricerca di un equilibrio tra esigenze di sicurezza nazionale e di ordine pubblico, da un lato, e libertà individuali, dall'altro. «Si pensi, ad esempio, come l'ininterrotto monitoraggio tecnico della funzionalità delle reti e la protezione dei dati che vi transitano siano essenziale presupposto per il pieno godimento del diritto alla privacy e dell'integrità dei sistemi oppure, sempre a titolo di esempio, come possa essere complesso ricercare il giusto equilibrio tra il diritto alla privacy e la necessaria azione di contrasto a crimini come l'uso della rete per lo scambio di materiale pedopornografico, lo spaccio di stupefacenti, l'incitamento all'odio o la pianificazione di atti di terrorismo. Reati che, oltre a ledere specifici diritti, rappresentano un attacco all'idea stessa di un dominio cibernetico libero, democratico ed aperto»[101].

Sembra quindi profilarsi un nuovo bene giuridico, che potremmo definire "*cyberspace* sano", grazie al quale ricomporre, almeno parzialmente, la frammentarietà del quadro legislativo descritto nella breve cronologia nazionale delle principali riforme legislative del paragrafo precedente[102].

---

[100] *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, CAPITOLO 1: PROFILI E TENDENZE EVOLUTIVE DELLE MINACCE E DELLE VULNERABILITÀ DEI SISTEMI E DELLE RETI DI INTERESSE NAZIONALE, p. 10.

[101] *Ivi*, p. 11.

[102] Già nel 1992, prima dell'avvento di Internet, il prof. Militello suggeriva l'esistenza di un nuovo bene giuridico, la cd. *"intangibilità informatica"*, in relazione al quale procedere in un intervento normativo di ampio respiro che evitasse la dispersione delle fattispecie incriminatrici in una pluralità di testi normativi. L'intangibilità informatica veniva identificata nella «multiforme esigenza di non alterare la relazione triadica fra dato della realtà, rispettiva informazione, e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento, ricezione). Tale relazione assume sovente un profilo economico […] Altre volte, come nel caso dei documenti informatici, vi è un'esigenza di tutelare o la rappresentazione della realtà incorporata nei dati informatici, su cui fare affidamento, o la riservatezza stessa delle informazioni. Sempre tuttavia sarebbe riduttivo limitare il profilo offensivo ai beni giuridici più tradizionali, come il patrimonio, la fede pubblica o l'economia pubblica, in quanto nessuno di essi, se isolatamente considerati, esaurisce la dimensione materiale delle offese realizzate dalla maggioranza degli illeciti informatici. Questi colpiscono tanto la conformità del dato con la realtà, quanto il possibile profilo patrimoniale di tale relazione. Né può trascurarsi che nella società contemporanea esiste un

Soffermando ora l'attenzione sulla definizione di "minaccia cibernetica", introdotta nel DPCM 24.01.13 e ripresa dal Quadro Strategico, risulta evidente come il legislatore abbia accolto una nozione che travalica i confini della categoria dei "reati ciberniciti".

Ricomprendendo «l'insieme delle condotte controindicate che possono essere realizzate nel e tramite lo spazio cibernetico ovvero in danno di quest'ultimo e dei suoi elementi costitutivi»[103], nell'alveo della minaccia cibernetica potrebbero essere ricondotti non solo i reati cibernetici in senso stretto ed in senso lato, ma anche i reati informatici, che pur non realizzandosi in o tramite la rete, hanno ad esempio come oggetto passivo i nuovi strumenti della tecnologia informatica.

Il contenitore "minaccia informatica" sembrerebbe idoneo quindi a raggruppare tutte le categorie di reati descritte nel terzo paragrafo del presente capitolo.

La nuova nozione di spazio cibernetico e la valorizzazione delle sue tre componenti (dimensione fisica, logica e sociale) porta quindi il legislatore a discostarsi dalla comune definizione di *cyber-crime*, riconducendo alla stessa, forse in modo improprio, attività tradizionalmente assimilate ai fenomeni, non necessariamente cibernetici, della ben più ampia arena della cd. criminalità informatica.

La "criminalità cibernetica", intesa quale una delle quattro macro-categorie in cui viene suddivisa la minaccia cibernetica[104], nel quadro Strategico viene

---

più generale interesse economico ad una circolazione rapida dei dati». V. MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Rivista trimestrale di diritto penale dell'economia*, 1992, p. 365 ss.

[103] *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, CAPITOLO 1, p. 11.

[104] *Ivi,* p. 12-13: «**Tipi di minaccia** A seconda degli attori e delle finalità si usa distinguere la minaccia cibernetica in quattro macro-categorie. Si parla in tal caso di

- *criminalità cibernetica (cyber-crime)*: complesso delle attività con finalità criminali (quali, per esempio, la truffa o frode telematica, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali);

- *spionaggio cibernetico (cyber-espionage)*: acquisizione indebita di dati/informazioni sensibili, proprietarie o classificate;

genericamente identificata come «il complesso delle attività con finalità criminali». Tra le fattispecie richiamate a titolo esemplificativo compaiono la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali, ovvero, per l'appunto, fattispecie informatiche solo eventualmente realizzabili in Internet.

Sembrerebbe quindi invertito la stesso rapporto intercorrente tra l'insieme "crimine informatico" e quello "*cyber-crime*", risultando in tal modo il primo un sottoinsieme del secondo.

La soluzione prospettata porterebbe all'illogica rischiosa conseguenza di negare la competenza penale dell'Unione europea in materia di *cyber-crime*, dato che, tra le aree individuate nell'art. 83 TFUE, viene menzionata la sola «criminalità informatica».

Per superare tale *impasse* forse sarebbe più corretto ritornare a valorizzare l'elemento della rete Intenet nel momento di identificazione dei reati cibernetici.

- *terrorismo cibernetico (cyber-terrorism)*: insieme delle azioni ideologicamente motivate, volte a condizionare uno stato o un'organizzazione internazionale;

- *guerra cibernetica (cyber-warfare)*: insieme delle attività e delle operazioni militari pianificate e condotte allo scopo di conseguire effetti nel predetto ambiente».

CAPITOLO TERZO

MODELLI DI REGOLAMENTAZIONE DELLA RESPONSABILITÀ DELL'*INTERNET SERVICE PROVIDER*

SOMMARIO: 1. *US Communications Decency Act* (CDA) e *Digital Millennium Copyright Act* (DMCA) - 2. *Gesetz zur Regelung der Rahmenbedingungen für Informations-und Kommunikationsdienste* (IuKDG) e *Telemediengesetz* (TMG) - 3. La Direttiva Europea sul Commercio Elettronico - 4. La normativa italiana di riferimento: il Decreto Legislativo n. 70/2003.

Tra le questioni giuridiche connesse all'esplosione della criminalità *on-line*, la problematica della responsabilità penale dell'*Internet service provider* (ISP), ossia, come specificato nel precedente capitolo, del soggetto che, a diversi livelli, gestisce il flusso d'informazioni che transitano via Internet, è sicuramente tra le più dibattute. La tematica risulta particolarmente complessa e delicata non con riguardo agli illeciti commessi direttamente dall'ISP nella veste di autore o coautore (trovando in tali casi applicazione le disposizioni comuni in tema di imputazione della responsabilità), ma in relazione a quelli realizzati dagli utenti della rete[1], per i quali sorgono innanzitutto limiti in virtù del principio di personalità di cui all'art. 27 Cost.

L'esigenza di configurare una responsabilità degli ISPs anche nell'ipotesi d'illeciti commessi dai terzi nasce dalla difficoltà con cui questi sono individuabili, potendo beneficiare dell'anonimato o di altri strumenti tecnici per mascherare la propria identità. E' inoltre chiaro che il prestatore di servizi,

[1] Cfr. RAZZANTE R., *Manuale di diritto dell'informazione e della comunicazione. Privacy, diffamazione e tutela della persona. Libertà e regole nella Rete*, Milano, 2013, p. 380 ss.

fornendoli di solito in forma d'impresa, sarà presumibilmente più solvibile rispetto al singolo autore del reato[2].

D'altra parte è ugualmente vero che prevedere obblighi di controllo e garanzia a carico dei *providers* renderebbe più onerosa la loro attività, con possibili conseguenti effetti inibitori sullo sviluppo libero della rete[3]: dal punto di vista economico i maggiori costi potrebbero essere addebitati agli internauti tramite l'aumento dei servizi a pagamento; dal punto di vista giuridico gli ISPs sarebbero inoltre portati a privilegiare forme di censura onde evitare di incappare in una responsabilità che, data la difficoltà tecnica del controllo sugli innumerevoli contenuti trasmessi, si avvicinerebbe molto ad una responsabilità di tipo oggettivo[4].

Preliminarmente alla disamina dei riferimenti normativi nazionali sul tema si rende necessario premettere qualche cenno sui sistemi che hanno influenzato i formanti legislativo, dottrinale e giurisprudenziale italiani[5].

---

[2] Cfr. MAGLI S., SPOLIDORO M. S., *La responsabilità degli operatori in Internet: profili interni e internazionali*, in *Il Diritto dell'Informazione e dell'Informatica*, 1997, p. 61 ss.

[3] Cfr. BUGIOLACCHI L., *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet Provider. Una sintesi di diritto comparato*, in *Il Diritto dell'Informazione e dell'Informatica,* 2000, p. 836 ss.

[4] Cfr. RODOTÀ S., *Relazione introduttiva: Libertà, opportunità, democrazia, informazione*, Convegno *Internet e privacy – Quali regole?*, cit.

[5] Per una visione complessiva della tematica della responsabilità del *provider* in chiave comparatistica cfr. KOELMAN K., HUGENHOLTZ B., *Online Services Provider Liability for Copyright Infringement*, WIPO Workshop on Service Provider Liability, Geneva, 9 dicembre 1999, in dare.uva.nl; BAISTROCCHI P., *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in *Santa Clara High Techology Law Journal*, Volume 19, Issue 1, Article 3, 2002, p. 111, anche in digitalcommons.law.scu.edu; EDWARDS L., *Role and responsibility of internet intermediaries in the field of copyright and related rights*, in wipo.int, 22 Giugno 2011.

1. *US COMMUNICATIONS DECENCY ACT* (CDA) E *DIGITAL MILLENNIUM COPYRIGHT ACT* (DMCA)

Gli Stati Uniti, culla della rivoluzione cibernetica, sono stati i primi ad affrontare le problematiche inerenti alla possibile rilevanza penale delle condotte degli ISPs per gli abusi e gli illeciti commessi in rete.

E' fondamentale in premessa segnalare che nel sistema americano, oltre alla responsabilità diretta dell'autore del reato (basata sulla sua *mens rea* oltre che su *actus reus*) e del compartecipe (*contributory liability*), viene riconosciuta una sorta di responsabilità indiretta-oggettiva per il fatto altrui, cd. *vicarious liability*, in presenza di determinate relazioni e per la tutela di specifici beni[6]. In modo

[6] Cfr. BALLON I. C., *Secondary trademark liability for internet and mobile sites and services and other intermediaries*, LAIPLA (Los Angeles Intellectual Property Law Association) spring seminar, Ojai, California, 6-8 Giugno 2014, in laipla.net; DIXON A. N., *Liability of users and third parties for copyright infringements on the Internet: overview of international developments*, in STROWEL A. (ed.), *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham, 2009, p. 12 ss.; FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010, p. 68 ss.; GATTEI C., *Considerazioni sulla responsabilità dell'Internet provider*, in interlex.it, 23 Novembre 1998. Con particolare riguardo alle forme di responsabilità penale per fatto altrui riconosciute nel sistema americano cfr. Corte Suprema della Pennsylvania, *Commonwealth v Koczwara*, 397 Pa. 575 (1959), 25 novembre 1959. Per una immediata comprensione della questione meritano di essere riportate testualmente le riflessioni conclusive del Giudice Cohen: «*At common law, any attempt to invoke the doctrine of respondeat superior in a criminal case would have run afoul of our deeply ingrained notions of criminal jurisprudence that guilt must be personal and individual. In recent decades, however, many states have enacted detailed regulatory provisions in fields which are essentially non-criminal, eg, pure food and drug acts, speeding ordinances, building regulations, and child labor, minimum wage and maximum hour legislation. Such statutes are generally enforceable by light penalties, and although violations are labelled crimes, the considerations applicable to them are totally different from those applicable to true crimes, which involve moral delinquency and which are punishable by imprisonment or another serious penalty. Such so-called statutory crimes are in reality an attempt to utilize the machinery of criminal administration as an enforcing arm for social regulations of a purely civil nature, with the punishment totally unrelated to questions of moral wrongdoing or guilt. It is here that the social interest in the general well-being and security of the populace has been held to outweigh the individual interest of the particular defendant. The penalty is imposed despite the defendant's lack*

particolare gli intermediari cibernetici sarebbero indirettamente responsabili per le violazioni realizzate dagli utenti nel caso in cui controllino l'attività illecita e ne traggano beneficio economico[7].

Poiché raramente i fornitori dei servizi sono gli autori diretti della violazione o possono essere chiamati a rispondere di concorso colposo[8], se non altro per le difficoltà di dimostrare gli elementi della *coulpability*, particolarmente interessante risulta l'indagine della terza ipotesi.

Negli US la regolamentazione della responsabilità dei *providers* per i contenuti immessi dai propri utenti è "verticale" nel senso che, a differenza del modello europeo, consta di norme per settori determinati. Nello specifico si rinvengono una forma d'immunità relativa a tutti i tipi di materiale, ad eccezione della proprietà intellettuale (IP), e *"safe harbours"* in materia di violazione del *copyright*[9].

Il primo settore in cui si è affrontata la problematica della responsabilità "indiretta" degli ISPs è stato quello connesso alla *"indecency"*.

---

of a criminal intent or mens rea». (Testo integrale della sentenza in justia.com). Come nel nostro sistema, quindi, la configurabilità di una responsabilità penale per fatto altrui in determinati settori, si scontra con il principio cardine della colpevolezza personale ed individuale. Il riconoscimento della *vicarious liability* risulta tutt'altro che pacifico, sollevando inoltre problematiche in ordine alla garanzia del "giusto processo" di cui al Quinto e Quattordicesimo Emendamento della Costituzione degli Stati Uniti.

[7] Cfr. *United States District Court for the Southern District of New York, Shapiro, Bernstein e Co. v. HL verde Co.*, 316 F.2d 304 (2d Cir.1963).

[8] La responsabilità del compartecipe richiede che lo stesso abbia *knowledge* dell'attività illecita e contribuisca alla condotta dell'autore materialmente o moralmente. A riguardo cfr. United States Court of Appeals for the Second Circuit*, Tiffany Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010). Per un esaustivo commento al caso ed un'analisi delle difficoltà riscontrate nel rinvenire una responsabilità degli ISPs per la vendita di materiali contraffatti da parte degli utenti cfr. ABDEL-KHALIK J., *Is eBay counterfeiting?*, in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, London, 2013, p. 142 ss.

[9] Cfr. TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, cit., p. 3 ss.

Nel febbraio del 1996 il Congresso ha approvato il *Communications Decency Act* (CDA)[10], nel tentativo di frenare la dilagante diffusione in Internet di materiale osceno e limitarne l'accesso ai minori[11].

Onde garantire comunque lo sviluppo della rete e preservare il libero mercato, nel titolo 47 del *U.S. Code* è stata prevista innanzitutto l'immunità del *provider* per i contenuti osceni ed indecenti immessi in rete[12], a meno che quest'ultimo *«is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications»*[13] o *«provides access or*

[10] Il CDA rappresenta il titolo quinto del *Telecommunications Act*, con il quale si è proceduto ad una significativa revisione dell'intero sistema delle telecomunicazioni, precedentemente disciplinato dal *Communications Act* del 1934, includendo anche Internet tra i *"broadcasting and spectrum allotment"*. Cfr. ECONOMIDES N., *The Telecommunications Act of 1996 and its impact*, in nyu.edu, Settembre 1998; HAZLETT T. V., *Economic and Political Consequences of the 1996 Telecommunications Act*, in *Hastings Law Journal* 50-1998/1999, p. 1359 ss., anche in heinonline.org. Con riguardo specifico al CDA cfr. CANNON R., *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, in *Federal Communications Law Journal*, Volume 49-Issue1, Article 3, 1996, anche in indiana.edu; LANGDON R. T., *The Communications Decency Act § 230: Make Sense? Or Nonsense?-A Private Person's Inability to Recover if Defamed in Cyberspace*, in *St. John's Law Review*, Volume 73-Issue 3, Article 11, 1999, anche in stjohns.edu.

[11] Le preoccupazioni per i rischi legati all'utilizzo delle nuove tecnologie e la necessità di un intervento son ben rappresentate dalle parole del senatore Exon: *«The information superhighway should not become a red light district. This legislation will keep that from happening and extend the standards of decency which have protected telephone users to new telecommunications devices. Once passed, our children and families will be better protected from those who would electronically cruise the digital world to engage children in inappropriate communications and introductions. The Decency Act will also clearly protect citizens from electronic stalking and protect the sanctuary of the home from uninvited indecencies»* (141 Congr. Rec. S1953, daily ed. Feb. 1, 1995).

[12] 47 *U.S. Code* § 230 (e) (1) *«No person shall be held to have violated subsection (a) or (d) of this section solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication»*.

[13] 47 *U.S. Code* § 230 (e) (2).

connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person»[14].

Alla sezione 231 è stata regolamentata invece l'esclusione di responsabilità per gli intermediari che forniscano materiale pericoloso adottando misure volte a limitare l'accesso dei minori (ad es. attraverso la richiesta dell'*"adult personal identification number"*).

Di estrema importanza, infine, la disposizione di cui alla sezione 230 (c) (1), che ha escluso l'equiparabilità dei *providers* ai normali editori, determinandone l'irresponsabilità civile in riferimento alle informazioni fornite dai terzi quando l'ISP, dimostrata la sua buonafede, impedisca l'accesso alle informazioni ritenute offensive, oscene o lesive a qualsiasi titolo dei diritti altrui, ovvero intervenga bloccando tali contenuti su istanza di un utente che segnali l'illiceità dell'informazione (cd. *good samaritan prevision*)[15].

Ad un solo anno di distanza dall'entrata in vigore del CDA alcune norme in esso contenute criminalizzanti la "*knowing transmission of obscene or indecent messages to any recipient under 18 years of age"* nonchè la "*knowing sending or*

---

[14] 47 *U.S. Code* § 230 (e) (3).

[15] 47 *U.S. Code* § 230 (c): *Protection for "Good Samaritan" blocking and screening of offensive material (1) Treatment of publisher or speaker*

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph.

Nella successiva *Section* 230 (f) (2) si specifica la nozione di *interactive computer service* definito come: *«any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational».*

displaying to a person under 18 of any message that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs", sono state dichiarate incostituzionali per violazione del Primo emendamento della Costituzione che tutela, tra le altre, anche la libertà di parola e di stampa[16].

Nessun giudizio d'illegittimità ha colpito invece la *good samaritan prevision*, che, anzi, è divenuta pietra angolare del sistema e viene applicata in senso ampio dalle Corti[17].

Pur essendo specificata nella sezione 230 (e) l'esclusione di qualsiasi incidenza dell'immunità in esame sul diritto penale, sulla *Intellectual property law,* sulla *State law*[18] e *Communications privacy law*, il riconoscimento della

[16] Cfr. Corte Suprema Federale, sent. *Reno v American Civil Liberties Union* (ACLU), 521 U.S. 844, consultabile alla pagina supreme.justia.com, con la quale nel 1997 il *"free speech"* in Internet assurge a principio fondamentale e viene dichiarata l'illegittimità costituzionale del *Telecommunication Act* -§223(a)(1), (B)(ii), (d)- nella parte in cui stabilisce sanzioni penali ed amministrative in relazione alle fattispecie di diffusione e agevolazione della diffusione via Internet a minori di comunicazioni oscene o offensive della decenza. Cfr. DOUGLAS M. F., *Reno v. ACLU*, in PARKER R. A., *Free speech on trial*, Tuscaloosa, 2003, p. 298 ss.; DOUGLAS M. F., TUMAN J. S., *Freedom of Expression in the Marketplace of Ideas*, California, 2010, p. 289 ss.

[17] Per un'analisi della giurisprudenza di riferimento precedente e successiva rispetto al "punto di non ritorno" rappresentato dalla *good samaritan prevision* in lingua italiana cfr. RISTUCCIA R., TUFFARELLI L., *La natura giuridica di Internet e la responsabilità del provider*, in interlex.it, 19 Giugno 1997; NATOLI R., *La tutela dell'onore e della reputazione in internet: il caso della diffamazione anonima*, in *Europa e diritto privato*, n. 2/2001, p. 441 ss.; DE CATA M., *La responsabilità civile dell'Internet service provider*. *Collana Università degli studi di Milano - Bicocca dip. dir. Economia*, 2010.

[18] Interessante a tal proposito notare come in realtà la sezione 230 incida anche sulle scelte d'incriminazione dei singoli Stati. Nel 2012 lo Stato di Washington ha adottato una legge (SB 6251) **in materia di prostituzione minorile in rete**, che tra i dettami configurava una responsabilità penale degli ISPs per **la pubblicazione di annunci pubblicitari per la compravendita di servizi erotici con minori.** Gli attivisti di *Electronic Frontier Foundation* (EFF) ed i responsabili di *Internet Archive* hanno presentato ricorso contro la legge in questione proprio per conflitto con la sezione 230 del CDA. Il caso è stato chiuso il 10 dicembre 2012, quando il giudice distrettuale Ricardo Martinez, in virtù della violazione della sezione in esame nonché della sospetta incostituzionalità della legge ha riconosciuto che «*Backpage and the Internet Archive were to be awarded permanent injunctive» and «recover $200,000 for costs and*

responsabilità penale *in action* dei *providers* è stato limitato ai soli casi di partecipazione diretta nell'illecito e quindi di fornitura di "propri" contenuti illegali o di materiale contributo alla lorocreazione[19].

La responsabilità degli ISPs in materia di *intellectual property*[20], per l'appunto sottratta dalla generale immunità di cui alla sezione 230 (c), è stata

---

attorneys' fees from the Office of the Attorney General». V. *Backpage.com v McKenna, et al.* in dmlp.org.

Stessa sorte è toccata poi al simile Statuto del New Jersey A3352 (consultabile in state.nj.us), cfr. *News* 4 Luglio 2013 in punto-informatico.it.

[19] Cfr. in modo particolare corte Suprema della Calafornia, sent. 20 novembre 2006, *Barrett v Rosenthal*, in cui si ripercorrono in modo approfondito la storia legislativa della sezione 230 (c) (1) e la giurisprudenza relativa (ad es. *leading case Zeran v America Online*). Testo integrale della sentenza in casp.net. V. in commento FALETTI E., *La responsabilità dell'internet provider in diritto comparato per materiale pubblicato da terzi*, in *Diritto dell'Internet*, n. 2/2007, p. 137 ss.

In senso critico parte della dottrina sta mettendo in luce come l'immunità garantita agli ISPs dalla sezione 230 del CDA disincentivi totalmente qualsiasi attività volta al controllo e alla rimozione dei contenuti illeciti postati dagli utenti, con importanti ripercussioni negative sulla tutela delle vittime. V. BARTOW A., *Barnes v. Yahoo! And Section 230 ISP immunity*, in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, cit., p. 161: *«only a refashioning of Section 230 immunity will induce online service providers to find cost-effective ways to assist Internet harassment victims. They will not evolve into true Good Samaritans without powerful legal incentives to do so»*.

[20] La *World Intellectual Property Organization (WIPO)*, agenzia specializzata delle Nazioni Unite creata nel 1967 con finalità di sviluppo della protezione della proprietà intellettuale nel mondo, che attualmente conta 187 stati membri, tra i quali gli USA e l'Italia, nella *Convention Establishing the World Intellectual Propriety* (WIPO), conclusa a Stoccolma il 14 luglio 1969, all'art. 2 (viii) ha stabilito che "*Intellectual Property" «shall include the rights relating to:*

- literary, artistic and scientific works,

- performances of performing artists, phonograms, and broadcasts,

- inventions in all fields of human endeavor,

- scientific discoveries,

- industrial designs,

- trademarks, service marks, and commercial names and designations,

- protection against unfair competition,

and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields».

disciplinata tramite il *Digital Millennium Copyright Act* (DMCA)[21], del 28 ottobre 1998, che, con il cd. *"provvedimento porto sicuro"*[22], ha inserito nel Titolo 17 dello *U.S. Code* la sezione 512, rubricata *Limitations on liability relating to material online*, che prevede clausole limitative della responsabilità dei *providers* relativamente alle violazioni del *copyright* commesse dai loro utenti[23].

Si tratta quindi di un arcilessema comprendente i diritti connessi alla proprietà industriale e al *copyright* (inteso nei termini di diritto d'autore e diritti connessi di cui al secondo punto dell'articolo in esame).

Per un'analisi approfondita del sistema americano in materia di *copyright*, sia dal punto di vista normativo che giurisprudenziale, si rinvia, anche per gli ampi richiami bibliografici, a FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, cit., p. 68 ss.

[21] Per uno sguardo complessivo al DMCA v. *The digital millennium copyright act of 1998: U.S. Copyright Office Summary*, in copyright.gov, Dicembre 1998. Il DMCA oltre a prevedere norme specifiche in materia di diritto d'autore implementa due trattati del 1996 del WIPO ovvero il *WIPO Copyright Treaty e il WIPO Performances and Phonograms Treaty*.

[22] DMCA *Title II – "Online Copyright Infringement Liability Limitation Act" (OCILLA) detto anche* DMCA 512. In riferimento ai *safe harbours* e al loro *background* giurisprudenziale e normativo cfr. REICHMAN J. H., DINWOODIE R. G., SAMUELSON P., *A reverse notice and takedown regime to enable public interest uses of technically protected copyrighed works*, in STROWEL A. (ed.), *Peer-to-peer file sharing and secondary liability in copyright law*, cit., p. 235 ss.

[23] Introdotti dal *Copyright Law* del 1987, i *criminal offenses* in materia di *copyright infringement* sono contenuti nella sezione 506 del Titolo 17 dello *U.S. Code* il quale prevede:

«(a) Criminal Infringement.

(1) In general.— Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed

(A) for purposes of commercial advantage or private financial gain;

(B) by the reproduction or distribution, including by electronic means, during any 180–day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or

(C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

(2) Evidence. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright.

(3) Definition. In this subsection, the term "work being prepared for commercial distribution" means

Innanzitutto, per beneficiare delle esenzioni è richiesto il rispetto da parte degli ISPs di due condizioni generali, ovvero adottare e ragionevolmente attuare, anche informando i propri utenti, *«a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers»*[24], nonché accogliere e non interferire con le *standard technical measures* di protezione del *copyright*[25].

(A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution

(i) the copyright owner has a reasonable expectation of commercial distribution; and

(ii) the copies or phonoecords of the work have not been commercially distributed; or

(B) a motion picture, if, at the time of unauthorized distribution, the motion picture

(i) has been made available for viewing in a motion picture exhibition facility; and

(ii) has not been made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a motion picture exhibition facility.

(b) Forfeiture, Destruction, and Restitution. Forfeiture, destruction, and restitution relating to this section shall be subject to section 2323 of title 18, to the extent provided in that section, in addition to any other similar remedies provided by law.

(c) Fraudulent Copyright Notice. Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than $2,500.

(d) ***Fraudulent Removal of Copyright Notice.*** *Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than $2,500.*

(e) ***False Representation.*** *Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than $2,500.*

(f) ***Rights of Attribution and Integrity.*** *Nothing in this section applies to infringement of the rights conferred by section 106A (a)».*

[24] 17 *U.S. Code* §512 (i) (1) (A).

[25] Ai sensi dell *17 U.S. Code* §512 (i) (2) le *standard technical measures* sono *«technical measures that are used by copyright owners to identify or protect copyrighted works and*

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

I *safe harbours* descritti nella sezione 512 vengono quindi differenziati sulla base dell'attività svolta dall'ISP.

Una prima totale esenzione di responsabilità è prevista nel caso in cui il *service provider* operi quale mero canale per la trasmissione dai dati[26], ovvero si identifichi in una *«entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received»*[27].

La trasmissione del materiale che viola il *copyright* deve iniziare da o sotto la direzione di un terzo e procedere attraverso un iter tecnico-automatico senza che il *provider* operi la selezione del materiale e del destinatario. Le eventuali copie intermedie, infine, devono essere accessibili solo al destinatario per un periodo non superiore a quello che *«is reasonably necessary for the transmission, routing, or provision of connections»*[28].

Per quanto riguarda le altre limitazioni di responsabilità, invece, il legislatore adotta una accezione più ampia di *service provider*, descritto nei termini di *«provider of online services or network access, or the operator of facilities therefor»*[29].

In riferimento all'attività di *caching*, ovvero *«the intermediate and temporary storage of material on a system or network»*[30], l'esenzione opera se il materiale

---

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks».

[26] 17 *U.S. Code* § 512 (a).

[27] 17 *U.S. Code* § 512 (k) (1) (A).

[28] *17 U.S. Code* § 512 (a) (4).

[29] *17 U.S. Code* § 512 (k) (1) (B).

[30] *17 U.S. Code* § 512 (b). La memorizzazione intermedia e temporanea di dati ha un impatto molto positivo sulla fluidità del traffico telematico permettendo di ridurre notevolmente il tempo di attesa per le richieste successive degli utenti concernenti le stesse informazioni. Tra gli aspetti negativi del *caching* invece si annoverano la possibilità che i dati inviati siano obsoleti e che i

illecito, immesso nella rete dal terzo e archiviato in modo automatico, venga trasmesso al richiedente senza che l'ISP ne modifichi in alcun modo il contenuto. E' necessario inoltre che il *provider* garantisca la perfetta conformità della copia offerta agli utenti a quella originale, mediante gli opportuni aggiornamenti, nonché la riproduzione delle medesime modalità di accesso; non interferisca con la raccolta delle cd. *hit information*[31]; ed infine, risponda *expeditiously* agli avvisi degli utenti relativi alla pubblicazione di materiale senza autorizzazione del titolare del *copyrigh*, rimuovendo o bloccando il materiale illecito qualora lo stesso sia già colpito da queste misure nel sito di origine, o sia stato oggetto a medesimo ordine da parte di un tribunale[32].

Il *safe harbour* nel caso di *storage of information on systems or networks at direction of users*[33] è concesso a condizione che il *provider* non abbia *actual knowledge* dell'illeceità dei contenuti o dell'attività che si svolge nello spazio che egli concede alla totale gestione dell'utente, ovvero *constructive knowledge* cioè *«is not aware of facts or circumstances from which infringing activity is*

---

providers non siano in grado di controllarne la "popolarità", ovvero il numero di richieste precise di un determinato *file*.

[31] *Cfr. 17 U.S. Code* § 512 (b) (2) (C) *«the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology—*

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person».

[32] L'art. 17 *U.S. Code* § 512 (b) (2) (E) (Ii) precisa che l'utente, nell'inviare la *notification*, deve allegare alla stessa la dichiarazione attestante la rimozione o il blocco nel sito originale ovvero il relativo ordine del tribunale. Questo per evitare che semplici avvisi degli utenti possano legittimare opere di censura da parte dei *cache providers.*

[33] 17 *U.S. Code* § 512 (c).

apparent»[34]; o ancora se *«upon gaining such knowledge or awareness, acts expeditiously to remove, or disable access to the material»*[35]. L'ISP, inoltre, se ha il diritto e la capacità di controllare l'attività illecita, non deve trarne alcun beneficio finanziario e, ricevuta dal soggetto specificatamente designato[36] una

[34] 17 *U.S. Code* § 512 (c) (1) (A) (ii). La valutazione del parametro della *knowledge* in tal caso viene anche detta "red flag" test. V. SENATOR HATCH, *The Digital Millenium Copyright Act of 1998, Report together with Additional Views to Accompany S. 2037*, Report 105-190, 11 Maggio 1998, p. 44, in digital-law-online.info: *«Subsection (c)(1)(A)(ii) can best be described as a ''red flag'' test. As stated in subsection (l), a service provider need not monitor its service or affirmatively seek facts indicating infringing activity (except to the extent consistent with a standard technical measure complying with subsection (h)), in order to claim this limitation on liability (or, indeed any other limitation provided by the legislation). However, if the service provider becomes aware of a ''red flag'' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action. The ''red flag'' test has both a subjective and an objective element. In determining whether the service provider was aware of a ''red flag,'' the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a ''red flag''—in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances—an objective standard should be used».*

Dal testo normativo, sembrerebbe quindi che la *knowledge* e la *awareness* in tal caso siano totalmente indipendenti dalla *takedown notice*. In realtà in giurisprudenza questa distinzione e tutt'altro che pacifica: v. *U.S. District Court for the Southern District of New York*, *Viacom International, Inc. v YouTube, Inc.*, 07 Civ. 2103. In dottrina cfr. in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*: HASSANABADI A., *Red flags of "piracy" online*, p. 112; TRAVIS H., *Who controls the Internet? The second circuit on YouTube, p. 136 ss*.

[35] 17 *U.S. Code* § 512 (c) (1) (A) (iii).

[36] Cfr. 17 *U.S. Code* § 512 (c) (2) «*Designated agent. — The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:*

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory».

regolare notizia o denuncia di presunta violazione[37], deve rapidamente attivarsi per disabilitarne l'accesso o rimuovere il materiale.

Molto simili sono le condizioni in relazione alle quali è ammessa l'esenzione di responsabilità per il collegamento tramite *information location tools*[38] (ovvero *directory, index, reference, pointer, or hypertext link*, etc.) a siti contenenti materiali illeciti. Anche in tal caso, infatti, è essenziale l'assenza dell'*actual knowledge or awareness* e del *financial benefit directly attributable to the activity* (qualora l'intermediario abbia il diritto e la capacità di controllarla), ed è prevista la medesima procedura di *notice and take down*[39].

Con riguardo alle *non-profit educational institutions* che operano nella veste di *providers*, la sezione 512 (e) stabilisce che le stesse non rispondono per le violazioni del *copyright* commesse dagli studenti, dai dipendenti o dallo *staff* di ricerca se l'illecito realizzato non coinvolge la fornitura dell'accesso *on-line* ai materiali didattici che sono stati consigliati o richiesti nell'ultimo triennio e, in questo periodo, l'ente non ha ricevuto più di due *notification*s relative alle volizioni commesse dal soggetto. L'istituzione deve inoltre fornire ai propri utenti materiali informativi che descrivano con precisione e promuovano il rispetto della normativa posta a tutela del *copyright*.

---

[37] Ai sensi del 17 *U.S. Code* § 512 (c) (3) la *notification* può dirsi regolare e quindi fa sorgere *l'actual knowledge or awareness* in capo all'ISP solamente ove sia inviata in forma scritta all'agente designato e rechi la firma di una persona autorizzata ad agire per conto del titolare del diritto esclusivo che si presume violato (che si dichiara tale *«under penalty of perjury»*), l'identificazione del materiale che in buona fede si ritiene immesso in rete senza autorizzazione ed informazioni di contatto. La sezione 512 (f) prevede che in caso di false dichiarazioni il denunciante sarà responsabile per tutti i danni, compresi i costi sostenuti dal denunciato, dal titolare del diritto di *copyright* nonché dall'ISP che in buona fede, confidando nella regolarità e veridicità della *notification*, ha proceduto al *take down* dei contenuti.

[38] 17 *U.S. Code* § 512 (d).

[39] All'art. 17 *U.S. Code* § 512 (d) (3) si precisa che *«the information described in subsection (c) (3) (A) (iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link»*.

In chiusura della sezione 512 viene infine prevista l'esclusione della sussistenza in capo agli ISPs di un obbligo generale di monitorare la rete o ricercare attivamente fatti che rivelino la presenza di materiale illecito *«except to the extent consistent with a standard technical measure complying with the provisions of subsection»*[40].

Il divieto di imporre doveri di controllo sembra pertanto attenuato sulla base dei possibili sviluppi delle misure tecnologiche di protezione cui i fornitori debbono uniformarsi. Se in futuro tali tecnologie permetteranno il monitoraggio senza costi sostanziali sul fornitore, né oneri eccessivi sui suoi sistemi, l'obbligo di sorveglianza potrebbe con esse sorgere.

Elemento precipuo del sistema dei *safe harbours* è la cosiddetta pratica del "*notice and take down*" che vede l'intervento dei *providers* per la rimozione dei contenuti illeciti a seguito delle denunce inviate dagli utenti.

Se da un lato questo approccio permette di coinvolgere gli intermediari nell'attività di monitoraggio e pulizia della rete, dall'altro, come denunciato da recenti indagini, ha ripercussioni dannose sulla libertà di espressione.

I *providers*, infatti, onde evitare controversie ed in virtù dalla completa esclusione di responsabilità in caso del blocco del materiale realizzato in "buona fede", sarebbero inclini a rimuovere o bloccare i *notified content* senza le opportune indagini[41], realizzando così un'opera di censura pur non essendo provvisti dell'autorità di un tribunale o della conoscenza delle specifiche disposizioni giuridiche[42] che regolano il *Digital Dilemma*[43]. Certamente

[40] 17 *U.S. Code* § 512 (i).

[41] Cfr. le interessanti indagini AHLERT C., MARSDEN C., YUNG C., *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation*, in ox.ac.uk, 1 Maggio 2004; URBAN J., QUILTER L., *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act: Summary Report*, 2005, in law.berkeley.edu.

[42] A tal riguardo basti ricordare il principio del *fair use*, previsto nel titolo 17, § 107 del *Copyright Act* che rende le opere protette da *copyright* disponibili al pubblico senza la necessità di autorizzazione, a condizione che tale libero utilizzo sia *«for purposes such as criticism, comment,*

rappresentano viceversa essenziali elementi per scoraggiare opere di censura arbitrarie la disciplina dettagliata prevista per le notifiche, le sanzioni in casi di false accuse, la necessità che l'ISP notifichi al denunciato ogni *takedown notice*, il quale potrà a sua volta inviare una contro notifica per richiedere che il materiale resti disponibile ed infine il "porto sicuro" riconosciuto al fornitore dei servizi che, in attesa della pronuncia della autorità giudiziaria, decida di mantenere le informazioni *on-line* in seguito alla *counter notice*[44].

Per completare il quadro appena tracciato risulta necessario segnalare che nei primi mesi del 2015 la *Federal Communications Commission* (FCC)[45] ha

---

news reporting, teaching (including multiple copies for classroom use), scholarship, or research». La finalità di questa eccezione al diritto di *copyright* è quella di incentivare *«the progress of science and useful arts»,* così come sancito nella Costituzione (*Article I, Section 8*). In Italia sembrerebbe assimilabile al *fair use* la disposizione approvata nel 2007 e codificata al comma 1 *bis* dell'art. 70 della Legge sul diritto d'autore, secondo cui: «È consentita la libera pubblicazione attraverso la rete internet, a titolo gratuito, di immagini e musiche a bassa risoluzione o degradate, per uso didattico o scientifico e solo nel caso in cui tale utilizzo non sia a scopo di lucro. Con decreto del Ministro per i beni e le attività culturali, sentiti il Ministro della pubblica istruzione e il Ministro dell'università e della ricerca, previo parere delle Commissioni parlamentari competenti, sono definiti i limiti all'uso didattico o scientifico di cui al presente comma». Cfr. voce *Fair Use* in wikipedia.org. In giurisprudenza cfr. sul punto il famoso caso *"Dancing Baby"*, pendente dal 7 luglio 2015 dinnanzi alla Corte d'Appello della California, *Lenz v.Universal Music Group Inc. et al*, 5:07-cv-03783, in eff.org/document/9th-circuit-opinion-lenz.

[43] Viene definito in tali termini il problematico bilanciamento in rete tra interesse pubblico alla diffusione dei materiali e il diritto del titolare del *copyright*. V. *Committee on Intellectual Property Rights and the Emerging Information Infrastructure*, *The Digital Dilemma: Intellectual Property in the Information Age*, Washington, 2000, anche *on-line* in nap.edu.

[44] Cfr. EDWARDS L., *Role and responsibility of internet intermediaries in the field of copyright and related rights*, cit., p. 12 ss., anche con riguardo ai sistemi alternativi rispetto alla procedura di *notice and take down*.

[45] La FFC è un'agenzia governativa creata con il Communications Act del 1934, incaricata di tutti gli usi dello spettro radio (incluse trasmissioni radio e televisive), e tutte le telecomunicazioni interstatali (via cavo, telefoniche e satellitari) e le comunicazioni internazionali che provengono e sono destinate agli Stati Uniti. È un tassello chiave della politica americana delle telecomunicazioni ed ha il compito di tracciare le linee guida che l'industria delle

approvato definitivamente la riclassificazione degli ISPs come *carrier* telefonici tradizionali[46]. Si tratta di un essenziale passo nella lotta per la difesa del diritto alla libertà di espressione, degli interessi dei consumatori e dell'evoluzione tecnologica.

La riqualificazione non ha un valore puramente formale, ma incide in modo profondo sulla regolamentazione dell'attività dei *providers* che si trovano in tal modo, come *utility* pubbliche, soggette al Titolo II del *Communication Act* concernente i *common carriers.*

Tramite questa misura si ancorano le problematiche relative all'ISP ad una base normativa che vieta il blocco dei pacchetti di dati, il *throttling*[47] della banda di rete e l'accesso a pagamento alle *"fast lane"* ad alte prestazioni e si garantisce alla FCC poteri di valutazione sulle possibili violazioni del diritto dei consumatori al cd. *Open Internet*[48].

2. *GESETZ ZUR REGELUNG DER RAHMENBEDINGUNGEN FÜR INFORMATIONS-UND KOMMUNIKATIONSDIENSTE* (IUKDG) E *TELEMEDIENGESETZ* (TMG)

La Germania rappresenta la nazione che per prima, nel panorama europeo, si è dotata di una disciplina organica concernente espressamente la responsabilità degli operatori di Internet. Già agli inizi degli anni novanta, dottrina e

---

telecomunicazioni è chiamata a seguire onde garantire la neutralità della rete. Cfr. voce *Net neutrality in the United States* e voce *Federal Communications Commission* in en.wikipedia.org.

[46] Cfr. *News*: *FCC Adopts Strong, Sustainable Rules to Protect the Open Internet*, in fcc.gov, 26 Febbraio 2015.

[47] Il *throttling* è il rallentamento intenzionale di servizi Internet da parte del *provider.* Pur avendo la potenziale funzione positiva di evitare congestioni della rete ove le richieste superino le capacità dei *server*, tale forma di limitazione intacca la neutralità della rete, ovvero il principio guida che conserva Internet libero e aperto, in virtù del quale i fornitori di servizi non possono discriminare tra i diversi tipi di contenuti e applicazioni *on-line* privilegiandone alcuni. V. voce *Bandwidth throttling* in en.wikipedia.org.

[48] Cfr. MARUCCIA A., *Net neutrality USA, le nuove regole*, in punto-informatico.it, 27 Febbraio 2015.

giurisprudenza, consapevoli dei cambiamenti epocali legati all'utilizzo delle nuovo tecnologie ed alla diffusione di Internet, si sono interrogate circa la necessità di individuare criteri attraverso i quali evitare un estensione incontrollata della responsabilità dei *providers*[49].

Il primo passo verso la regolamentazione specifica della rete Internet risale al 1996 con la pubblicazione del *Report Info 2000: Deutschland's Weg in die Informationsgesellschaft* (*Info 2000: Germany's Way into the Information Society*)[50] che ha preparato la promulgazione della legge quadro sui servizi d'informazione e di comunicazione *Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste* (IuKDG)[51], in vigore dal 1° agosto

[49] Cfr. SIEBER U., *The international emergence of Criminal Information Law*, Köln, 1992; SIEBER U., *Information technology crime*, Köln, Berlin, Bonn, München, 1994. In riferimento ai primi interventi in materi di criminalità informatica cfr. PICOTTI L., *Studi di diritto penale dell'informatica*, Verona, 1992, p. 33 ss.

Ricordiamo inoltre come la prima inchiesta penale avviata nel 1995 da un *prosecutor* tedesco a carico di un *provider* abbia acceso il dibattito sulla tematica della responsabilità a livello internazionale: si tratta del famoso caso che ha visto il direttore della ditta *CompuServe GmbH* indagato per concorso in diffusione di materiale pedopornografico, avendo permesso agli utenti tedeschi di accedere, tramite i propri *server*, ai computer della società madre americana (*CompuServe Inc*.), ospitante in *newsgroup* e *news-server* il materiale illecito. Cfr. *AG* München, sentenza 28 maggio 1998, in lingua inglese in kuner.com, con cui il direttore è stato condannato a due anni di pena detentiva e la successiva sentenza in appello LG München, sentenza 17 novembre 1999, 20 Ns 465 Js 173158/95, in netlaw.de, con cui la Corte ne dichiara la non colpevolezza in accordo con quanto espresso da autorevole dottrina, per tutti v. SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer. Le nuove sfide di internet*, trad. it. a cura di Sforzi, in *Rivista trimestrale di diritto penale dell'economia*, 1997, p. 743 ss. – p. 1193 ss.

[50] *Bundesministerium für Wirtschaf* (BMWi), febbraio 1996, Info2000 in *bmwi*.de.

[51] Legge federale IuKDG cd. *"Multimedia Law"*, testo in lingua inglese *in* kuner.com. Per un commento in lingua italiana alle disposizioni normative in tema di responsabilità penale dei *providers* contenute nella legge quadro (IuKDG) e nella relativa legge sui servizi telematici (TDG) cfr. SEMINARA S., *La responsabilità penale degli operatori su Internet*, in *Diritto dell'Informazione e dell'Informatica*, 1998, p. 759 ss.; PICOTTI L., *Fondamento e limiti della responsabilità penale dei Service Providers*, in *Diritto Penale e Processo*, n. 31/1999, p. 379 ss. (in particolare nota 26 per i riferimenti ai contributi della dottrina tedesca sul punto). In lingua

1997. Lo IuKDG ha istituito una legge sui servizi telematici (TDG) tra i quali sono stati anche inclusi *«Angebote zur Nutzung des Internets oder weiterer Netze»* ovvero i servizi di accesso a Internet o altre reti[52].

In accordo con i principi sanciti successivamente a livello europeo tramite la Direttiva 2000/31/CE, il § 5 TDG[53] ha escluso la sussistenza di un generale dovere di controllo in capo ai *services providers*, definiti nel § 3 TDG come «persone fisiche o giuridiche o gruppi di persone che rendono disponibili teleservizi propri o di terzi ovvero che forniscono l'accesso ad essi», mentre ha tracciato innanzitutto una loro responsabilità, secondo le leggi generali, con riferimento ai "propri materiali".

In dottrina il concetto di "proprietà" è stato inteso, sin dall'origine, come "diretta riconducibilità al *provider*" sussistente qualora il fornitore sia autore del materiale ovvero se ne appropri non indicandone la paternità o ancora «laddove eserciti un controllo preventivo di congruità e/o liceità sui materiali da rendere accessibili, come responsabile della loro immissione in rete»[54]. In modo particolare la responsabilità legata ai "propri contenuti" è strettamente connessa

---

inglese cfr. KOOPS B., PRINCE C., HIJAMANS H, *ICT Law and Internationalisation: A Survey of Government Views*, The Hague, 2000.

[52] § 2, n. 3TDG.

[53] § 5 TDG: *Verantwortlichkeit (1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich. (2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. (3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung. (4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.*

[54] Cfr. SEMINARA S., *La responsabilità penale degli operatori su Internet*, cit., p. 761 ss. I primi commentatori della legge hanno messo bene in luce come il requisito della "proprietà" dei contenuti susciti numerose problematiche nel caso dell'utilizzo dei cd. *link* (richiamo degli autori tedeschi che per primi si sono occupati della questione in SEMINARA S., op. cit., nota 21).

allo scopo della messa a disposizione per l'utilizzo da parte degli utenti. L'espressione *zur Nutzung* ha segnato pertanto una netta distinzione tra dati rilevanti e non, ed ha identificato il momento consumativo del reato con la "messa a disposizione" del materiale, indipendente dal successivo utilizzo[55].

In relazione ai "contenuti altrui tenuti a disposizione per l'utilizzo", invece, il § 5 TDG ha subordinato la configurabilità della responsabilità dei *providers* alla "conoscenza" nonché alla "possibilità tecnica" ed "esigibilità" di un intervento volto ad impedire la diffusione del materiale[56]. La responsabilità in tal caso è stata quindi strutturata come un "mancato impedimento" delimitato in virtù del ben noto problema tecnico del controllo e dei relativi costi.

Per evitare che gli operatori della rete fossero soggetti ad obblighi sproporzionati perlopiù pericolosi per la libera circolazione delle idee, il legislatore tedesco ha fatto ricorso alle clausole della possibilità tecnica e dell'esigibilità, interpretate, dalla dottrina maggioritaria, avendo a riferimento in modo particolare il profilo della tutela dei contenuti leciti e l'efficacia delle misure adottate[57].

---

[55] Cfr. PICOTTI L., *Fondamento e limiti della responsabilità penale dei Service Providers*, cit., p. 384 ss.

[56] In tal senso cfr. BGH, decreto di archiviazione 13 febbraio 1998, in uni-sb.de, in cui si afferma che la legge in esame non ha mutato nulla ovvero, esplicitando i generali principi penalistici, richiede che «nel momento in cui i *providers* consentono l'accesso alla rete, essi devono essere considerati come destinatari di determinati doveri per la sicurezza del traffico. Un concreto obbligo di agire è ipotizzabile solo quando l'agente sia consapevole delle circostanze che determinano l'insorgere di tale obbligo ed egli abbia la possibilità di impedire la verificazione dell'evento attraverso una condotta esigibile: così mentre un dovere di controllo non risulterebbe ne' possibile ne' esigibile, l'obbligo di impedire l'accesso ai materiali illeciti sussiste quando il *provider* abbia conoscenza che determinati contenuti punibili sono disponibili in rete».

[57] Cfr. FORNASARI G., *Il ruolo della esigibilità nella definizione della responsabilità penale del Provider*, p. 423 ss., in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004. In modo particolare l'autore sostiene che le clausole delimitative in esame costituirebbero la "cattiva" trasposizione a livello legislativo della Dichiarazione finale della Conferenza ministeriale europea di Bonn dell'8 luglio 1997, la quale raccomanda che i *providers* non siano soggetti a regole irragionevoli, sproporzionate e discriminatorie.

E' stato infine escluso dall'area della responsabilità per il materiale dei terzi, l'*access provider*, in quanto fornitore di mero accesso alla rete al pari degli operatori telefonici, e il *proxy-cache server*, che si limita a memorizzare i materiali altrui a richiesta degli utenti in modo automatico e per una breve durata.

Si tratta quindi di un sistema di responsabilità in linea con le soluzioni dogmatiche sviluppatesi in dottrina con riferimento agli operatori dei tradizionali mezzi di comunicazione (stampa, radio, tv, posta e telefono).

L'antesignano Prof. Sieber, prima dell'approvazione dello IuKDG, riguardo alla trasmissione di dati illeciti in Internet, concludeva, dopo un'analisi del sistema vigente, per una piena responsabilità penale del *provider* in relazione ai propri contenuti; per una sua circoscritta responsabilità qualora influisse sulla composizione contenutistica dei dati offerti; per l'esclusione della responsabilità nel caso di mero sostegno tecnico alla trasmissione di dati altrui e per la necessità che, nella misura in cui fossero riconosciuti doveri di controllo e di sorveglianza, agli stessi venisse data un'interpretazione restrittiva in virtù dei principi di fattibilità ed esigibilità tecnico-economica, valorizzando sul piano della esigibilità elementi quali la pericolosità dei dati in questione[58].

Attualmente la normativa inerente alla responsabilità degli ISPs è inserita nel "*Telemediengesetz*" (TMG)[59], entrato in vigore il 1° marzo 2007, che ha comportato l'abrogazione del *Teledienstegesetz* e della *Teledienstedatenschutzegesetz* (*Teleservice Data Protection Law*) ed implementato la direttiva europea sull'*e-Commerce* 2000/31/CE. Il TMG offre

[58] Cfr. SIEBER U, *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di internet*, cit., p. 782-783.

[59] Cd. "*Telemedia Act*", english version in cgerli.org. Per un commento alla legge cfr. DÖRR D., JANICH S., *The criminal responsibility of Internet Service Providers in Germany*, in *Mississippi Law Journal*; v. 80, n. 4, 2011, p. 1247 ss.; HOEREN T., *Liability for Online Services in Germany*, in *German Law Journal*, v. 10, n. 5, 2009, p. 561 ss.; NAGEL D., *I fornitori di servizi internet in Germania tra forme di responsabilità e doveri di collaborazione*, in LUPARIA L. (a cura di), *Internet provider e giustizia penale*, *Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, p. 232 ss.

una regolamentazione della responsabilità "orizzontale" ed ha permesso il superamento della distinzione tra *teleservices* (la cui disciplina era contenuta nel TDG) e *mediaservices* (oggetto del MDStV).

Il TMG si applica alle informazioni elettroniche e ai servizi di comunicazione reperibili in Internet[60] e, nel delineare i profili di responsabilità dei fornitori di tali servizi ne da una classificazione[61].

Il § 7 TMG riguarda i fornitori di servizi che mantengono le proprie informazioni pronte per l'uso; mentre il § 8 TMG gli intermediari che trasferiscono contenuti di terzi o organizzano l'accesso al loro uso, anche se per far ciò li memorizzino in modo automatico, intermedio e transitorio, per un periodo non più lungo di quello che ragionevolmente necessita la trasmissione. Un sottoinsieme di questa categoria di *provider* è rappresentato da quelli che - secondo il § 9 TMG- automaticamente memorizzano temporaneamente le informazioni di terzi al fine di renderne il trasferimento più efficiente (cd. *provider proxy-cache*, fornitore di stoccaggio intermedio volto all'accelerazione

---

[60] TMG, *Abschnitt 1 Allgemeine Bestimmungen § 1 Anwendungsbereich «(1) Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). Dies*es *Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird».*

Il TMG riprende la definizione di *service provider* già espresso nel IuKDG. La qualità essenziale che contraddistingue il *provider* è pertanto quella di permettere l'uso dei mezzi telematici, rendendoli disponibili o fornendone l'accesso. Le sezioni inerenti alla responsabilità del TMG ricalcano le sezioni 8-11 TDG e le sezioni 6-9 MDStv.

[61] Come nella precedente normativa i profili di responsabilità sono essenzialmente legati alla funzione svolta dall'operatore. D'altra parte, come evidenziato in dottrina, è «necessario chiedersi quali funzioni la persona interessata svolga all'interno della rete e quali servizi egli offra ai suoi utenti. Solo una tale analisi di funzioni può rappresentare il punto di partenza per formulare ed esprimere una valutazione giuridica in termini corretti» cfr. SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer. Le nuove sfide di internet*, cit., p. 758 ss.

della trasmissione di contenuti consultati frequentemente). Infine il § 10 TMG concerne i fornitori di servizi che salvano informazioni di terzi per l'utente.

E' possibile pertanto distinguere tra *content provider*, *access provider*, *proxy-cache provider* e *host provider*, sulla scorta delle modalità attraverso le quali vengono offerti i diversi servizi.

Come la precedente normativa del TDG, il TMG non contiene una regolamentazione autonoma della responsabilità dei *providers*, ne' distingue tra profili penalistici, civilistici o di diritto pubblico, ma costituisce una sorta di filtro[62] per la successiva applicazione delle normative specifiche.

In relazione ai propri contenuti il TMG prevede che *«Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich»*[63]: ovvero i *providers* che creano e offrono le proprie informazioni agli utenti sono pienamente responsabili delle stesse ai sensi della normativa generale[64].

La disposizione in esame ha sollevato numerosi interrogativi circa la linea di demarcazione tra contenuti propri e altrui[65]. Come suggerito in dottrina il titolare

[62] Cfr. BGH, sentenza del 23 settembre 2003, VI ZR 335/02, in lexetius.com; commento HOEREN T., in MMR 3/2004, p. 168-169. La normativa in dottrina e giurisprudenza è stata interpretata, già nella sua precedente versione, nel senso che il controllo del soddisfacimento dei requisiti in essa stabiliti deve essere realizzato in una fase precedente e propedeutica all'esame della normativa di riferimento. Cfr. inoltre *Deutscher Bundestag Drucksache* 14/6098, p. 23, in bundestag.de.

[63] § 7 TMG.

[64] I *content providers*, quindi, sia per i propri contenuti sia per quelli dei terzi trattati come fossero propri, potranno godere della protezione di cui all'art 5 della *Grungesetz* (Costituzione Tedesca), che tutela la libertà di espressione e di diffusione del proprio pensiero, libertà di stampa e cronaca, specificando che «tali diritti trovano limite nella normative generale, nelle norme a protezione dei minori, e nel diritto all'onore personale», nonché, per i profili penalistici, nella scriminante dell'esercizio di una facoltà legittima *ex* §193 StGB.

[65] In modo particolare è ancora molto dibattuta la configurabilità della responsabilità per le informazioni cui il *content provider* rinvia tramite *link*. Durante la vigenza del TDG, con sentenza del 12 maggio 1998, 312 O 85/98, in netlaw.de, il Landgericht di Amburgo ha sancito che con

dell'*homepage* in Internet, affinché sia chiara la distinzione tra le proprie informazioni e quelle dei terzi e di conseguenza non possa essere chiamato a rispondere di quest'ultime, dovrebbe servirsi di avvisi di questo tipo: "*Stai per uscire dal nostro sito. Non ci assumiamo alcuna responsabilità per il contenuto del sito seguente"*[66]. L'assenza di *warning* simili potrebbe implicare che i contenuti pubblicati dai terzi siano trattati dal *provider* "come se fossero propri" e da qui discenderebbe la responsabilità per gli stessi[67].

---

l'inserimento di un *link* si partecipa all'eventuale responsabilità per i contenuti del sito collegato a meno che si prendano espressamente le distanze da essi. Tale affermazione è stata richiamata e confermata anche nella più recente sentenza BGH del 7 ottobre 2009, I ZR 109/06, in lexetius.com.

[66] Numerosi i *content providers* tedeschi che hanno inserito nelle proprie *homepage* avvisi di tale tenore: *"Haftungshinweis: Die Inhalte meiner Seiten wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte kann ich jedoch keine Gewähr übernehmen. Als Dienstanbieter bin ich gemäß § 7 Abs.1 TMG für eigene Inhalte auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich. Nach §§ 8 bis 10 TMG bin ich als Dienstanbietern jedoch nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werde ich diese Inhalte umgehend entfernen. Mein Angebot enthält Links zu externen Webseiten Dritter, auf deren Inhalte ich keinen Einfluss habe. Deshalb kann ich für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werde ich derartige Links umgehend entfernen".* Si avvisa quindi il lettore che il *provider* non è responsabile per i contenuti cui rinvia tramite *link*, ma solo per i propri contenuti e, in relazione a questi, si impegna alla rimozione nel momento in cui sia edotto della natura loro illecita.

[67] Cfr. HOEREN T., *Liability for Online Services in Germany*, cit., p. 562 ss.

In realtà, questa impostazione, che trae origine dalle disposizioni concernenti la stampa, non sembra accettabile o per lo meno non nella totalità dei casi[68]. Dichiarazioni simili a quelle menzionate potrebbero avere un rilievo, ad esempio con riguardo ai reati di diffamazione e ingiuria, ma non giustificherebbero un'esclusione della responsabilità in materia di pedo-pornografia o violazione del *copyright*[69].

Anche in giurisprudenza è stato più volte chiarito come, onde stabilire se un'informazione pubblicata da terzi per il tramite del *provider* possa essere assimilata alle informazioni prodotte da quest'ultimo, è necessaria la valutazione obiettiva delle circostanze specifiche del caso concreto[70]. In modo particolare secondo le indicazioni *Bundesgerichtshof* (BGH), anche quando gli utenti siano in grado di identificare il soggetto resosi autore delle informazioni, le stesse possono essere considerate del *provider* se quest'ultimo ne controlla il contenuto quanto alla completezza e correttezza, svolgendo un'attività simile all'editore. Questa situazione si verificherebbe ad esempio nel caso in cui il fornitore di servizi agisca

[68] Così DÖRR D., JANICH S., *The criminal responsibility of Internet Service Providers in Germany*, cit., p. 1254 ss.

[69] Con riguardo al *Copyright Act* - UrhG, cfr. FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, cit., p. 373 ss., in particolare nota 15 per i riferimenti ai contributi della dottrina tedesca.

[70] Cfr. ad esempio, LG Düsseldorf, sentenza 14 agosto 2002, 2a O 312/01, in jurpc.de, con cui la Corte afferma che, in relazione al caso specifico della gestione di un *guestbook* di lettere di diffida, il *provider* ha l'obbligo di controllare la non diffamatorietà dei post pubblicati proprio perché, per le caratteristiche particolari dello stesso *guestbook, «er damit rechnen muss»*. Egli, cioè, deve aspettarsi che i contenuti siano diffamatori. Pertanto, in assenza di controllo è come se il *provider* accettasse il contenuto dei *post* facendoli propri. V. inoltre LG Amburgo, sentenza 3 settembre 2010, 308 O 27/09, in rechtsprechung-hamburg.de, con riferimento al fatto che i contenuti in caso di anonimato devono essere considerati come fossero del *provider*. Cfr. poi KG Berlin, sentenza 10 luglio 2009, 9 W 119/08, in berlin-brandenburg.de, nella quale si afferma che i criteri chiave per comprendere quando i contenuti sono trattati dal *provider* come se fossero propri sono: il tipo di acquisizione dei dati, il loro scopo e la presentazione effettiva degli stessi. Per la Corte la valutazione dovrebbe per l'appunto confrontarsi con il quadro complessivo delle circostanze dal punto di vista di un osservatore oggettivo.

quale "moderatore" nell'ambito di *newsgroup* o di *mailing-lists*[71]. Altro indizio della volontà dell'ISP di "far proprie" le informazioni altrui sarebbe infine rintracciabile nella concessione a suo favore dei relativi diritti d'uso[72].

In relazione ai contenuti altrui, invece, la disciplina distingue il regime applicabile agli *access providers* e *proxy-cache providers* da quello previsto per gli *hosting providers*.

In riferimento ai primi, come precedentemente fissato nel § 5 TDG, *«Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich»*[73]. In particolare, conformemente alla disposizione di cui all'art. 12 della direttiva europea 2000/31/CE di seguito illustrata, i *providers* che si limitano a mere attività di trasferimento di informazioni di terzi soggetti ovvero di accesso, non sono responsabili a condizione che essi «1. non abbiano dato inizio alla trasmissione 2. non abbiano selezionato il destinatario della trasmissione 3. non abbiano selezionato o modificato l'informazione trasmessa».

Per i cd. *proxy-cache providers*, invece, l'attività di «automatica, intermedia e temporanea conservazione dei contenuti» non costituisce fonte di responsabilità qualora gli stessi «1. non modifichino l'informazione trasmessa 2. rispettino le condizioni d'accesso alle rispettive informazioni 3. rispettino le regole sull'aggiornamento delle informazioni specificate dagli standard d'uso del settore 4. non interferiscano con l'utilizzo lecito della tecnologia per la raccolta, secondo le regole di settore, dei dati sull'impiego delle informazioni 5. nel momento in cui vengano a conoscenza del fatto che le informazioni alla fonte iniziale della trasmissione sono state rimosse dalla rete o che l'accesso ad esse è stato disabilitata, oppure che un organo giurisdizionale o un'autorità amministrativa ne

---

[71] Cfr. SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer. Le nuove sfide di internet*, cit., p. 752 ss.

[72] Cfr. BGH, sentenza 12 novembre 2009, I ZR 166/2007, in lexetius.com.

[73] § 8 TMG.

ha disposto il ritiro o l'inaccessibilità, agiscano immediatamente per rimuovere o disabilitare l'accesso alle informazioni che sono memorizzate ai sensi della presente disposizione». I *proxy-cache providers* quindi devono rispettare le procedure fissate dal legislatore onde garantire la perfetta conformità della copia offerta agli utenti a quella originale. Per tale motivo non solo dovranno riproporre le modalità di accesso fissate dal sito originale ma anche svolgere periodici aggiornamenti ed eliminare le informazione che sono state rimosse, bloccate o di cui è stato disposta la rimozione/blocco da parte dell'autorità giudiziaria-amministrativa, per impedire che tale materiale continui ad essere usufruibile nonostante le misure disposte nei confronti dell'*origin source*.

In entrambe i casi l'esenzione dalla responsabilità non può essere applicata qualora il *provider* volutamente *absichtlich zusammenarbeite* al destinatario del proprio servizio per commettere illeciti.

La *ratio* dell'ampia esclusione della responsabilità soprariportata è strettamente connessa alla necessità di non gravare chi si occupa di operazioni di mero supporto tecnico alla trasmissione dati di obblighi di controllo difficilmente attuabili, sia dal punto di vista economico che tecnico, e dalla dubbia efficacia. La situazione presenterebbe numerose analogie con il tradizionale servizio postale[74].

D'altro canto la disciplina in esame risulta pienamente in linea con le esigenze di sviluppo della società dell'informazione che necessita per l'appunto che questi fornitori di servizi non siano ostacolati nelle loro attività da obblighi eccessivi[75].

L'*access provider* e il *proxy-cache provider* non sono responsabili nemmeno quando siano a conoscenza dell'illeceità delle informazioni trasmesse. La condizione della *"Kenntnis von der rechtswidrigen Handlung oder der Information"*, quale fondamneto dell'eventiuale responsabilità, infatti, è stata fissata dal legislatore solamente in relazione agli *hosting providers*.

Ha suscitato però un acceso dibattito l'attenuazione dell'assenza di responsabilità per i contenuti forniti dai terzi prevista, sia nel caso di semplice

[74] Cfr. SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer. Le nuove sfide di internet*, cit., p. 768 ss.

[75] Cfr. *Deutscher Bundestag Drucksache* 14/6098, p. 24, in bundestag.de.

accesso sia per l'attività di *caching*, nella seconda parte del § 7 TMG, in virtù del quale, sebbene gli *access* e *proxy-cache providers* non siano chiamati a monitorare le informazioni trasmesse o a ricercare circostanze dalle quali si possa evincere la perpetrazione di attività illecite[76], resta fermo l'obbligo di rimuovere nonché di impedire l'accesso a contenuti secondo la normativa generale. La disposizione ha suscitato la critica della dottrina più sensibile, poiché non riproducendo la formula concernente la esigibilità e possibilità tecnica della

[76] Cfr. LG Köln, sentenza 31 agosto 2011, Az. 28 O 362/10, in telemedicus.info. La Corte, in relazione alla tematica del cd. *file-sharing*, ha sancito che è irragionevole imporre al fornitore di accesso l'adozione di filtri nonchè contrario alla legislazione vigente e alla tutela della segretezza delle telecomunicazioni. La Corte inoltre ha puntualizzato che *«Art. 8 Abs. 3 der Richtlinie 2001/29/EG erlaubt im Wege richtlinienkonformer Auslegung nationaler Verbotsvorschriften kein Vorgehen von Rechteinhabern gegen „Vermittler" im Wege gerichtlicher Anordnungen, wenn in den zugrunde liegenden nationalen Rechtsvorschriften keine ausreichende Rechtsgrundlage für ein solches Vorgehen enthalten ist»*. L'ordine del Tribunale, cioè, non può costituire la base giuridica per imporre meccanismi di filtraggio.

chiusura presente nel TDG[77], potrebbe fungere quale *escamotage*, per introdurre via *"back door"* un'indefinita responsabilità degli *access providers*[78].

Secondo quanto disposto dal § 10 TMG gli *hosting providers*, sono responsabili delle informazioni che "ospitano" a condizione che essi abbiano conoscenza della loro illeceità e che, nel caso di richieste di risarcimento danni, siano emersi fatti o circostanze in virtù dei quali l'illiceità sia evidente ovvero non abbiano agito prontamente al fine di rimuovere le informazioni o disabilitarne l'accesso, una volta ottenuta tale conoscenza.

La "conoscenza", come specificato in giurisprudenza, concerne l'illeceità del contenuto[79] e deve essere effettiva. Onde evitare un ampliamento eccessivo della sfera di punibilità, essa viene ristretta ai soli casi di dolo intenzionale o diretto[80].

---

[77] La giurisprudenza sembra comunque dar rilievo al principio "*ad impossibilia nemo tenetur"*, consapevole della difficoltà di attuare misure di blocco di tale sorta e della loro scarsa efficacia. Cfr. la recente OLG Hamburg, sentenza 21 novembre 2013, 5 U 68/10, in jurpc.de, nella quale si pone in luce innanzitutto l'inutilità di misure di blocco, data la facilità e rapidità delle tecniche utilizzabili per il loro aggiramento. La Corte, inoltre, mostra come, pur ammettendo l'efficacia di alcune misure di blocco, le stesse risultino inammissibili in quanto sarebbe inevitabile impedire la disponibilità anche di contenuti legittimi, con violazione dei principi fondamentali fissati nella Carta Costituzionale. Di rilievo il principio stabilito al riguardo nella sentenza del BGH del 12 maggio 2010, I ZR 121/08, in openjur.de, in virtù della quale anche i proprietari di accesso privato WLAN hanno l'obbligo di esaminare se la loro connessione *wireless* è protetta attraverso adeguate misure di sicurezza contro il rischio di essere utilizzate da terzi non autorizzati per commettere violazione del *copyright*. Ovviamente, secondo il principio "*ad impossibilia nemo tenetur"*, l'operatore privato non sarà chiamato ad adattarsi continuamente, con relativo dispendio di risorse finanziare, alle più recenti tecnologie inerenti la sicurezza della rete. L'obbligo di verifica, dunque, sarebbe rapportato al momento dell'installazione del *router*. In materia, per un'analisi completa in chiave comparatistica, cfr. CODIGLIONE G. G., *Indirizzo IP, reti Wi-Fi e responsabilità per illeciti commessi da terzi*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2013, p. 107 ss.

[78] Cfr. HOEREN T., *Liability for Online Services in Germany,* cit., p. 565 ss.

[79] Cfr. *ex multis* OLG Düsseldorf, sentenza 7 giugno 2006, I 15 U 21/06, in LawCommunity.de, nella quale la Corte afferma i seguenti principi fodamentali: *1.Der Betreiber eines Internetforums ist verpflichtet, ihm bekannt gewordene Beiträge rechtsverletzender Art unverzüglich zu löschen; 2. Die Verpflichtung des Forumsbetreibers, ehrverletzende Inhalte zu löschen, entsteht erst mit der Kenntnisnahme von diesen Äußerungen.* Non sussiste in capo al

Pertanto l'apertura di un'indagine penale nei confronti del direttore di un *provider* richiede, innanzitutto, che egli stesso sia consapevole dell'illecita dei dati, non essendo sufficiente che lo sia ad esempio un impiegato della ditta, ed in secondo luogo che sia ben chiara la loro collocazione delle informazioni illecite[81].

---

provider, pertanto, alcun obbligo di sorveglianza o di ricerca in merito ai contenuti diffamatori e, solamente nel momento in cui sia edotto della natura illecita degli stessi, sorgerà l'obbligo di rimuoverli. V. inoltre ULYS*, Study on the Liability of Internet Intermediaries, Country Report - Germany*, in europa.eu, 12 novembre 2007, p. 3: *«According to the German Federal Court of Justice ("Schöner Wetten") the liability exemptions of the TMG are not applicable to hyperlinks. Following this decision lower courts have held that the liability exemptions equally do not apply to search engine operators. As regards the extent of the obligations to examine that rest on a person who places or perpetuates a hyperlink, the Federal Court of Justice in "Schöner Wetten" held that such obligations were subject to various factors like the knowledge of the person setting up the hyperlink, the circumstances indicating that the website serves unlawful purposes and the opportunities available to the person who sets up a hyperlink to reasonably notice the illegality of this activity. Where a hyperlink only facilitates access to generally accessible sources, the principles of constitutional freedom of speech and freedom of the press require the court to limit the obligations to examine. In another case a Higher Regional Court found that the hyperlink in question (at least) facilitated location of a website where a software producer had advertised software designed to crack copy protection. By setting up a hyperlink the defendant had knowingly and causally contributed to copyright infringements committed by the software producer».* Sembrerebbe quindi che, quando il collegamento ipertestuale offerto dall'ISP facilita il raggiungimento del sito in cui è possibile utilizzare programmi per scaricare materiale in violazione del *copyright*, il *provider* contribuisca consapevolmente e causalmente all'attività illecita commessa dal produttore del *software* per il *download*.

Per un'analisi completa delle responsabilità dei fornitori di *hosting* anche in relazione ai *link* v. BGH, sentenza 12 luglio 2012, I ZR 18/2011, testo in lingua inglese in anti-piracy.nl.

[80] Cfr. *ex multis* BGH, sentenza 23 settembre 2003, VI ZR 335/02; OLG Düsseldorf, sentenza 26 febbraio 2004, I 20 U 204/02. V. inoltre ULYS*, Study on the Liability of Internet Intermediaries*, cit., p.2: *«According to German courts, knowledge in terms of § 10 TMG is actual, positive human knowledge, but not negligent ignorance or contingent intent (dolus eventualis). Only in very extreme cases may "knowledge" be interpreted as "turning a blind eye to the illegal action or information". The courts have so far rejected any such wider interpretation. Furthermore § 10 TMG provides for the liability of host providers to pay damages in cases of deliberate and gross negligence, which can be assumed only in cases of "obvious" illegality».*

[81] Cfr. OLG Hamburg, sentenza 2 marzo 2010, Az 7 U 70/09, in telemedicus.info.

Con riferimento alle cause civili di risarcimento danno, l'effettività della conoscenza sussiste, oltre che nel caso di esplicito provvedimento dell'autorità giudiziaria competente, qualora l'illeceità sia così evidente da essere riconoscibile dall'uomo medio, senza la necessità di particolari indagini in fatto od in diritto[82].

Oltre ad essere un requisito di difficile interpretazione, l'effettiva conoscenza, come denunciato da parte della dottrina e della giurisprudenza, potrebbe in realtà innescare un circolo vizioso di disincentivazione di qualsiasi tipologia di controllo dei contenuti ospitati, premiando il *provider* totalmente incurante. Per questo le Corti tedesche, nonostante il divieto espresso di un obbligo generale di controllo, hanno talvolta imposto meccanismi di filtraggio *ex* § 7, comma 2, TMG, per evitare la perpetrazione di condotte della cui illeceità si può presumere la conoscenza da parte del *provider* in virtù dell'affinità con casi già trattati o della particolarità del settore[83].

Per quanto riguarda infine la cd. *"notice and take down"*, il legislatore tedesco non ha specificato alcun requisito in merito alla *notification*. Nonostante tale lettura le Corti hanno fissato uno *standard* minimo per valutare se ed in relazione a quali denunce sorga l'obbligo in capo ai *providers* di attivarsi per bloccare il materiale, identificato in termini molto simili a quello previsto nel DMCA. In modo particolare, in un caso attinente a violazioni del *copyright*, è stato specificato ad esempio che la denuncia dell'utente deve contenere indicazioni precise che permettano al *provider* di identificare i contenuti illeciti,

[82] Cfr. BGH, sentenza 25 ottobre 2011, VI ZR 93/10, in openjur.de.

[83] Ad esempio, nel caso di *upload* e *download* di *file* musicali, cfr. LG München, sentenza 30 marzo 2000, I 7 O 3625/98, confermata in appello l'anno successivo, entrambe in www.dejure.org. La Corte, nella sentenza in questione, afferma che se il *provider* offre la possibilità di scambiare canzoni della categoria *"pop"*, la consapevolezza dell'illegittimità per violazione del *copyright* può essere presunta giacché la protezione da esso offerta non scade fino a settanta anni dopo la morte dell'autore. Cfr. inoltre OLG Düsseldorf, sentenza 24 febbraio 2009, I 20 U 204/02, con cui la Corte, specifica che, una volta venuto a conoscenza dell'illecita dei contenuti, il *provider*, non solo deve bloccare la specifica offerta immediatamente (il caso riguardava la piattaforma *e-bay*), ma anche prendere precauzioni per garantire che non ci saranno, per quanto possibile, ulteriori violazione simili. Sebbene non si parli di obbligo generale di esaminare le offerte prima della pubblicazione su Internet, questi sistemi di filtraggio, sembrerebbero violare il divieto di cui dell'art. 15 della direttiva *e-Commerce*.

nonché allegare documenti attestanti il diritto d'autore che si ritiene violato e la richiesta di bloccare o cessare l'attività illecita[84].

3. LA DIRETTIVA EUROPEA SUL COMMERCIO ELETTRONICO

In Europa, come anticipato, si è optato per un regime di responsabilità "orizzontale" che si applica agli illeciti civili e penali ed abbraccia la totalità dei contenuti.

Hanno rappresentato tappe fondamentali per la successiva elaborazione della Direttiva *e-Commerce* l'adozione da parte della Commissione Europea del Libro Verde sulla protezione dei minori e della dignità umana nei servizi audiovisivi e della Comunicazione al Parlamento Europeo e al Consiglio in materia di "informazioni di contenuto illegale e nocivo su Internet"[85].

Già nel 1996 la Commissione evidenziava come *l'assegnare con precisione le diverse responsabilità* in relazione ai materiali di contenuto illegale[86] (di qualsiasi

[84] Cfr. OLG München, 21 settembre 2006, 29 U 2119/06, in dejure.org:

[85] V. Commissione Europea - IP/96/930, 16 ottobre 1996, in europa.eu. La Comunicazione presenta gli interventi a breve termine mentre il libro Verde è volto a incentivare il dibattito a lungo termine per l'elaborazione di politiche sulla tutela specifica dei minori e della dignità umana in rapporto all'avvento delle nuove tecnologie. Testo integrale in privacy.it.

[86] Commissione Europea, *Comunicazione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale ed al Comitato delle regioni. Informazioni di contenuto illegale e nocivo su Internet*, Bruxelles, 16/10/96 COM(96) 487. La commissione Europea, nell'*incipit* della dichiarazione, distingue tra i contenuti illegali ed i contenuti nocivi: «Queste due categorie di contenuti pongono questioni di principio radicalmente differenti, cui vanno date risposte giuridiche e tecnologiche molto diverse. Sarebbe pericoloso confondere *problemi distinti quali quello del possibile accesso di minorenni a materiale pornografico destinato agli adulti e quello dell'accesso di adulti alla pornografia infantile*. Occorre definire chiaramente le priorità e mobilitare le risorse disponibili per affrontare i problemi più gravi, vale a dire la lotta ai contenuti criminali, consistente ad esempio nel reprimere la pornografia infantile o lo sfruttamento della novità tecnologica dell'Internet a fini criminali.

a. Contenuto criminale

natura essi siano: pornografia infantile, violazione di diritti d'autore, offerte fraudolente, diffamazione etc.) fosse uno *step* essenziale per garantire la sicurezza

---

Esiste tutta una gamma di norme che limitano per motivi differenti l'impiego e la distribuzione d'informazioni con determinati contenuti. La violazione di tali norme comporta l'illegalità del materiale.

In alcuni casi non si tratta di tutelare l'ordine pubblico, quanto piuttosto i diritti delle singole persone (tutela della vita privata e del buon nome) e di un ambiente atto a consentire la fioritura delle attività di creazione di materiale (tutela della proprietà intellettuale). Contro contenuti tali da configurare reati quali l'infrazione del diritto d'autore, la diffamazione, l'invasione della sfera privata od una pubblicità comparativa illegale si procederà di norma su iniziativa della persona i cui diritti siano lesi nell'ambito di un'azione civile per danni ovvero mediante un ordine del tribunale, benché tali diritti possano eventualmente venir parimenti tutelati in sede penale od amministrativa (tutela dei dati). Anche i fornitori di servizi potranno venir coinvolti in azioni riguardanti il contenuto delle informazioni giacché potranno venir accusati di averne agevolato la diffusione. Determinato materiale viene inoltre *considerato criminale* dalle legislazioni degli Stati membri. In questa categoria rientrano ad esempio la pornografia infantile, la tratta degli esseri umani, la divulgazione di materiale razzista o gli incitamenti all'odio razziale, il terrorismo ovvero tutte le forme di frode (ad esempio l'impiego fraudolento delle carte di credito). L'esatta definizione dei comportamenti illeciti varia da un paese all'altro. All'interno dell'UE ad esempio, anche alla pornografia infantile, campo in cui più unanime è il consenso, in alcuni Stati membri si applicano specifiche disposizioni di legge: si veda il Libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e d'informazione. In altri, disposizioni d'indole più generale attinenti alla pubblicazione di materiale osceno. Come ad esempio nel caso della pubblicazione del "Mein Kampf" di Adolf Hitler ovvero della propugnazione di tesi storiografiche "revisioniste" (tendenti cioè a negare che l'Olocausto abbia avuto luogo), che sono entrambe vietate in alcuni Stati. Possono inoltre insorgere difficoltà pratiche per fare rispettare la legge nel caso in cui determinati atti siano perseguibili in uno Stato membro ma non in un altro.

b. Contenuto nocivo

I valori e la sensibilità altrui possono venir oltraggiati da diversi tipi di materiale, che esprimano opinioni politiche, credenze religiose o pareri in tema di razza etc. La nozione di nocuità risente di differenze culturali. Ogni paese può raggiungere proprie conclusioni nel definire il confine tra ciò che è consentito e ciò che non lo è. Risulta dunque indispensabile che le iniziative internazionali tengano conto della diversità delle norme morali nei diversi paesi per esaminare la possibilità d'arrivare a norme idonee a tutelare le persone contro il materiale offensivo pur garantendo la libertà d'espressione. In questo contesto è implicito che i diritti fondamentali, e specialmente quello della libertà d'espressione, vadano pienamente rispettati (per quanto concerne i limiti negli Stati membri si veda il Libro verde sulla tutela dei minori e della dignità umana, Allegato III)».

in rete mantenendo il giusto equilibrio tra libero flusso delle informazioni e la tutela del pubblico interesse: «Nel caso in cui i *fornitori di servizi* forniscano anche materiale sul World Wide Web ovvero nell'ambito dei *newsgroups* ovviamente essi ne sono responsabili alla stessa stregua di qualsiasi autore o fornitore di materiale; se però il materiale viene fornito da terzi occorre che la questione della responsabilità dei fornitori di servizi sia chiara»[87].

La Commissione proponeva quindi l'esperienza di alcuni Stati membri (Austria, Germania, Francia e Regno Unito) nei quali la responsabilità giuridica dei *providers* poteva essere invocata in relazione al materiale ospitato sul loro *server* soltanto qualora fosse ragionevole attendersi che essi fossero consapevoli di una sua illegalità manifestamente apparente ovvero non avessero adottato provvedimenti per eliminarlo una volta che la loro attenzione fosse stata chiaramente attirata su di esso.

Essenziali sono state anche le riflessioni emerse durante la conferenza Ministeriale europea sul tema *"Global Information Networks: Realising the Potential"*, tenutasi a Bonn nel luglio 1997[88], che hanno portato ad un proficuo

[87] *Ivi*, punto 4 B (i).

[88] Cfr. Dichiarazione finale della Conferenza Ministeriale Europea, *Global Information Networks: Realising the Potential*, Bonn 6-8 Luglio 1997, in gandalf.it. Alla Conferenza hanno partecipato non solo i Ministri degli stati membri dell'UE ma anche membri dell'*European Free Trade Association*, membri della Commissione Europea, personalità dagli Stati Uniti, Canada, Giappone e Russia, rappresentanti delle imprese e dei consumatori e numerose organizzazioni europee e internazionali. In modo particolare con riguardo alla tematica che qui interessa, nella dichiarazione si afferma che: «I Ministri sottolineano l'importanza della definizione chiara delle norme legali riguardo alla responsabilità per i contenuti dei vari attori coinvolti nella catena che va dalla creazione all'utilizzo. Riconoscono la necessità di fare chiara distinzione tra la responsabilità di chi produce e mette in circolazione i contenuti e quella degli intermediari. I Ministri sottolineano che le regole sulla responsabilità riguardo ai contenuti debbano essere basate su di un insieme di regole comuni tali da assicurare un campo di azione comune e omogeneo. Perciò gli intermediari come gli operatori di rete e i *provider* non sono, in generale, responsabili dei contenuti. Tale principio dovrebbe essere applicato in modo tale che gli intermediari come gli operatori di rete e i *provider* non siano soggetti a regole irragionevoli, sproporzionate o discriminatorie. In ogni caso la terza parte che opera il servizio di *hosting* di tali contenuti non dovrebbe esercitare un ruolo di controllo sui contenuti che non ha ragione di ritenere illegali. Si

dibatto in materia culminato nella proposta della Commissione di un "Piano di azione comunitario per promuovere l'uso sicuro di Internet", successivamente adottato dal Consiglio dell'Unione europea[89].

Di lì a poco la delicata questione della responsabilità dei *providers* in riferimento ai contenuti illeciti pubblicati sulle loro reti è stata affrontata nella Direttiva 2000/31/CE[90] comunemente detta *e-Commerce* che, ad oggi, rappresenta il modello legislativo di riferimento per i Paesi membri dell'Unione europea.

La direttiva fornisce innanzitutto la definizione di "prestatore", inteso quale «persona fisica o giuridica che presta un servizio della società d'informazione»[91], a sua volta descritto come qualsiasi «servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica, mediante apparecchiature elettroniche di elaborazione (compresa la compressione digitale) e di memorizzazione di dati, e a richiesta individuale di un destinatario di servizi»[92]. La direttiva poi unifica

---

dovrebbe tener conto di quanto tali intermediari abbiano ragionevole motivo di conoscere, e ragionevole possibilità di controllare, i contenuti. I Ministri ritengono che le regole sulla responsabilità debbano realizzare il principio di libertà di parola, rispettare gli interessi pubblici e privati e non imporre agli attori oneri sproporzionati».

[89] Commissione Europea, *Proposta di decisione del Consiglio che adotta un Piano pluriennale d'azione comunitaria per promuovere l'uso sicuro di Internet*, 27 novembre 1997, pubblicata sulla G.U. n. C 48 del 13.02.1998. Nella proposta, oltre all'invito allo sviluppo di sistemi di autodisciplina e di controllo dei contenuti tramite filtri e sistemi di valutazione che consentano a genitori ed insegnanti di selezionare contenuti adeguati ai minori, tra le linee di azione individuate per limitare la circolazione di materiale illegale anche l'istituzione di una rete europea di centri (*hot-line*) volti alla raccolta delle segnalazioni di contenuti illeciti degli utenti.

[90] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, 8 giugno 2000, *Relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)*, pubblicata sulla G.U.C.E. del 17.07.2000. La direttiva riguarda in particolare settori ed attività *on-line* quali: giornali, banche dati, servizi finanziari, servizi professionali (di avvocati, medici, contabili, agenti immobiliari), servizi ricreativi (ad esempio, video a richiesta), commercializzazione e pubblicità dirette e servizi d'accesso a Internet.

[91] *Ivi*, art. 2 b).

[92] *Ivi*, Considerando 17-18; art. 2 a).

consumatori e non consumatori nell'unica categoria dei "destinatari" ovvero coloro i quali utilizzano i servizi della società d'informazione, a scopo professionale e non, in particolare per «ricercare o rendere accessibili delle informazioni»[93].

Nella quarta sezione viene affrontata specificatamente la tematica della responsabilità dei prestatori intermediari. Già ad una prima lettura risulta chiara l'influenza del *Digital Millenium Copyright Act* statunitense e della legislazione tedesca[94].

Anche nel modello europeo, a fronte della varietà dei servizi offerti dagli operatori, si è optato per discipline differenziate in base all'attività da essi concretamente svolta, indipendentemente dalla loro classificazione.

Riproducendo quasi fedelmente alcune formule del DMCA, la direttiva esonera da qualsiasi responsabilità gli intermediari che abbiano un ruolo "passivo", ovvero esercitino un'attività automatica di ordine meramente tecnico consistente nel fornire accesso ad una rete di comunicazione o trasmettere informazioni, a tale fine anche temporaneamente memorizzate per un tempo non superiore a quello ragionevolmente necessario per la trasmissione, immesse da terzi soggetti e non conosciute ne' controllate dal *provider* (cd. attività di *mere conduit*)[95].

Parimenti viene limitata la responsabilità per la memorizzazione temporanea di informazioni originate dagli utenti (cd. attività di *caching*), effettuata solo

---

[93] *Ivi*, art. 2 d).

[94] Sul punto cfr. RICCIO M. G., *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e Responsabilità*, n. 2/2003, p. 1157 ss. Secondo l'autore la scelta di appianare le differenze normative tra Europa e U.S. tramite una Direttiva "figlia" del DMCA e del TDG è stata sicuramente molto saggia data la natura transfrontaliera di Internet.

[95] Il *provider* quindi nell'attività di *mere conduit* beneficia dell'esonero totale della responsabilità qualora non sia coinvolto in alcun modo nell'informazione trasmessa ovvero non sia a lui imputabile l'origine della trasmissione, la scelta del destinatario o la modifica del contenuto. V. direttiva 2000/31/CE, Considerando 42, 43; art. 12.

scopo di facilitare il successivo inoltro dei contenuti richiesto da altri destinatari, a condizione che il *provider* si mantenga in una posizione di neutralità ovvero «a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso»[96].

Vengono quindi ripresi nuovamente i concetti di *actual knowledge* e *constructive knowledge* della normativa americana nell'ambito della disciplina dell'attività di *hosting* in relazione alla quale il *provider* non risponderà se non effettivamente a conoscenza della illeceità dei contenuti memorizzati, anche se, civilmente, basta che sia al corrente di fatti o circostanze che rendono manifesta la violazione. L'*hosting provider*, inoltre, per godere della limitazione della responsabilità, dovrà rispettare la procedura di *take down*, ovvero non appena al corrente dell'illeceità dei contenuti, deve agire prontamente per rimuoverli o disabilitarne l'accesso[97].

A differenza di quanto previsto nel DMCA la *knowledge* non è ancorata a determinati avvisi da parte degli utenti e la procedura di blocco non è specificata. Nella mente del legislatore europeo la lacuna in merito alla procedura di *"notice and take down"* avrebbe dovuto essere colmata grazie ad appositi codici di

[96] *Ivi*, art. 13. Il requisito della conoscenza, alla luce dell'articolo 15 della direttiva, dovrà essere interpretato nel senso che gli ISPs la potranno ottenere tramite le informazioni ricevute dai terzi, stante il divieto di monitoraggio dei materiali. Cfr. BAISTROCCHI P., *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, cit., p. 122 ss.

[97] Direttiva 2000/31/CE , Considerando 46, art. 14.

condotta e ad interventi legislativi nazionali in sede di attuazione della direttiva[98]. Chiaro comunque che, in assenza di statuizione in merito, risulta difficile per gli ISPs comprendere quando possano ritenere fondato un reclamo presentato da un utente, quando debbano agire prontamente per rimuovere il materiale e se l'eventuale eliminazione dello stesso li esponga o meno ad ulteriori responsabilità[99].

Gli esoneri dalla responsabilità previsti nella direttiva lasciano comunque impregiudicata la possibilità per gli Stati membri di introdurre azioni inibitorie di altro tipo (quali ordinanze da parte di organi giurisdizionali o autorità amministrative che obblighino il prestatore ad impedire o porre fine alla violazione, ad informare senza indugio le autorità competenti circa presunte attività illecite, a comunicare le informazioni che consentono di individuare i destinatari dei loro servizi al fine di individuare e prevenire le violazioni), ovvero procedure per la rimozione/disabilitazione all'accesso delle informazioni

[98] Cfr. Commisione Europea, COM(l998) 586 final 98/0325 (COD), *Proposal for a European Parliament and Council directive on certain-legal aspects of electronic commerce in the internal market*, Brussels, 18 Novembre 1998, p. 29 ss., in pitt.edu: *«Article 14 Hosting [...] Service providers will not lose the exemption from liability if after obtaining actual knowledge or becoming aware of facts and circumstances indicating illegal activity, they act expeditiously to remove or to disable access to the information. This principle established in the second indent of the paragraph, provides a basis on which different interested parties may lay down procedures for notifying the service provider about information that is the subject of illegal activity and for obtaining the removal or disablement of such information (sometimes referred to as 'notice and take down procedures'). It should nevertheless be stressed that these procedures do not and cannot replace existing judicial remedies. The Commission is actively encouraging industry self-regulatory systems, including the establishment of codes of conduct and hot line mechanisms»*. V. inoltre direttiva 2000/31/CE, Considerando 40; art. 16.

[99] Le tendenze registrate, negli Stati membri dell'UE, rispetto al concetto di *knowledge,* di cui all'art. 14 della direttiva, sono diverse. In alcuni Stati, come la Spagna, è richiesta una comunicazione ufficiale dell'autorità competente. In altri, come Germania e Austria, i requisiti minimi necessari per la sussistenza della conoscenza dell'illeceità dei contenuti sono fissati a livello giurisprudenziale. Infine si registra, nel settore specifico della tutela del *copyright*, la tendenza di un gruppo di Stati ad introdurre uno procedura *notice-and-taking-down.* Cfr. ULYS*, Study on the Liability of Internet Intermediaries, Final Report*, in europa.eu, 12 novembre 2007.

illecite[100]. Agli Stati membri viene vietato invece, ai sensi dell'art. 15 della direttiva, di imporre ai *providers* obblighi generali di sorveglianza sui contenuti trasmessi o di ricerca attiva di circostanze e fatti dai quali emergano indizi di attività illecite.

A differenza del modello americano, nella direttiva non si rinvengono disposizioni *ad hoc* in merito alla responsabilità dei motori di ricerca, delle istituzioni *non-profit* o in materia di collegamenti ipertestuali, ne' disposizioni riguardanti le possibili responsabilità a seguito della rimozione dei contenuti presumibilmente illegittimi.

Questa lacuna, come il vuoto normativo in tema di *"notice and take down"*, avrebbe dovuto essere oggetto di riesame ai sensi dell'art. 21 della direttiva. In realtà, ad oggi, non si è ancora provveduto e, nella totale vaghezza normativa, ampi margini di discrezionalità, minacciosi per la libertà di espressione, vengono quindi riconosciuti all'autorità giudiziaria nel momento in cui si debba stabilire se il *provider* possa o meno godere del sistema dei *safe harbors* europei.

Da segnalare infine che, per migliorare l'efficacia del sistema di applicazione dei diritti di proprietà intellettuale contro la contraffazione e la pirateria informatica, sono iniziati nel 2007 negoziati sull'accordo internazionale commerciale anticontraffazione (ACTA)[101], a lungo rimasti segreti e culminati il 26 gennaio 2012 con la firma da parte di 22 Stati membri dell'Unione europea (tra cui l'Italia), oltre a Stati Uniti d'America, Australia, Canada, Giappone, Repubblica di Corea, Stati uniti messicani, Regno del Marocco, Nuova Zelanda, Repubblica di Singapore, Confederazione svizzera.

---

[100] Direttiva 2000/31/CE, Considerando 45, 48; art. 12 comma 3; art. 13 comma 2; art. 14 comma 3; art. 15 comma 2.

[101] V. ACTA *Key Elements* in laquadrature.net, *Final test: Council of the European union*, *Anti-counterfeiting trade agreement between the European Union and its member states, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America*, Brussels, 23 August 2011, in europa.eu.

L'accordo, sebbene non divenuto legge per l'UE a seguito della bocciatura del Parlamento[102], è molto interessante per comprendere gli scenari futuribili e gli orientamenti internazionali che potrebbero affermarsi in materia di responsabilità penale degli ISPs[103].

In modo particolare la quarta sezione rubricata *"criminal enforcement"* prevede un obbligo per gli Stati aderenti di introdurre sanzioni e procedimenti penali almeno in relazione ai casi intenzionali di contraffazione di marchi o di pirateria realizzati su "scala commerciale", ossia identificabili come attività commerciali volte all'ottenimento di vantaggi economici o commerciali diretti ed indiretti[104].

Un secondo obbligo di criminalizzazione riguarda i casi di importazione o esportazione deliberata di prodotti di marca contraffatti o di beni coperti da diritti d'autore piratati su scala commerciale[105].

---

[102] Il Parlamento europeo, chiamato a ratificare l'accordo, l'ha respinto il 4 luglio 2012. L'ACTA nel suo *iter* europeo ha incontrato critiche sin dalla sua iniziale presentazione. A favore della sua bocciatura le cinque commissioni parlamentari chiamate a pronunciarsi in merito (ovvero la Commissione per l'Industria, la ricerca e l'energia, la Commissione Giuridica, la Commissione per le Libertà civili, la giustizia e gli affari interni, e la Commissione per lo Sviluppo), la raccomandazione del relatore David Martin della Commissione per il Commercio internazionale, nonché una petizione firmata da 2.8 milioni di cittadini di tutto il mondo. Per un quadro complessivo della vicenda cfr. *News: ACTA-per-principianti*, in europarl.europa.eu. Tutti i documenti della procedura sono reperibili sullo stesso sito: n. Procedura 2011/0167.

[103] Il Parlamento europeo, nel recente rapporto sulla Strategia in merito ai diritti di proprietà intellettuale negli accordi coi Paesi terzi, nel chiedere alla Commissione di legiferare nuovamente sulla materia, tenendo conto delle innovazioni tecnologiche, ha proprio utilizzato come modello il fallito ACTA. V. TAMBURRINO C., *UE, la proprietà intellettuale riparte da ACTA*, in punto-informatico.it, 19 Giugno 2015; v. inoltre la relazione della parlamentare europea MOSCA A., *Una breve scheda sullo stato dell'arte della normativa europea sui diritti di proprietà intellettuale*, in alessiamosca.it, 22 Marzo 2015.

[104] Cfr. ACTA, art. 23, comma 1. Il requisito della *commercial scale* in realtà, anche se così specificato, risulta estremamente vago e suscettibile di diverse e molteplici interpretazioni, che potrebbero ad esempio permetterne l'applicazione nel caso dell'attività del *file-sharing*. Cfr. *News: ACTA: Updated Analysis of the Final Version*, 9 Dicembre 2010, in laquadrature.net.

[105] ACTA, art. 23, comma 2: *«willful importation and domestic use, in the course of trade and on a commercial scale, of labels or packaging: (a) to which a mark has been applied without*

E' infine da precisare che, secondo l'accordo, in riferimento ai reati summenzionati anche le condotte di *"aiding and abetting"* dovrebbero essere oggetto di penalizzazione: è proprio questa previsione che potrebbe essere utilizzata in futuro per obbligare gli Stati a procedere penalmente nei confronti degli ISPs anche quando non siano gli autori dei reati.

4. LA NORMATIVA ITALIANA DI RIFERIMENTO: IL DECRETO LEGISLATIVO N. 70/2003

Attualmente la responsabilità degli ISPs nell'ordinamento italiano è disciplinata dal Decreto Legislativo del 9 aprile 2003, n. 70, con il quale si è dato attuazione alla direttiva 2000/31/CE.

Anche a livello nazionale le diverse ipotesi di responsabilità sono state collegate alle funzioni che possono essere esercitate dal *provider*[106].

Ricalcando pedissequamente le formule di cui agli artt. 12 e ss. della direttiva *e-Commerce*, il d.lgs. n. 70/2003 prevede *safe harbors* nell'ambito delle attività di *mere conduit*, *caching* ed *hosting*.

A differenza di quanto stabilito in sede europea, la *knowledge*, che determina l'obbligo per il prestatore di intervenire "immediatamente" per bloccare le informazioni illecite, è connessa alle comunicazioni delle autorità competenti. L'interpretazione letterale della norma sembrerebbe comportare che il *provider* non debba attivarsi in caso di semplice "denuncia" anonima[107]. Il legislatore

---

authorization which is identical to, or cannot be distinguished from, a trademark registered in its territory; and (b) which are intended to be used in the course of trade on goods or in relation to services which are identical to goods or services for which such trademark is registered».

[106] Sulla scorta del testo comunitario il *provider* viene definito all'art. 2, comma 1 lett. B., come «la persona fisica o giuridica che presta un servizio della società dell'informazione».

[107] I tribunali italiani, interpretando restrittivamente l'art. 16 del d.lgs. 70/2003, si stanno per l'appunto orientando nel senso di ritenere necessaria l'emissione di un provvedimento giuridico-amministrativo al fine di poter ritenere integrato il requisito dell'effettiva conoscenza del materiale

italiano con questo inciso individuerebbe quindi una base per la procedura di "*notice and take down"*, lasciando però totalmente imprecisati punti cruciali quali la specificazione delle autorità competenti[108], delle modalità della *notification*, della eventuale responsabilità del *provider* in relazione ai contenuti rimossi e della procedura di ripristino dei contenuti nel caso in cui essi si rivelino legittimi[109].

A fronte della possibilità, riconosciuta agli Stati membri dalla direttiva *e-*

---

illecito. La stessa tendenza si sta registrando anche nell'ordinamento francese. Sul punto cfr. FALETTI E., *La responsabilità dell'Internet Provider in Diritto Comparato per materiale pubblicato da terzi*, cit., p. 137 ss.

[108] Tra le autorità competenti vi è anche l'Agcom (Autorità per le garanzie nelle comunicazioni). Ciò è desumibile dall'art. 1 del Codice delle comunicazioni elettroniche (d.lgs. n. 259/2003) che la qualifica come Autorità nazionale per tutto il settore delle comunicazioni elettroniche, nonché dal d.lgs. n. 44/2010 che, ampliando i poteri di vigilanza dell'Agcom in materia di diritto d'autore, ha previsto che quest'ultima, al pari dell'autorità giudiziaria, possa esigere che il prestatore impedisca o ponga fine alle violazioni ed emanare disposizioni regolamentari necessarie per rendere effettiva la tutela dei diritti d'autore e di proprietà intellettuale per i servizi audiovisivi. L'AGCOM, proprio in conformità a tali disposizioni ha emanato, con delibera n. 680/13/CONS del 12 dicembre 2013, un regolamento per la tutela del diritto d'autore sulle reti di comunicazione elettronica, in relazione al quale è stata di recente sollevata questione di legittimità costituzionale, dichiarata inammissibile con sentenza della Corte Costituzionale n. 247/2015. L'AGCOM, a seguito della suddetta sentenza, può quindi continuare nella sua attività di valutazione delle richieste dei detentori dei diritti d'autore, e d'inibizione nei confronti dei siti che ospitano contenuti che violano il *copyright*. Per una ricostruzione della vicenda v. POLLICINO O., BASSINI M., *Le parole contano", ovvero "tanto rumore per nulla". Sulla (prevista) inammissibilità della questione di legittimità costituzionale della base giuridica del Regolamento AGCOM #ddaonline*, in medialaws.eu, 4 Dicembre 2015; BOTTA' G., *Regolamento AGCOM, la Corte Costituzionale non decide*, in punto-informatico.it, 4 Dicembre 2015.

[109] Cfr. COMANDE' G., *Al via l'attuazione della direttiva sul commercio elettronico, ma… serve maggiore coordinamento*, in *Danno e Responsabilità*, n. 8-9/2003, p. 809 ss. Negli ultimi anni sono state presentate diverse proposte di riforma dell'articolo in esame. Ad esempio, la cd. "proposta Fava", bocciata nel febbraio 2011 dalla Camera dei Deputati, prevedeva la possibilità per i *providers* di rimuovere i contenuti illeciti non solo sulla base della segnalazione delle autorità competenti, ma anche di qualsiasi soggetto interessato. V. PIROZZOLI A., *La responsabilità dell'Internet Service Provider. Il nuovo orientamento giurisprudenziale nell'ultimo caso Google*, cit.

Commerce, di imporre agli ISPs obblighi informativi, nel rispetto del divieto di introdurre obblighi generali di sorveglianza dei contenuti trasmessi o memorizzati o di ricerca attiva di fatti o circostanze dalle quali emergano profili di illiceità, l'art. 17 prevede che gli operatori sono comunque tenuti «a. ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; b. a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite»[110].

In modo particolare, ai sensi del terzo comma dell'art. 17 il *provider* è civilmente responsabile nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso ai contenuti, ovvero se, pur essendo a conoscenza del carattere pregiudizievole dei contenuti di cui permette l'accesso, non informa le autorità competenti[111].

Fatta eccezione che per qualche profilo, il quadro nazionale è totalmente in linea con le scelte europee e risulta privo di disposizioni chiarificatrici od innovative. L'atteggiamento "cauto" e di passivo accoglimento del legislatore

[110] Art. 17, comma 2, d.lgs. n. 70/2003. L'imposizione di tali obblighi di segnalazione/denuncia ha suscitato critiche in dottrina sulla base del rilievo che il nostro codice penale prevede obblighi di tale natura esclusivamente a carico dei pubblici ufficiali e degli incaricati di pubblico servizio in relazione ai reati dei quali abbiano avuto notizia nell'esercizio o a causa delle loro funzioni (artt. 361, 362 c.p.) o ancora dei cittadini limitatamente ai delitti contro la personalità dello Stato puniti con l'ergastolo (art. 34 c.p.). L'imposizione di tali obblighi di collaborazione a carico del *provider* mal si concilierebbe con la connotazione privatistica di imprenditore propria di quest'ultimo, trasformandolo in una sorta di "garante dei contenuti" trasmessi. Sul punto cfr. SPAGNOLETTI V., *La responsabilità del provider per i contenuti illeciti in internet*, in *Giurisprudenza di merito*, 2004, p. 1922 ss.

[111] Come evidenziato in dottrina, il problema è stabilire quando è possibile affermare che il prestatore è "a conoscenza" delle violazioni. Cfr. PINO G., *Assenza di un obbligo generale di sorveglianza a carico degli Internet Services Providers sui contenuti immessi da terzi in rete*, in *Danno e Responsabilità*, n. 9/2004, p. 832 ss.

italiano è stato perlopiù oggetto di numerose critiche in dottrina[112]. Per la complessità del tema e la difficoltà di comprendere appieno i concetti vaghi disseminati nel tessuto normativo europeo, la ratifica della direttiva europea tramite il d.lgs. n. 70/2003 rappresenta un'occasione persa per fissare disposizioni precise in tema di responsabilità dei *providers* e, per alcuni versi, come di seguito esposto, ha acuito i dubbi e le incertezze riscontrate in ambito giurisprudenziale già da prima della sua entrata in vigore.

E' infine necessario segnalare che, negli ultimi anni, sono stati introdotti specifici obblighi per gli ISPs che arricchiscono il quadro sopra delineato[113].

Ai sensi dell'art. 11 del Decreto cyber-sicurezza del 24 gennaio 2013, «gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici»[114] sono tenuti a

---

[112] Cfr. RICCIO M. G., *La responsabilità degli internet providers nel d.lgs. n. 70/03*, cit., p. 1158 ss. Secondo l'autore «Il d.lgs. n. 70/03 non sembra […] aver apportato profonde modifiche al tessuto delineato alla direttiva comunitaria. Si tratta, però, di un profilo che appare assolutamente criticabile. Il legislatore comunitario deve far fronte ad un problema del quale il suo "collega" nazionale non è investito: scrivere un testo legislativo che possa essere compreso in tutti gli Stati membri, tenendo conto delle differenze (talora profonde) esistenti tra i singoli sistemi giuridici. In sintesi, era lecito attendersi che il recepimento della direttiva n. 31 del 2000 facesse chiarezza […] se questo è l'approccio del legislatore interno, non sarebbe più celere ed economico saltare il momento del recepimento interno, rendendo immediatamente e direttamente vigente il testo della direttiva? Che senso ha un legislatore che, mutilando il proprio ruolo e intraprendendo una ingiustificata e inopportuna strada di *self-restraint*, si limita ad adempire ad una funzione - come correttamente osservato - "notarile" (e l'accostamento appare finanche eufemistico)?». Fortemente critico dell'impostazione adottata dal Legislatore, non solo a livello linguistico ma redazionale nel suo complesso, anche ZENO-ZENCOVICH V., *Note critiche sulla nuova disciplina del commercio elettronico dettata dal d.lgs. 70/03*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 3/2003, p. 505 ss.

[113] Come sarà illustrato nel capitolo che segue, doveri peculiari di collaborazione si rinvengono anche nel campo specifico della lotta alla pedopornografia, al terrorismo, al gioco d'azzardo nonché nell'ambito della tutela della *privacy*, del diritto d'autore e della proprietà industriale.

[114] Art. 11 DPCM 24.01.13.

comunicare al Nucleo per la sicurezza cibernetica ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici; ad adottare *best practices* e misure finalizzate a garantire la sicurezza cibernetica; a fornire informazioni agli organismi di informazione per la sicurezza e a consentire agli stessi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza, nei casi previsti dalla legge n. 124/2007; ed infine a collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

Anche il Decreto Legge 18 febbraio 2015, n. 7[115] (Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione), convertito con Legge del 17 aprile 2015, ha previsto un nuovo obbligo per gli ISPs, ovvero quello di inibire l'accesso ai siti che l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, fatte salve le iniziative e le determinazioni dell'autorità giudiziaria, inserisce nell'elenco di siti utilizzati per le attività e condotte di cui agli artt. 270 *bis* (associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico) e 270 *sexies* (condotte con finalità di terrorismo) c.p., elenco nel quale confluiscono anche le segnalazioni effettuate dagli organi di polizia giudiziaria[116].

---

[115] Per un primo commento al decreto cfr. VIGANÒ F., *Pubblicato sulla Gazzetta Ufficiale il nuovo decreto legge in materia di contrasto al terrorismo*, in penalecontemporaneo.it, 23 Febbraio 2015; BALSAMO A., *Decreto antiterrorismo e riforma del sistema delle misure di prevenzione*, in penalecontemporaneo.it, 2 Marzo 2015. Poichè strettamente inerente alla materia trattata nel presente lavoro si segnala inoltre che il decreto in esame ha introdotto nel codice penale la circostanze aggravante «se il fatto è commesso mediante strumenti informatici o telematici» all'art. 270 *quinquies (*addestramento ad attività con finalità di terrorismo anche internazionale), nonché agli artt. 302 (istigazione a commettere un delitto doloso contro la personalità dello Stato), 414, comma 3 (pubblica apologia di delitto) e 414, comma 4 (pubblica istigazione o apologia di delitti di terrorismo o crimini contro l'umanità).

[116] Il decreto, approvato all'indomani dei fatti di Parigi e della strage presso la redazione di *Charlie Hebdov*, crea una vera e propria lista nera che ha l'obiettivo di oscurare quei siti che

Inoltre, ai sensi dell'art. 2, comma 4, del d.l. n. 7/2015 «quando si procede per i delitti di cui agli articoli 270 *bis*, 270 *ter*, 270 *quater* e 270 *quinquies* del codice penale commessi con le finalità di terrorismo di cui all'articolo 270 *sexies* del codice penale, e sussistono concreti elementi che consentano di ritenere che alcuno compia dette attività per via telematica, il pubblico ministero ordina, con decreto motivato, ai fornitori di servizi di cui all'articolo 16 del decreto legislativo 9 aprile 2003, n. 70, ovvero ai soggetti che comunque forniscono servizi di immissione e gestione, attraverso i quali il contenuto relativo alle medesime attività è reso accessibile al pubblico, di provvedere alla rimozione dello stesso. I destinatari adempiono all'ordine immediatamente e comunque non oltre quarantotto ore dal ricevimento della notifica. In caso di mancato adempimento, si dispone l'interdizione dell'accesso al dominio internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale»[117].

Nelle recenti riforme legislative, a fronte dell'evoluzione tecnologica e delle nuove forme assunte dalla minaccia terroristica e dalla minaccia alla sicurezza cibernetica, il ruolo dell'ISP quale collaboratore dell'Autorità nell'ambito dell'attività di repressione e di prevenzione di tali illeciti risulta ormai

---

inneggiano ai *kamikaze*. Cfr. TAMBURRINO C., *Italia, la Rete dell'antiterrorismo*, in punto-informatico.it, 11 Febbraio 2015.

[117] Art 2, comma 4, d.l. n. 7/2015. Nell'articolo in questione non viene specificato se il decreto del pubblico ministero debba essere convalidato da parte del giudice secondo le disposizioni generali dell'art. 321 c.p.p. (oggetto del sequestro preventivo), peraltro richiamato nella seconda parte della disposizione. La legge n. 43 del 17 aprile 2015 di conversione, con modificazioni, del decreto ha inserito al comma 4, dopo le parole: «il pubblico ministero ordina con decreto motivato,» le seguenti: «preferibilmente per il tramite degli organi di polizia giudiziaria di cui al comma 2 dell'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155»; dopo il secondo periodo il seguente: «In caso di contenuti generati dagli utenti e ospitati su piattaforme riconducibili a soggetti terzi, è disposta la rimozione dei soli specifici contenuti illeciti»; ed infine al terzo periodo ha aggiunto «, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite».

lapalissiana[118] e rende ancor più necessario un ripensamento sull'eventuale configurabilità di una responsabilità da reato del *provider*.

[118] Da segnalare che in Francia, proprio a causa degli ultimi attacchi terroristici, è stato approvato il *Décret n. 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* che permette il blocco (tramite DNS) di determinati siti onde inibire l'accesso a contenuti pedopornografici o di carattere terroristico senza bisogno dell'intervento di un giudice, ma a semplice richiesta della Direzione generale della polizia nazionale e della sua unità specializzata in crimini informatici. Gli ISPs devono soddisfare la richiesta entro 24 ore. A poche settimane dalla sua approvazione la normative è già stata applicata: i siti, accusati di essere *pro-jihad* e bloccati dagli ISP senza passare al vaglio del potere giudiziario, sembrano essere cinque. Cfr. GEUSS C., *Sites featuring terrorism or child pornography to be blocked in France ISPs will have to block questionable content within 24 of notice*, in arstechnica.com, 7 Febbraio 2015; TAMBURRINO C., *Francia, il Terrore e il terrorismo*, in punto-informatico.it, 18 Marzo 2015.

CAPITOLO QUARTO

RILIEVI PENALISTICI SULLA RESPONSABILITÀ *DELL'INTERNET SERVICE PROVIDER*

SOMMARIO: 1. Responsabilità commissiva: a) Ipotesi di autoria; b) Ipotesi di concorso - 2. Responsabilità omissiva - 3. Responsabilità *ex* art. 57 c.p. - 4. Ermeneutiche giurisprudenziali della Corte europea dei diritti dell'uomo e della Corte di giustizia dell'Unione europea.

Le disposizioni previste per gli ISPs, dianzi esposte, non fissano specifiche ipotesi di reato. Pertanto, onde valutare la configurabilità di una responsabilità penale o amministrativa da reato dei *providers* (a seconda che gli stessi si identifichino in una persona fisica o giuridica) è necessario esaminare, alla luce della normativa seppur sinteticamente richiamata, le regole penali di parte generale e specificatamente gli istituti del concorso di persone nel reato (art. 110 c.p.)[1], della responsabilità per omesso impedimento dell'evento (art. 40, comma 2,

[1] Nel vigente ordinamento, il concorso di persone nel reato, previsto all'art. 110 c.p., è concepito come una struttura unitaria nella quale confluiscono tutti gli atti dei partecipi. Abbandonato definitivamente il modello differenziato del Codice Zanardelli, quello unitario opta per una tipizzazione dell'illecito in cui l'azione tipica è costituita dall'insieme delle condotte dei singoli compartecipi, legate eziologicamente all'evento lesivo. Dell'effettivo contributo causale di ciascuno si tiene conto in sede di quantificazione concreta della pena. Gli elementi costitutivi della fattispecie del concorso, che, nasce dall'integrazione tra norma generale di cui all'articolo 110 c.p. e la singola norma incriminatrice di parte speciale sono: la pluralità di soggetti; la realizzazione di un fatto costituente reato; il contributo causale di ciascun concorrente alla realizzazione comune; l'elemento soggettivo (coscienza e volontà del fatto criminoso; volontà di concorrere con altri alla realizzazione del reato). Per un'analisi degli aspetti fondamentali dell'istituto e i richiami alla

c.p.)[2], nonché la disciplina dei delitti commessi a mezzo della stampa, pur nella consapevolezza che la tematica non si presta ad una soluzione unica e applicabile ad ogni ipotesi, essendo sempre necessario sagomare l'individuazione dei soggetti responsabili nel greto delle sfumature del caso concreto.

1. RESPONSABILITÀ COMMISSIVA

a) Ipotesi di autoria

Riprendendo la suddivisione descritta nel secondo capitolo ed in modo particolare la struttura a strati proposta da Vanberg[3], si può affermare con sicurezza che, a livello di *content layer*, l'ISP sarà autonomamente responsabile per i contenuti di cui è autore o coatore e, presentando nella quasi totalità dei casi una struttura organizzativa complessa, risponderà secondo le regole previste in tema di responsabilità da reato delle persone giuridiche.

---

bibliografia essenziale in tema v. RINALDINI F., *art. 110 c.p.*, in DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato*, cit., p. 1514 ss.

[2] L'art. 40, comma 2, c.p., pone una clausola di equivalenza in base alla quale il mancato impedimento di un evento che si ha l'obbligo giuridico di impedire corrisponde a cagionarlo. La *ratio* della disposizione va ricercata nell'intenzione dell'ordinamento di assicurare a determinati beni giuridici una tutela rafforzata, attribuendo ad altri soggetti, diversi dall'interessato, l'obbligo di evitarne la lesione.

La natura omissiva dei reati determina un'analisi diversa del nesso causale che deve sussistere tra condotta ed evento: nei reati caratterizzati da condotte attive è necessario valutare se l'evento si sarebbe realizzato anche in assenza dell'azione, mentre nelle fattispecie omissive la problematica della causalità è particolarmente complessa, perché è necessario valutare l'efficacia eziologica di un *nihil* e cioè di una azione non compiuta che, quindi, sul piano fenomenico, nulla avrebbe potuto determinare. E' necessario pertanto verificare se la realizzazione dell'azione omessa avrebbe impedito l'evento. Per un'analisi degli aspetti fondamentali dell'istituto ed i richiami alla bibliografia essenziale in tema v. D'ALESSANDRO F., *art. 40 c.p.: B) L'equivalenza tra azione ed omissione*, in DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato*, cit., p. 430 ss.; ROMANO M., *Commentario sistematico del codice penale I*, sub. *art. 40 c.p*, Milano, 1995, p. 337 ss.

[3] V. p. 44.

A livello giurisprudenziale particolarmente interessante risulta la questione concernente i servizi di completamento delle ricerche.

Le previsioni di auto-completamento vengono generate automaticamente da un algoritmo in base a una serie di fattori oggettivi, quale ad esempio la frequenza con cui gli utenti hanno cercato un termine in passato[4]. Tale *software* si occupa quindi di associare delle parole a quelle digitate dall'utente nel *box* del motore di ricerca durante l'esecuzione della *query* (ricerca).

L'algoritmo comporta evidentemente che il motore di ricerca ponga in essere un'attività, seppur automatica, e, nel caso in cui la funzione di auto-completamento produca effetti degni di tutela civile o penale, sono sorte alcune difficoltà nell'applicare l'esenzione di responsabilità prevista per i *provider* dalla direttiva europea *e-Commerce* e dal relativo decreto legislativo di recepimento nel nostro ordinamento[5].

Secondo un primo orientamento, in relazione alla specifica attività di completamento delle ricerche, sarebbe totalmente errata l'assimilabilità dei motori di ricerca ai *content providers*[6].

---

[4] La funzione di *auto-complete* è particolarmente utile poiché permette di risparmiare tempo durante le ricerche, trovando le informazioni più rapidamente e senza dover digitare interamente la *query*, correggendo errori ortografici e ripetendo una ricerca preferita tra le previsioni passate. V. voce *websearch* in support.google.com.

[5] Cfr. PERON S., *La diffamazione tramite i motori di ricerca*, in personaedanno.it, 3 Aprile 2011; SCANNICCHIO T., *La responsabilità del motore di ricerca per la funzione «auto-complete»*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2012, p. 1212 ss.; RICCIO M. G., *Google: sulle ricerche automatiche esclusa la diffamazione*, in diritto24.ilsole24ore.com, 4 Maggio 2012; PIROZZOLI A., *La responsabilità dell'internet service provider. Il nuovo orientamento giurisprudenziale nell'ultimo caso Google*, in *Rivista AIC*, n. 3/2012, 25 Settembre 2012; POLLICINO O., *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi costituzionali*, n. 1/2014, p. 45 ss.

[6] Cfr. Tribunale di Pinerolo, ord. 30 aprile 2012; Tribunale di Firenze, ord. 25 maggio 2012; Particolarmente interessante, nell'ordinanza del Tribunale fiorentino, il ridimensionamento della costante tendenza giurisprudenziale a ritenere idonea la diffida stragiudiziale (ai sensi dell'art. 16 del d.lgs. 70/2003) per far acquisire all'ISP la consapevolezza del fatto illecito. Il Giudice ha infatti precisato che, per attivare le conseguenze in termini di responsabilità dell'ISP, è necessario che le competenti autorità abbiano dichiarato il carattere illecito dei contenuti ovvero ne abbiano

Gli ISPs non potrebbero cioè essere qualificati come autori dei contenuti visualizzati attraverso il *software auto-complete* poiché tale servizio riproduce statisticamente solamente il risultato delle ricerche più popolari effettuate dagli utenti, non frasi di senso compiuto né manifestazioni di pensiero del motore di ricerca stesso[7].

La configurabilità di reati quali la diffamazione sarebbe quindi totalmente esclusa, dato che l'automatismo del processo porrebbe la funzione di completamento al di fuori della sfera di *dominium* del *provider*, escludendone la *suitas*[8] della condotta.

Non sembrano in realtà travisare la natura della funzione coloro i quali, discostandosi da tale impostazione, vi intravedono una forma di elaborazione dati solo astrattamente "neutra". Essendo basato su sistemi di algoritmi matematici che operano in virtù di criteri prescelti dal suo ideatore, il solo fatto che la modalità operativa del sistema completi la ricerca in maniera automatica non renderebbe

---

ordinato all'ISP la rimozione, o, infine, che le informazioni/contenuti abbiano effettivamente causato pregiudizi accertati tramite decisione di un'autorità competente comunicata al *provider*. La mera diffida di parte non sarebbe pertanto sufficiente.

[7] Cfr. Tribunale di Milano, ord. 25 marzo 2013, con nota di SCANNICCHIO T., *Il provider non risponde degli accostamenti diffamatori prodotti automaticamente dal motore di ricerca*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 2/2013, p. 380 ss. Il servizio in questione, secondo il Tribunale, deve essere qualificato come mero servizio di *caching*, cioè di memorizzazione temporanea di informazioni fornite dagli stessi utenti, senza alcuna responsabilità in relazione al loro contenuto a norma dell'art. 15 d.lgs. 70/2003. Pertanto, nel caso trattato (in cui il ricorrente, inserendo nella stringa di ricerca di *Google* il proprio nome e quello della fondazione a lui stesso intitolata, si era accorto che l'auto-completamento li associava a termini come "truffa", "truffatore", "plagio" e "setta"), il Tribunale meneghino chiarisce come, proprio ai sensi della legislazione vigente che vieta l'obbligo di filtraggio preventivo da parte degli ISPs, prima di un'esplicita richiesta dell'autorità giudiziaria, il *provider* non aveva il dovere di rimuovere i risultati delle ricerche automatiche asseritamente lesivi.

[8] Intesa quale coscienza e volontà dell'azione *ex* art. 42, comma 1, c.p.

completamente "neutro" l'abbinamento. Quest'ultimo, infatti, presuppone comunque una scelta commerciale precisa e ne costituisce il frutto[9].

Il ruolo attivo del motore di ricerca ne comporterebbe la responsabilità per i risultati che il sistema di completamento automatico produce. In modo particolare l'ISP dovrebbe pertanto operare non un controllo preventivo sui dati presenti nel sistema, il che pare inesigibile, sia in considerazione del numero indeterminabile di parole con un potenziale significato negativo, sia del fatto che il medesimo termine potrebbe avere significati del tutto diversi se abbinato a specifici vocaboli, ma *ex post* sui risultati: «è il risultato improprio ottenuto con l'applicazione di detto sistema a determinare la responsabilità di chi dello stesso si avvale»[10].

In Europa questo indirizzo è stato seguito innanzitutto dalla Corte d'appello di Parigi, che, con sentenza del 14 dicembre 2011, ha negato la possibilità di appellarsi alla natura automatica del servizio onde applicare l'esenzione di responsabilità del *provider* prevista nella direttiva *e-Commerce.*

La Corte ha osservato che, come il motore di ricerca può limitare l'accesso alla pornografia e alle comunicazioni razziali, esso sarà necessariamente in grado di intervenire anche nei confronti delle associazioni di parole che risultino diffamatorie o ingiuriose. Secondo i giudici francesi *Google* non è stato in grado

[9] Cfr. Tribunale di Milano, ord. 21/25 gennaio 2011; ord. 24 marzo 2011. La decisione del Tribunale di Milano riguarda un'ipotesi di diffamazione tramite motore di ricerca: un imprenditore che pubblicizzava la sua attività anche tramite Internet, non appena digitava il proprio nome e cognome in *Google*, scopriva che il servizio di auto-completamento delle ricerche suggeriva le parole "truffa" o "truffatore". Il Tribunale di Milano ha accolto il ricorso d'urgenza volto alla rimozione di tali abbinamenti, confermando la decisione anche nell'ordinanza collegiale all'esito del reclamo.

[10] Tribunale di Milano, ord. 24 marzo 2011 (consultabile anche in personaedanno.it). Innegabile secondo il Collegio la diffamatorietà dell'associazione tra il nome del ricorrente e la parola "truffa" e "truffatore": «L'utente che legge tale abbinamento è indotto immediatamente a dubitare dell'integrità morale del soggetto il cui nome appare associato a tali parole ed a sospettare una condotta non lecita da parte dello stesso», essendo tutt'altro che dimostrato la tesi presentata da *Mountain View* secondo la quale l'utente di Internet sarebbe perfettamente in grado di discernere i contenuti offerti *on-line*.

di dimostrare che le parole suggerite sono solo il frutto di un calcolo statistico di tutte le precedenti ricerche con gli stessi termini e, data la possibilità dell'intervento, è stata riconosciuta la fondatezza della domanda attorea di risarcimento nei confronti della società[11].

Anche sul fronte tedesco la situazione non pare molto diversa: il BGH, recentemente, non solo ha richiamato il *provider Google* al miglioramento della funzione s*uggest*, ma ha anche chiarito che, nel caso in cui il motore di ricerca non si adegui alla richiesta dell'utente che si sente diffamato, la querela nei suo confronti è più che legittima[12].

Il *provider*, in base al secondo orientamento esposto, sarebbe responsabile per i suggerimenti elaborati dal servizio di auto-completamento: non si tratta di una responsabilità per le informazioni create ed immesse da terzi, o di una responsabilità per omesso controllo, ma di responsabilità connessa ad un proprio dato ovvero l'associazione di parole che grazie a tale *software* viene a costituirsi.

Sul piano strettamente penale, ancorando l'elemento soggettivo all'effettiva conoscenza[13] dell'illeceità del suggerimento, non sembrano esservi ostacoli

[11] Testo sent. in legalis.net. Per riflessioni sulla pronuncia v. TAMBURRINO C., *Google diffama suggerendo*, in punto-informatico.it, 30 Dicembre 2011; RICCIO M. G., *Suggest-ioni e inserzioni: a proposito di due recenti sentenze*, in medialaws.eu, 4 Gennaio 2012; POLLICINO O., *"Suggest search": le posizioni del giudice di Milano e di Parigi*, in diritto24.ilsole24ore.com, 23 Gennaio 2012; BIANCHI D., *Google ha diffamato per le Corti di Australia, Francia e Italia*, in personaedanno.it, 20 Novembre 2012.

[12] Cfr. BGH, sentenza 14 maggio 2013, VI ZR 269/12, in dejure.org.

[13] Secondo costante giurisprudenza della Corte di Cassazione, ai fini della sussistenza dell'elemento psicologico del reato *ex* art. 595 c.p. è sufficiente anche il dolo eventuale, ricadendo nella coscienza e volontà dell'offesa anche l'accettazione del rischio dell'offesa (cfr. *ex multis* Cass. pen., sent n. 7597/99). Nel particolare caso di diffamazione tramite la funzione di *auto-complete*, però, proprio perchè la stessa si avvale di algoritmi matematici e automatici, risulta insufficiente un'imputazione a titolo di dolo eventuale, non potendosi prescindere in tale contesto specifico dai richiami all'effettiva conoscenza dell'illeceità del dato o dell'attività presenti nel d.lgs. 70/2003 con riguardo ai *provider*. Il motore di ricerca, a parere di chi scrive, nell'ambito dell'attività di auto-completamento risulta una figura con tratti intermedi tra il *content provider* e *l'hosting provider*, pertanto il requisito soggettivo dell'effettiva conoscenza risulta essenziale per evitare una eccessiva penalizzazione in un campo in cui l'automazione del processo, prima

all'astratta configurabilità, nell'ipotesi in esame, del reato di diffamazione di cui all'art. 595 c.p.[14].

Certo, la specificità della fattispecie richiederebbe una riflessione approfondita in ordine al momento consumativo del reato o meglio al momento in cui la condotta del *provider* acquista la sua rilevanza penale[15], stante la necessità

---

dell'effettiva conoscenza grazie alla segnalazione dell'utente, rende il risultato fuori dalla sfera del "voluto".

[14] Circa la configurabilità del reato di diffamazione *on-line* cfr. *ex multis* Cassazione penale, sent. n. 4741/00; diffamazione mediante posta elettronica n. 29221/11, 44980/12; diffamazione mediante sito *web* n. 25875/96; n. 16262/08. In dottrina v. PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, cit., p. 283 ss. V. inoltre MARINI G., DI LA MONICA M., MAZZA L., *Commentario al Codice Penale*, cit., p. 539 e ss.

Da segnalare come l'art. 2, comma 3, del Disegno di legge C. 925-B, Proposta di legge: S. 1119. - COSTA: *"Modifiche alla legge 8 febbraio 1948, n. 47, al codice penale, al codice di procedura penale e al codice di procedura civile in materia di diffamazione, di diffamazione con il mezzo della stampa o con altro mezzo di diffusione, di ingiuria e di condanna del querelante nonché di segreto professionale. Ulteriori disposizioni a tutela del soggetto diffamato"*, prevede proprio la riformulazione del delitto di diffamazione in questi termini: «**Art. 595 - (Diffamazione)** *Chiunque, fuori dei casi indicati nell'articolo 594, comunicando con più persone, offende l'altrui reputazione, è punito con la multa da euro 3.000 a euro 10.000. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della multa fino a euro 15.000. Se l'offesa è arrecata con un qualsiasi mezzo di pubblicità, in via telematica ovvero in atto pubblico, la pena è aumentata della metà*». La modifica in esame renderebbe quindi esplicita la possibilità che l'offesa venga realizzata in via telematica. L'art. 3 della proposta di legge, introdotto dal Senato, prevede inoltre misure a tutela del soggetto diffamato o del soggetto leso nell'onore o nella reputazione: «1. Fermo restando il diritto di ottenere la rettifica o l'aggiornamento delle informazioni contenute nell'articolo ritenuto lesivo dei propri diritti, l'interessato può chiedere l'eliminazione, dai siti *internet* e dai motori di ricerca, dei contenuti diffamatori o dei dati personali trattati in violazione di disposizioni di legge. 2. L'interessato, in caso di rifiuto o di omessa cancellazione dei dati, ai sensi dell'articolo 14 del decreto legislativo 9 aprile 2003, n. 70, può chiedere al giudice di ordinare la rimozione, dai siti *internet* e dai motori di ricerca, delle immagini e dei dati ovvero di inibirne la diffusione. 3. I diritti di cui al comma 2 possono essere esercitati dagli eredi o dal convivente». Per un primo commento al disegno di legge in esame cfr. MONTANARI M., *Il Senato approva il ddl. in materia di diffamazione*, in penalecontemporaneo.it, 11 Novembre 2014.

[15] Quanto mai attuale sembra a tal riguardo la lucida analisi di ADORNATO C., *Il momento consumativo del reato*, Milano, 1966.

che, per i profili di automaticità della condotta, si considerino presenti tutti gli elementi richiesti dalla norma per la sussistenza del reato solo dopo la ricezione della segnalazione circa l'illeceità dei contenuti.

Purtroppo il vero sbarramento è rappresentato dal fatto che nel nostro ordinamento l'art. 595 c.p. non compare nell'elenco dei reati per i quali è prevista la relativa responsabilità degli enti ai sensi del d.lgs. 231/2001, quindi, per ora, data l'abituale struttura organizzativa complessa dei motori di ricerca, il profilarsi di una responsabilità da reato risulta precluso.

La mancanza di una interpretazione uniforme della giurisprudenza e della dottrina sulla questione esaminata rende ancora una volta evidente la necessità di un intervento legislativo.

E' interessante notare comunque come, in questo clima d'incertezza, a causa delle modalità attraverso le quali sta cambiando il volto del terrorismo, oggi più che mai dipendente dalla rete Internet per il reclutamento di nuovi adepti nonché per la diffusione della propria campagna del terrore, uno dei più famosi e popolari motori di ricerca si è di recente "censurato" e ha superato il tabù dell'automatismo della funzione di *complete*, agendo direttamente sulla stessa e rimuovendo la frase *"How can I Join ISIS"*, per evitare che la stessa diventi un vero e proprio veicolo di reclutamento di uomini per il gruppo autoproclamatosi Stato Islamico[16].

Riguardo alle altre attività poste in essere dal *provider* (*applications layer, logical layer* e *phisical layer)*, secondo orientamento ormai consolidato sia in dottrina che in giurisprudenza, troverà applicazione il normale paradigma della

[16] Cfr. SCHWARTZ B., *Google Removes "How Can I Join ISIS" Autosuggestion*, in searchengineland.com, 6 Febbraio 2015. L'ONU, tramite un recente rapporto, ha chiesto esplicitamente la collaborazione delle grandi aziende ICT per combattere ISIS ed Al-Qaeda online, ed Europol ha annunciato un piano per costituire una *task force* volta al monitoraggio della propaganda sui *social media.* V. *News: IS online: Can it be stopped?*, 22 Giugno 2015, bbc.com; *Internet companies being misused as extremist mouthpiece, say UN experts*, 25 Giugno 2015, theguardian.com.

responsabilità per fatto proprio. L'ISP, pertanto, risponderà in tutte le ipotesi in cui realizzi violazioni dirette delle norme[17].

Particolarmente interessante a tal proposito è la responsabilità per registrazione del *domain name*[18] nell'ambito della problematica concernente l'utilizzazione di Internet per fini promozionali.

E' evidente come, contrariamente al numero IP, il nome di dominio potrebbe avere in alcune circostanze rilevanza assimilabile a quella del marchio[19] qualora s'identifichi nel nome di un'azienda o di un suo prodotto o servizio[20].

La procedura di registrazione di un nome di dominio viene avviata, da parte del soggetto interessato, mediante una richiesta al *provider* designato per la loro

---

[17] Cfr. GAMBULI M., *La responsabilità penale del provider per i reati commessi in internet*, in altalex.com, 24 Ottobre 2005; INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, cit. p. 5 ss.

[18] Il nome a dominio è un indirizzo alfanumerico che consente di identificare in modo certo ed univoco una presenza (*host*) su Internet. In termini più semplici, il nome di dominio rappresenta una forma accessibile di un indirizzo alfanumerico corrispondente ad un sito Internet.

[19] Cfr. GALLI C., voce *Marchio e altri segni distintivi*, in treccani.it.

Secondo quanto disposto dall'art. 20 del Codice della proprietà industriale (d.lgs. 30/2005) il titolare del marchio registrato ha facoltà di farne uso esclusivo ed ha il diritto di vietare ai terzi, salvo proprio consenso, l'utilizzo: 1) di un marchio identico per prodotti identici; 2) di un marchio simile per prodotti affini se può creare confusione per il pubblico; 3) di un marchio identico o simile per prodotti anche diversi a patto che: a) l'uso del segno avvenga senza giusto motivo; b) l'uso del segno consenta di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o rechi pregiudizio al titolare.

I diritti di marchio d'impresa registrati non permettono invece al titolare di vietare ai terzi l'uso nell'attività economica del marchio d'impresa se tale uso si rende necessario per indicare la destinazione di un prodotto o servizio, come accessori o pezzi di ricambio, purché l'uso stesso sia conforme ai principi della correttezza professionale (art. 21 c.p.i.). L'uso deve essere tale da non ingenerare confusione o indurre in inganno il pubblico circa la natura, qualità o provenienza di prodotti o servizi e non deve ledere un altrui diritto di autore, di proprietà industriale, o altro diritto esclusivo di terzi.

[20] Cfr. *ex multis* Cassazione civile, sent. 3 dicembre 2012, n. 24620; Tribunale di Palermo, sez. spec. propr. industr. ed intell., sent. 16 ottobre 2010; Tribunale di Bologna, sez. spec. propr. industr. ed intell., sent. 14 novembre 2011 (tutte le sentenze di merito sono consultabili in GADI, Giurisprudenza annotata di diritto industriale).

gestione[21] avente ad oggetto la possibilità di registrare il *domain name* scelto e che si intende presumibilmente utilizzare. Se le condizioni per la registrazione sono rispettate e il relativo corrispettivo viene pagato, il *provider* si obbliga contrattualmente a far figurare tale nome di dominio nella sua banca dati e a collegare gli utilizzatori di Internet che lo digitano esclusivamente all'indirizzo IP indicato dal suo titolare.

Fatta eccezione per qualche isolata sentenza[22], la giurisprudenza italiana occupatosi della questione, con acume e lungimiranza, già all'inizio del nuovo millennio riconosceva una responsabilità civile del *provider* che cura la registrazione di un nome di dominio coincidente con un marchio noto[23].

---

[21] Per l'assegnazione dei nomi di dominio di primo livello generici (come .com, o .org) è competente l'*Internet Corporation for Assigned Names and Numbers* (ICANN), un ente privato che delega l'assegnazione dei nomi a dominio e la gestione dei registri ad organismi chiamati *Registry*. I nomi di dominio di primo livello .eu sono invece assegnati dall'associazione senza scopo di lucro *European Registry for Internet Domains* (EUR*id*) secondo i termini previsti dal regolamento n. 733/2002 del Parlamento europeo e del Consiglio, del 22 aprile 2002. La registrazione del *domain name* nella maggior parte dei casi viene gestita per conto degli utenti finali dai cd. *Registrar*, *provider* che offrono diversi servizi legati alla rete, dal normale *hosting* alla creazione e gestione di siti *web*. Il principio base della registrazione di un *host name* è dato dalla tempestività della registrazione, risultando di proprietà di colui che per primo lo ha registrato ("*first come, first served"*). Ciò ha portato nel corso degli anni a gravi anomalie quali l'acquisto dei nomi di dominio più semplici da ricordare al fine di rivenderne in un secondo tempo la proprietà ai soggetti interessati ad un prezzo assai più elevato rispetto a quello di registrazione, c.d. *cybersquatting* o *domain grabbing*. Come primi commenti al fenomeno cfr. *ex multis* ANTONINI A., *La tutela giuridica del nome di dominio*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2001, p. 813 ss.; CASSANO G., *Cybersquatting*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2001, p. 83 ss. V. inoltre VALLE L., *Registrazione e tutela del domain name*, in NIVARRA L, RICCIUTO V. (a cura di), *Internet e il diritto dei privati*, Torino, 2002, p. 219 ss.

[22] Cfr. Tribunale di Firenze, sent. 23 novembre 2000, con commento CASSANO G., *Una «giurisprudenza toscana» sui nomi a dominio?*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 3/2001, p. 511 ss.

[23] Ricordiamo che secondo i canoni di correttezza posti dall'art. 2598 c.c. sulla concorrenza sleale, che tra l'altro definisce come "Atto di concorrenza sleale" l'uso di nomi o segni distintivi idonei a produrre confusione con l'attività di un concorrente, si può dire che la legittimità dell'uso del marchio altrui è subordinata a due condizioni essenziali: 1) l'uso del marchio altrui deve

Pur escludendo che al *domain name* si possa attribuire una qualificazione unica[24], il loro utilizzo - diretto od indiretto - in ambito commerciale o pubblicitario ne determina una «funzione non limitata a quella di un mero indirizzo che consente tecnicamente all'utente l'accesso al sito contrassegnato, bensì anche di segno distintivo, perché volto ad attirare l'attenzione degli utenti e ad invogliarli a visitare il sito»[25].

Il *domain name* in tale contesto assume quindi la veste di strumento che concorre all'identificazione del sito e dei beni e/o servizi offerti per il suo tramite.

Tale orientamento è stato successivamente espresso anche nel Codice della proprietà industriale (CPI), approvato con d.lgs. n. 30/2005 e modificato con d.lgs. n. 131/2010, che, stante il riconoscimento del *domain name* quale segno distintivo, all'art. 22, fissa il principio di unitarietà dei segni distintivi vietando di usare anche nel nome a dominio il marchio altrui o un segno simile se, a causa

---

corrispondere ad una semplice funzione descrittiva del servizio o prodotto offerto e non ad una funzione distintiva; 2) l'utilizzo del marchio deve avvenire nel rispetto della correttezza professionale, senza che possa ingenerarsi confusione nel mercato o inganno verso il pubblico circa la natura e la provenienza del bene o del servizio offerto.

I comportamenti che risultino violativi di questi principi sono certamente violativi del c.p.i. ed al contempo costituiscono atto illecito per concorrenza sleale ai sensi dell'articolo 2598 c.c.

Cfr. *ex multis* Tribunale di Roma, ord. 22 marzo 1999, con commento SAMMARCO P., *Assegnazione dei nomi a dominio su Internet, interferenze con il marchio, domain grabbing e responsabilità del provider*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2000, p. 67; Tribunale di Firenze, sent. 21 maggio 2001 (in *Dir. industriale*, 2001, p. 393 ss.); ; Tribunale di Catania, sent. 29 giugno 2004. Cfr. inoltre CASSANO G. - BUFFA F., *Responsabilità del content provider e dell'host provider*, in altalex.com, 14 Febbraio 2003; AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, cit., p. 25 227 ss. Breve Rassegna di giurisprudenza sul fenomeno dei *domain names* in unicam.it.

[24] E' facilmente intuibile il fatto che i *domain names* non sono sempre e necessariamente dei segni distintivi, né sempre e necessariamente sono segni distintivi imprenditoriali. E' solamente analizzando il caso concreto e avendo riguardo al contenuto e alla configurazione del sito che, qualora lo stesso abbia carattere commerciale, può ben equipararsi il nome a dominio ad un segno distintivo dell'ordine del marchio d'impresa. Cfr. Tribunale di Napoli, sent. 20 dicembre 2002; Tribunale di Milano, ord. 26 marzo 2003 (in GADI).

[25] Cfr. Tribunale di Bergamo, sent. 3 marzo 2003, anche *on-line*, in interlex.it.

dell'identità o dell'affinità tra le attività d'impresa dei titolari di quei segni ed i prodotti o servizi per i quali il marchio è adottato, possa determinarsi un rischio di confusione per il pubblico. Il divieto si estende, nel caso del marchio rinomato, anche se le attività esercitate non sono affini, evidentemente in ragione della maggiore confusione che si può ingenerare[26].

In ambito penale, con riferimento alla specifica ipotesi qui in esame, si potrebbe ipotizzare il profilarsi in capo al *provider* di una responsabilità per fatto proprio ai sensi dell'art. 517 c.p.[27], che disciplina la vendita o messa in circolazione di prodotti industriali con segni mendaci e, come chiarito dalla Suprema Corte, è volto alla tutela non del marchio ma bensì dell'ordine economico inteso nei termini di regolare e pacifico svolgimento dell'attività commerciale[28].

---

[26] Art. 22 c.p.i.: «*Unitarietà dei segni distintivi* 1. E' vietato adottare come ditta, denominazione o ragione sociale, insegna e nome a dominio aziendale un segno uguale o simile all'altrui marchio se, a causa dell'identità o dell'affinità tra l'attività di impresa dei titolari di quei segni ed i prodotti o servizi per i quali il marchio è adottato, possa determinarsi un rischio di confusione per il pubblico che può consistere anche in un rischio di associazione fra i due segni. 2. Il divieto di cui al comma 1 si estende all'adozione come ditta, denominazione o ragione sociale, insegna e nome a dominio aziendale di un segno uguale o simile ad un marchio registrato per prodotti o servizi anche non affini, che goda nello Stato di rinomanza se l'uso del segno senza giusto motivo consente di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o reca pregiudizio agli stessi».

[27] Per completezza ricordiamo che, sul piano penale, sanzione specifiche in materia di proprietà industriale si rinvengono anche nello stesso CPI, all'art. 127, che comunque fa salva l'applicazione delle fattispecie di cui agli artt. 472 e 517 c.p. Cfr. FLOR R., *La tutela penale della proprietà intellettuale ed il contrasto alla commercializzazione ed alla circolazione in Internet di opere o prodotti con segni falsi o alterati*, in CAMALDO L. (a cura di), *La circolazione e il contrabbando di prodotti contraffatti o pericolosi. La tutela degli interessi finanziari dell'Unione Europea e la protezione dei consumatori. Atti del Convegno europeo svoltosi a Milano il 31 maggio 2012, organizzato dal Centro Studi di diritto penale europeo, in stretta collaborazione con OLAF (Ufficio europeo per la lotta antifrode) e con UAE (Unione degli Avvocati Europei)*, Torino, 2013, p. 118 ss.

[28] Cfr. Cass. pen., sent. 5 luglio 1989, n. 9584. In particolare, la dottrina prevalente, per ordine economico intende: l'insieme di interessi relativi alla conservazione dei beni economici

La norma si riferisce ai nomi, marchi o segni distintivi, non necessariamente registrati, che imitano quelli già adottati da un altro imprenditore e che risultano idonei ad ingenerare confusione tra i consumatori[29].

Dando rilievo sia alla condotta di "messa in vendita" che a quella di "messa in circolazione", il reato è consumato non solo nel momento materiale della *traditio* della cosa dal venditore all'acquirente ma, ancor prima, quando vi sia stata una mera attività di messa a disposizione della cosa ai potenziali acquirenti[30].

E' chiaro che un dominio simile ad un marchio che individui una determinata azienda sia, per sua stessa natura, idoneo a trarre in inganno il consumatore medio ed integrare l'elemento materiale dell'art. 517 c.p.

Tramite legge 23 luglio 2009, n. 99 è stata introdotta nel d.lgs. 231/2001 la disposizione di cui all'art. 25 *bis*, che, in modo particolare, alla lettera b) del comma 1, prevede in relazione alla commissione del delitto in esame la sanzione pecuniaria fino a cinquecento quote nonché le sanzioni interdittive di cui all'art. 9, comma 2.

Qualora nel caso concreto siano rispettati i criteri d'imputazione fissati nel d.lgs. 231/2001, in capo al *provider* che abbia curato la registrazione di un *domain name* il quale, per il riferimento ad un nome, marchio o segno distintivo, nazionale o estero, è potenzialmente idoneo ad ingenerare confusione,

---

considerati indipendentemente dal diritto di proprietà, la libertà e normalità della produzione e degli scambi, la fiducia del commercio e l'ordine del lavoro. Cfr. ANTOLISEI F., *Manuale di diritto penale. Parte speciale,* II, Quindicesima Edizione integrata e aggiornata a cura di GROSSO F. C., Milano, 2008, p. 165 ss.; PATERNITI C., voce *Economia pubblica (delitti contro)*, in *Enciclopedia Giuridica Treccani*, p. 1 ss.; PICOTTI L., voce *Invenzioni industriali. III) Tutela penale*, in *Enciclopedia Giuridica Treccani*, 1989, p. 1 ss.

[29] Cfr. Cass. pen., sent. 12 gennaio 2012, n. 11406. Il reato di vendita di prodotti industriali con segni mendaci è integrato dalla mera attitudine del marchio "imitato" a trarre in inganno il consumatore sulle caratteristiche essenziali del prodotto, non essendo necessaria né la registrazione o il riconoscimento del marchio, né la sua effettiva contraffazione né, infine, la concreta induzione in errore dell'acquirente sul bene acquistato. V. inoltre Cass. pen., sent. 30 aprile 2009, n. 23819.

[30] Cfr. Cass. pen., sent. sent. 24 maggio 1990, n. 7217.

sembrerebbe ben potersi configurare una sua responsabilità, che rileva in modo autonomo ed indipendentemente dalla condotta del gestore del sito o di colui che si occuperà materialmente della vendita dei beni.

La fattispecie si porrebbe quindi su di un piano separato rispetto al commercio elettronico di beni contraffatti, interessando una fase antecedente, ovvero quella della pubblicizzazione del prodotto.

Non sembrerebbe potersi escludere a priori la configurabilità della fattispecie mediante il richiamo ad una presunta meccanicità e automaticità del processo di registrazione. Tale aspetto dovrà infatti essere valutato secondo le circostanze specifiche della fattispecie in causa, poiché se in genere l'organismo competente per la registrazione concede o nega la stessa sulla base della mera disponibilità del nome di dominio richiesto, non mancano *provider* che richiedono certificazioni specifiche in ordine alla sussistenza o meno di un diritto del richiedente in relazione al nome scelto[31].

La ricostruzione dianzi esposta sembra perlopiù essere totalmente confutata a livello europeo.

La direttiva 2000/31/CE esclude dalle "comunicazioni commerciali" le indicazioni necessarie per accedere direttamente all'attività dell'impresa, organizzazione o persona, tra le quali il *domain name*[32], ed in una recente

[31] Basti ricordare in ambito europeo il cd. *Sunrise period*, primo periodo di registrazione dei domini .eu sfruttabile solo dai richiedenti che vantassero diritti sul nome (marchi registrati, nomi geografici, nomi di società.). La registrazione, validata dalla *PriceWaterhouseCoopers* (Belgio), un ente accreditato dall'EURid, doveva essere accompagnata da documenti che provassero tali diritti. Cfr. voce *.eu* in it.wikipedia.org.

[32] Art. 2 della direttiva 2000/31/CE: «Ai fini della presente direttiva valgono le seguenti definizioni: (…) f) "comunicazioni commerciali": tutte le forme di comunicazione destinate, in modo diretto o indiretto, a promuovere beni, servizi o l'immagine di un'impresa, di un'organizzazione o di una persona che esercita un'attività commerciale, industriale, artigianale o una libera professione. Non sono di per sé comunicazioni commerciali: –le indicazioni necessarie

pronuncia in materia di pubblicità ingannevole[33], la Corte di Giustizia dell'Unione europea ha affermato che nella nozione di "pubblicità" definita, ai sensi delle direttive 84/450 e 2006/114, quale «qualsiasi forma di messaggio che sia diffuso nell'esercizio di un'attività commerciale, industriale, artigianale o professionale, allo scopo di promuovere la fornitura di beni o servizi»[34], può essere ricompreso solo l'utilizzo del nome a dominio o dei *metatag*, ma non l'operazione di registrazione.

Questo apparente contrasto tra ricostruzione italiana e orientamento europeo è rivelato nella stessa sentenza al punto 33, in cui si chiarisce che «Fatta eccezione per la BEST e per il governo italiano, tutte le parti in causa davanti alla Corte, ossia il sig. Peelaers e la Visys, i governi belga, estone e polacco, nonché la

---

per accedere direttamente all'attività di tale impresa, organizzazione o persona, come un nome di dominio ("domain name") o un indirizzo di posta elettronica, (…)».

[33] Cfr. CGU, sent. 11 luglio 2013, C-657/11. La controversia che ha dato luogo alla domanda di pronuncia pregiudiziale, proposta alla Corte dallo *Hof van Cassatie* (Belgio), concerne per l'appunto l'utilizzazione di Internet per fini promozionali. Alla Corte di Giustizia è stato chiesto se la nozione di "pubblicità" come prevista dall'articolo 2, numero 1, della direttiva 84/450/CEE, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di pubblicità ingannevole e dal corrispondente articolo 2, lettera a), della direttiva 2006/114/CE, concernente la pubblicità ingannevole e comparativA, per determinare se tale nozione comprenda, da un lato, la registrazione e l'uso di un nome di dominio e, dall'altro lato, l'uso di *metatags*. Questi ultimi sono parole codificate nel codice sorgente di un sito Internet. Quando viene effettuata una ricerca in linea mediante un motore di ricerca, i *metatags* sono da essi riconosciuti e contribuiscono a determinare l'ordine di visualizzazione dei vari siti Internet identificati da detto motore come quelli corrispondenti alla ricerca dell'utente. Esistono in linea di principio due tipi di metatags: i "*metatags* descrittivi" (*meta description tag*), che descrivono il contenuto di un sito, e i "*metatags* parole chiave" (*key words metatags*), che consistono in una serie di parole chiave che fanno riferimento al contenuto del sito stesso. La controversia dinanzi al giudice del rinvio riguardava l'utilizzo della seconda tipologia di *metatags*. Cfr. voce *Meta tag* in wikipedia.org.

[34] L'articolo 2, numero 1, della direttiva 84/450, ripreso *expressis verbis* dall'art. 2, lettera a), della direttiva 2006/114, stabilisce quanto segue: «Ai sensi della presente direttiva si intende per 1) "pubblicità", qualsiasi forma di messaggio che sia diffuso nell'esercizio di un'attività commerciale, industriale, artigianale o professionale, allo scopo di promuovere la fornitura di beni o servizi, compresi i beni immobili, i diritti e gli obblighi (…)».

Commissione europea, ritengono che la registrazione di un nome di dominio non possa essere qualificata come pubblicità»[35].

In modo particolare nella pronuncia si definisce la registrazione del *domain name* come un atto meramente formale, il quale, di per sé stesso, non implica necessariamente che questo verrà poi effettivamente utilizzato per creare un sito Internet e quindi sarà conosciuto dai potenziali consumatori. Risultando per tale motivo inidonea ad influenzare le scelte di questi ultimi, la registrazione non costituirebbe in sé comunicazione pubblicitaria-commerciale, ma, producendo l'effetto di privare i concorrenti della possibilità di registrare e di utilizzare quel nome di dominio per i propri siti, potrà all'occorrenza, essere inibita ai sensi di altre disposizioni giuridiche[36].

In realtà a parere di chi scrive, il mancato effettivo utilizzo del *domain name* registrato, lungi dal declassare l'operazione di registrazione in mera attività formale, rileverà sul piano dell'accertamento processuale delle responsabilità.

Ad esempio, con particolare riguardo alla fattispecie di cui all'art. 517 c.p., ed alla sua configurabilità in capo al *provider*, il mancato utilizzo del *domain name* per la creazione di un sito, renderà la registrazione penalmente irrilevante per mancanza di tipicità della condotta che si arresterebbe nella fase degli atti preparatori non punibili.

Indipendentemente dalla ricostruzione del delitto in esame in termini di reato di pericolo, ovvero di danno[37], non venendo gli utenti a conoscenza del *domain* sarà totalmente assente un qualsiasi pericolo di inganno del pubblico.

---

[35] Cfr. CGU, sent. 11 lugio 2013 2001, C-657/11, punto 33.

[36] *Ivi*, punto 43, 44.

[37] Da segnalare come sul punto dottrina e giurisprudenza non siano ancora giunte ad una ricostruzione unanime. Cfr. Cass. pen., sent. 25 gennaio 1960; *contra* Cass. pen., sent. n. 238557/2007. La questione risulta tutt'altro che irrilevante comportando ad esempio soluzione diametralmente opposte in tema di tentativo. Cfr. *ex multis* Cass. pen., sent. n. 26754/01; 23514/06; 28732/06.

Come più volte sancito dalla Corte Costituzionale il principio di offensività opera sia sul piano delle previsioni normative (offensività in astratto), che su quello dell'applicazione giudiziale (offensività in concreto)[38]. Nella veste di canone interpretativo-applicativo affidato al giudice esso impone l'accertamento, volta per volta, che il comportamento, per di più ove solo astrattamente pericoloso e dunque apparentemente carente di note di lesività, abbia raggiunto un *minimum* di offensività nella fattispecie oggetto di giudizio. Se la condotta risulta assolutamente inidonea a porre a repentaglio il bene giuridico tutelato verrà meno la stessa riconducibilità della fattispecie concreta a quella astratta.

b) Ipotesi di concorso

A tutti i livelli dell'Internet *provision*, fatte salve le esenzioni di responsabilità previste nel d.lgs. n. 70/2003, il concorso del *provider* nell'altrui illecito ai sensi dell'art. 110 c.p. sembrerebbe astrattamente configurabile, pur non senza dimenticare che il modello unitario di disciplina del concorso di persone nel reato rischia, ancor più nella rete, di condurre a effetti di dilatazione della responsabilità penale eccessivi[39].

---

[38] Cfr. *ex multis* Corte Costituzionale, sent. n. 437/89; 333/91; 519/00; 265/05; in senso conforme Cass. pen., S.U., n. 28605/08. Sulla "costituzionalizzazione" del principio di offensività v. VINCIGUERRA S., *Appunti sull'inoffensività, la tenuità dell'offesa e la tenuità del reato in Italia nel secondo Novecento*, in DOLCINI E., PALIERO C. E. (a cura di), *Studi in onore di Giorgio Marinucci*, Tomo II, Milano, 2006, p. 2078 ss.

In dottrina, data la vastità degli scritti occupatesi del principio di offensività, si consenta il rinvio, anche per la bibliografia di riferimento, al recente contributo del prof. DONINI M., *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in penalecontemporaneo.it, 20 Settembre 2013.

[39] Così PICOTTI L., *Internet e responsabilità penali*, in PASCUZZI G. (a cura di), *Diritto e informatica: l'avvocato di fronte alle tecnologie digitali*, Milano, 2002, p. 115 ss. In riferimento alle accuse di carenza di precisione nella valutazione sia dell'*an* che del *quantum* insita nel modello unitario o cd. della pari responsabilità dei concorrenti fissato nella formula di cui all'art. 110 c.p. cfr. DONINI M., *La partecipazione al reato tra responsabilità per fatto proprio e responsabilità per fatto altrui*, in *Rivista italiana di diritto e procedura penale*, 1984, p. 175 ss. Tra le recenti monografie sul tema v., anche per i richiami alla vasta e autorevole dottrina

In effetti, proprio nel concorso di persone emergono già di per sé gravi pericoli per il principio di riserva di legge, di tassatività e di personalità[40].

In base alla concezione unitaria del concorso di persone l'attività costitutiva può essere rappresentata da qualsiasi comportamento esteriore che fornisca un apprezzabile contributo[41] alla realizzazione collettiva del reato, in tutte o alcune delle fasi di ideazione, organizzazione ed esecuzione. Rileverà pertanto anche il mero rafforzamento dell'altrui proposito criminoso o l'agevolazione dell'opera dei concorrenti, senza la necessità che tra gli stessi vi sia un preventivo accordo, ritenendosi integrato l'elemento soggettivo dalla consapevolezza unilaterale del contributo recato alla condotta altrui[42].

Ove si mettano in relazione tali principi alle caratteristiche della rete ed al ruolo sempre più attivo degli utenti, il rischio di pan-penalizzazione sembra ancora più allarmante.

La concreta definizione dei contributi degli ISP da ricondurre all'alveo della responsabilità concorsuale desta quindi forti preoccupazioni.

---

occupatosi della questione, BIANCHI M., *Concorso di persone e reati accessori*, Torino, 2013. Per uno sguardo "storico" della norma in esame v. VASSALLI G., *Note in margine alla riforma del concorso di persone nel reato*, in DOLCINI E., PALIERO C. E. (a cura di), *Studi in onore di Giorgio Marinucci*, cit., p. 1939 ss.

[40] Sul punto cfr. BRICOLA F., *La discrezionalità nel diritto penale*, Milano, 1965, p. 157 ss.

[41] La giurisprudenza maggioritaria ha accolto il criterio della causalità agevolatrice, secondo il quale il contributo concorsuale assume rilevanza non solo quando abbia efficacia causale, ponendosi come condizione dell'evento lesivo, ma anche quando assuma la forma di contributo agevolatore ovvero quando il reato, senza quella particolare condotta, sarebbe stato ugualmente commesso ma con maggiore incertezza di riuscita o difficoltà. Cfr. Cass. pen., sent. n. 36818/12. Per un'analisi specifica sul tema cfr. AZZALI G., *Concorso di persone nel reato. La prospettiva causale*, in DOLCINI E., PALIERO C. E. (a cura di), *Studi in onore di Giorgio Marinucci*, cit., p. 1351 ss.

[42] Cfr. *ex multis* Cass. pen., sent. n. 18745/13; 11452/05; 40449/09.

L'interrogativo centrale della questione verte sull'identificazione del *quid pluris* che determina l'impossibilità di applicare l'esenzioni di cui al d.lgs. n. 70/2003 e qualifica la condotta come agevolatrice rispetto al reato.

Data l'essenzialità dell'attività del *provider* per ottenere l'utilizzo della rete ed i suoi servizi, dal punto di vista oggettivo, nei casi di travalicamento della soglia d'irresponsabilità di cui al d.lgs. n. 70/2003, il contributo causale sembrerebbe sussistere: «Il collegamento in rete, mediante la connessione fisica al *server* (od *hardware*); la predisposizione e messa a disposizione del *software* che ne rende possibile in ogni momento l'accesso; infine la costante fornitura di servizi ed interventi che garantiscono la concreta "tenuta a disposizione" per l'utilizzazione - anche in termini di ulteriore trasmissione, circolazione e scambio - dei dati e contenuti informativi o comunicativi in questione, rappresentano di certo un *contributo oggettivo* di partecipazione penalmente rilevante, in quanto avente natura causale o quantomeno agevolatrice, rispetto alla realizzazione di fatti illeciti, con tali mezzi, da parte degli autori […] Un tale contributo, in quanto *conditio sine qua non* della comunicazione o diffusione, può quindi fondare una responsabilità penale per partecipazione commissiva, ovviamente accanto agli altri requisiti oggettivi e soggettivi richiesti dall'ordinamento, pur di fronte alla possibilità di libera *scelta* di accesso da parte dell'utente»[43].

Sarà quindi il dolo di partecipazione a svolgere la funzione di vero e proprio discrimine tra contributi rilevanti e non ma, le difficoltà insite nelle complesse indagini in ordine al requisito subiettivo correlato ad attività che nella maggior parte dei casi sono perlomeno parzialmente automatizzate, amplificano il potere discrezionale del giudice ed il rischio di pronunce diametralmente opposte è latente[44].

Sembra comunque potersi affermare che, in virtù della disciplina fissata nel d.lgs. n. 70/2003 ed al particolare accento che il legislatore pone sulla effettiva

[43] Cfr. PICOTTI L., *La responsabilità penale dei service-providers in Italia*, in *Diritto penale e processo*, n. 3/1999, p. 501 ss.

[44] Cfr. PICOTTI L., *Internet e responsabilità penali*, cit., p. 122 ss.

conoscenza dell'illeceità dell'attività, dovrebbe essere esclusa la rilevanza del dolo nella sua forma eventuale. L'*actual knowledge* implicherebbe infatti una piena consapevolezza corrispondente esclusivamente a quella del dolo diretto[45].

Per la precipua caratteristica di meccanicità dei servizi offerti dal *provider* e la vastità di dati da esso gestiti, la configurabilità del dolo eventuale determinerebbe per lo più l'apoptosi dello stesso elemento soggettivo e la sua trasformazione, a livello processuale, in una sorta di *dolus in re ipsa*[46].

E' necessario rilevare che il requisito dell'effettiva conoscenza determina anche l'impossibilità del profilarsi di un concorso anomalo ex art. 116 c.p.

Per la sua sussistenza, infatti, oltre all'adesione psichica dell'agente ad un reato meno grave e alla commissione, da parte di un altro compartecipe, di un reato diverso e più grave, è necessario anche un nesso psicologico in termini di prevedibilità dell'evento diverso in concreto verificatosi[47].

L'astratta rappresentazione nell'agente del reato più grave non voluto come sviluppo logicamente prevedibile richiede una consapevolezza "inferiore" rispetto all'accettazione del rischio del verificarsi dell'evento caratteristica della forma del dolo eventuale, e risulta quindi ancor più inconciliabile al grado di piena conoscenza fissata nel d.lgs. n. 70/2003.

Problematiche risultano infine le ipotesi di concorso colposo dell'ISP nel delitto doloso dell'utente[48] e di una cooperazione nel delitto colposo ex art. 113 c.p[49].

---

[45] Cfr. INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, cit., p. 19, in modo particolare nota 93-94.

[46] Cfr. PICOTTI L., *Commento Art. 600-ter, III comma, c. p. (Pornografia minorile)* in CADOPPI A. (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006, p. 175 ss.; FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, cit., p. 464 ss.

[47] Cfr. *ex multis* Cass. pen., sent. n. 20649/10; S.U. 337/09.

[48] Ricordiamo che per molti autori, stante il dettato dell'art. 42 c.p., il concorso colposo nel delitto doloso non sarebbe nemmeno configurabile a meno che il legislatore intervenga

In entrambe i casi è innanzitutto necessario che il reato sia previsto anche nella forma colposa (diversamente sarebbe violato il disposto dell'art. 42, comma 2, c.p., secondo il quale nessuno può essere punito per un fatto preveduto dalla legge come delitto, se non l'ha commesso con dolo, salvo i casi di delitto preterintenzionale o colposo espressamente preveduti dalla legge) e che nella sua condotta siano effettivamente presenti tutti gli elementi che caratterizzano la colpa[50].

Se da un lato l'effettiva conoscenza determina la non configurabilità del mero concorso di cause indipendenti tra loro[51], dall'altro, la rilevanza del contributo colposo dell'ISP al reato doloso o colposo realizzato dall'utente, presuppone la sussistenza di specifiche discipline cautelari riferibili alla rete.

Gli *standards* di comportamento, attraverso i quali vagliare le condotte ai sensi dell'art. 43 c.p. e fondare il rimprovero "generico" di negligenza, imprudenza, imperizia, o quello di "colpa specifica", potrebbero essere rintracciati nei cd. codici di condotta o di auto-regolamentazione che tentano di armonizzare le varie regole di condotta, settore per settore, per renderle riconoscibili e possibilmente comuni a tutti *providers*[52].

---

tassativizzandolo. Cfr. MANTOVANI F., *Diritto penale. Parte generale*, Ottava Edizione, Padova, 2013, p. 545 ss.

[49] La cooperazione nel delitto colposo ex art. 113 c.p. si verifica quando più persone pongono in essere una condotta nella reciproca consapevolezza di contribuire all'azione od omissione altrui, cagionando, infine, l'evento non voluto. Ciascun cooperante *ex* art. 113, difatti, deve essere unicamente consapevole dell'esistenza di quell'azione altrui, che lede, in concomitanza con la propria condotta, un bene giuridico penalmente rilevante.

[50] Cfr. *ex multis* Cass. pen., sent. n. 34385/2011.

[51] Nella cooperazione le volontà dei soggetti devono tutte confluire consapevolmente all'interno della condotta da cui derivi l'evento non voluto; nei casi, invece, di concorso di cause indipendenti l'evento consegue a una mera coincidenza di azioni o omissioni, non collegate da alcun vincolo soggettivo. E' il profilo psicologico della consapevolezza dell'altrui condotta che quindi distingue le due ipotesi. Cfr. *ex multis* Cass. pen., sent. n. 6215/2010.

[52] Per una riflessione comparativa sui codici di condotta v. TROPINA T., CALLANAN T., *Self- and co-regulation in cybercrime, cybersecurity and national security*, Cham-Heidelberg, 2015; ZICCARDI G., *Internet provider, computer ethics e codici di auto-regolamentazione della condotta*, in LUPARIA L. (a cura di), *Internet Provider e Giustizia Penale*, cit., p. 179 ss.; MARSDEN C. T., *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*,

Le pronunce giurisprudenziali italiane occupatesi del concorso del *provider* nell'altrui reato si sono in realtà concentrate tendenzialmente non tanto sull'elemento soggettivo quanto su quello oggettivo.

Si è registrata infatti una tendenza, certo non sempre lineare, a rintracciare il *quid pluris* idoneo a qualificare la condotta dell'ISP in termini di contributo ai sensi dell'art. 110 c.p. tramite particolari indici rivelatori della "non passività" del *provider*, per sè stessi idonei ad impedire l'applicazione delle esenzioni di cui al d.lgs. n. 70/2003[53].

Cambridge, 2011, p. 39 ss.; BRUNST P., SIEBER U., *Cybercrime Legislation in Germany* in BASEDOW J., KISCHEL U., SIEBER U., (eds.), *German National Reports to the XVIII International Congress of Comparative Law*, 2010, p. 789 ss.

[53] Cfr. *ex multis* Cassazione penale, sent. 29 settembre 2009, n. 49437, caso *The Pirate Bay* con la quale è stato confermato il sequestro del sito che permetteva lo scambio di opere coperte dal diritto d'autore: «Se il sito *web* si limitasse a mettere a disposizione il protocollo di comunicazione (quale quello *peer-to-peer*) per consentire la condivisione di file, contenenti l'opera coperta da diritto d'autore, ed il loro trasferimento tra utenti, il titolare del sito stesso sarebbe in realtà estraneo al reato. Però se il titolare del sito non si limita a ciò, ma fa qualcosa di più - ossia indicizza le informazioni che gli vengono dagli utenti, che sono tutti potenziali autori di *uploading*, sicchè queste informazioni (i.e. chiavi di accesso agli utenti periferici che posseggono, in tutto o in parte, l'opera), anche se ridotte al minimo, ma pur sempre essenziali perchè gli utenti possano orientarsi chiedendo il *downloading* di quell'opera piuttosto che un'altra, sono in tal modo elaborate e rese disponibili nel sito, ad es. a mezzo di un motore di ricerca o con delle liste indicizzate - il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati. C'è un *quid pluris* in quanto viene resa disponibile all'utenza del sito anche una indicizzazione costantemente aggiornata che consente di percepire il contenuto dei file suscettibili di trasferimento. A quel punto l'attività di trasporto dei *file* (*file transfert*) non è più agnostica; ma si caratterizza come trasporto di dati contenenti materiale coperto da diritto d'autore. Ed allora è vero che lo scambio dei file avviene da utente ad utente (*peer-to- peer*), ma l'attività del sito *web* (al quale è riferibile il protocollo di trasferimento e l'indicizzazione di dati essenziali) è quella che consente ciò e pertanto c'è un apporto causale a tale condotta che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone ex art. 110 c.p.». V. inoltre Tribunale di Milano, sent. 20 gennaio 2001, n. 6096; Tribunale di Milano, sent. 19 maggio 2011, n. 8748; Tribunale di Roma, ord. 22 marzo 2011, con nota di GIOVANELLA F., *La responsabilità per linking*

L'addebito all'ISP di una responsabilità per concorso nel reato posto in essere dagli utenti che ne sfruttano i servizi è stato ancorato ad una serie di attività.

I *safe harbours* sono stati applicati solamente nei casi di totale neutralità e passività degli intermediari, sul presupposto che i considerando 42 e 44 della direttiva 2000/31/CE escludono la compatibilità delle esenzioni in essa previste con indici di supposta "attività", stabilendo testualmente che «le deroghe alla responsabilità […] riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate»[54] e che «il prestatore che deliberatamente collabori con un destinatario del suo servizio al fine di commettere atti illeciti non si limita alle attività di semplice trasporto *("mere conduit"*) e di *"caching"* e non può pertanto beneficiare delle deroghe in materia di responsabilità previste per tali attività»[55].

In realtà questo filone di pronunce sembra basato su un'erronea lettura della direttiva 2000/31/CE. Infatti i *Considerando* 42 e 44 si occupano segnatamente di *mere conduit* e di *caching providers*. L'attività di *hosting* risulta perlopiù trattata specificatamente nel considerando 46, che fissa la regola secondo la quale «per godere di una limitazione della responsabilità, il prestatore di un servizio della società dell'informazione consistente nella memorizzazione di informazioni deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso alle medesime non appena sia informato o si renda conto delle attività illecite», e successivamente dettagliata nell'art. 14.

---

a files audiovisivi contraffatti e l'incerta natura del motore di ricerca, , in *Danno e Responsabilità,* n. 8-9/2011, p. 847 ss.

[54] Dir. 2000/31/CE, Considerando 42.

[55] Dir. 2000/31/CE, Considerando 44.

La possibilità di creare una categoria di intermediari atipici che, proprio per la modalità di gestione dei contenuti offerti dagli utenti, ad esempio attraverso indicizzazione automatica, non dovrebbe essere assimilata nè agli *hosting providers* puri nè ai *content providers*[56], e comunque resterebbe estranea alla disciplina de d.lgs. n. 70/2003, è stata di recente esclusa dalla Corte d'appello di Milano[57], la quale ha dato pienamente voce alla lettura della direttiva 2000/31/CE da ultimo esposta.

Si tratta di una decisione destinata a fare giurisprudenza avendo stabilito con forza che l'offerta da parte dell'*hoster* di funzionalità accessorie non può escludere l'applicabilità del regime di limitazione della responsabilità del d.lgs. 70/2003.

La pronuncia in esame si uniforma all'orientamento della Corte di Giustizia dell'Unione Europea che, come approfondiremo nel prossimo capitolo, è incline ad escludere l'ammissibilità di un *hosting provider* di natura ibrida ed a ritenere l'intermediario responsabile dei contenuti pubblicati solamente ove, ricevuta una

[56] Cfr. in modo particolare giurisprudenza e dottrina in merito al reato di cui all'art. 600 *ter*, comma 3, c.p.: PICOTTI L., *Commento Art. 600-ter, III comma, c. p. (Pornografia minorile)*, cit.; RESTA F., *Diffusione telematica della pedopornografia. Pedopornografia on-line. Verso un sistema di tutela a strategia integrata?*, in *Diritto dell'internet*, n. 3/2007, p. 221 ss.; DE NATALE D., *Attività di contrasto alla pedopornografia online: aspetti problematici della responsabilità delle persone fisiche e degli enti*, in *Rivista trimestrale di diritto penale dell'economia*, n. 22/2009, p. 793 ss.; ID., *Attività di contrasto alla pedopornografia on line: aspetti problematici della responsabilità delle persone fisiche e degli enti (parte seconda)*, in *Rivista trimestrale di diritto penale dell'economia*, n. 23/2010, p. 1 ss.

In riferimento alla responsabilità concorsuale in tema di diritto d'autore v. FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, cit., p. 460 ss.; nonché Tribunale di Roma, ord. 17 agosto 2011; Tribunale di Roma, ord. 20 ottobre 2011.

[57] Corte d'appello di Milano, sez. spec. in materia d'impresa, sent. 29/2015, in riforma della sent. del Tribunale di Milano n. 10893/2011. A commento v. BELLEZZA M., *Yahoo! Vs RTI: a new era for ISP's liability in Italy?*, in medialaws.eu, 26 Gennaio 2015; BASSINI M., POLLICINO O., *Evoluto, ma non attivo. La Corte d'appello di Milano travolge la più recente giurisprudenza sull'hosting*, in diritto24.ilsole24ore.com, 27 Gennaio 2015.

segnalazione qualificata, puntuale e circoscritta, non si sia adoperato per porre fine alla violazione[58].

Purchè l'*hoster* non partecipi all'elaborazione dei contenuti, trasformandosi in un vero e proprio *content provider*, la disapplicazione delle tutele previste nella direttiva *e-Commerce* non risulterebbe legittima, essendo errata l'individuazione di una sottocategoria di *provider* definibili come "attivi" in virtù della complessità dei servizi offerti o del particolare interesse del gestore a conseguire vantaggi economici[59].

Alla luce di quanto esposto potremmo dunque affermare che i *safe harbours* di cui al d.lgs. 70/2003 non opereranno rendendo ammissibili la configurabilità di un concorso, fermo restando la necessaria sussistenza degli altri requisiti previsti ex art. 110 c.p., nell'attività di trasporto o memorizzazione temporanea qualora l'ISP ne controlli o gestisca il contenuto prestando un servizio non meramente tecnico e neutro, mentre, nell'attività di memorizzazione di informazioni, ove sussista l'*actual knowledge* o la *awareness*[60].

---

[58] V. CGU, C-236/08, C-238/08 (caso *Google* c. *Louis Vuitton*); C-328/09 (caso *L'Oreal* c. *Ebay*); C-70/10 (caso *Scarlet Extended* c. *Sabam*); C- 360/10 (caso *Sabam* c. *Netlog*); C-314/12 (*UPC Telekabel Wien GmbH* c. *Constantin Film Verleih GmbH* e *Wega Filmsproduktionsgesellschaft mbH*).

[59] Cfr. Cassazione penale, sent. 3 settembre 2014, n. 5107: in mancanza della prova di un contributo specifico alla determinazione del contenuto del video illecito caricato dall'utente, che renderebbe il *provider* responsabile come coautore dello stesso, e della conoscenza effettiva della sua illeceità, la semplice ospitalità del video tramite servizio offerto dall'operatore *Google Video*, indipendentemente dalle funzionalità offerte ne determina l'irresponsabilità, dovendo trovare applicazione l'esenzione di cui al d.lgs. 70/2003. In prospettiva comparatistica v. Tribunale di Parigi, sent. 29 maggio 2012, con nota di SAMMARCO P., *Il ruolo di YouTube tra intermediario del commercio elettronico e fornitore di servizi di media audiovisivi*, in *Il Diritto dell'Informazione e dell'Informatica*, 2012, p. 965.

[60] In termini comparatistici v. *England and Wales Court of Appeal*, sent. 14 febbraio 2013, *Tamiz* v. *Google Inc.*, con nota di SCANNICCHIO T., *La responsabilità del provider di fronte alle corti inglesi: una vittoria di Pirro per Google?*, in *Il Diritto dell'Informazione e dell'Informatica*, 2013, p. 751 ss. Secondo la Corte, in seguito al momento in cui è notificata la presenza del materiale diffamatorio, l'ISP si rende responsabile divenendo "co-editore" del materiale stesso laddove non lo elimini.

2. RESPONSABILITÀ OMISSIVA

Una forma di responsabilità omissiva dei prestatori di servizi sarebbe configurabile se, a fronte della normativa vigente, potesse affermarsi la sussistenza di un obbligo di garanzia[61], presupposto d'applicabilità dell'art. 40, comma 2, c.p., il quale comporterebbe la punibilità a titolo autonomo (nel caso dei reati a forma libera) o, combinandosi con la disposizione di cui all'art. 110 c.p., per concorso omissivo nel reato realizzato dagli utenti[62].

La responsabilità per mancato impedimento dell'illecito altrui non può che avere un carattere eccezionale: «se il garante dispone di un potere di signoria sul decorso causale ed è quindi in grado di impedire attivandosi il verificarsi dell'evento, ciò normalmente non si verifica quando causa dell'evento è l'azione di un altro soggetto. La condotta umana, infatti, si svolge di regola al di fuori del potere di controllo di una persona diversa dall'agente […] E' possibile affermare che l'Hintermann sia concretamente in grado di impedire il fatto illecito di terzi

[61] Stante l'esigenza di economia espositiva sembra comunque opportuno ricordare sinteticamente che la posizione di garanzia costituisce uno speciale vincolo di tutela intercorrente tra un soggetto garante ed un determinato bene giuridico. Si suole distinguere tra posizione di garanzia cd. *di protezione*, il cui fine è quello di preservare il bene da tutti i pericoli che ne possono minacciare l'integrità, e posizione di garanzia cd. *di controllo*, avente lo scopo di neutralizzare determinate fonti di pericolo. Cfr. FIANDACA G., MUSCO E., *Diritto penale. Parte generale*, cit., p. 584 ss.; ANTOLISEI F., *Manuale di diritto penale. Parte generale*, cit., p. 255 ss.; Cfr. MANTOVANI F., *Diritto penale. Parte generale*, cit., p. 132 ss.

[62] Cfr. MINOTTI D., *Responsabilità penale: il provider è tenuto ad "attivarsi"?*, in interlex.it, 5 Maggio 2003; IANNI V., *La responsabilità in sede penale dell'internet service provider alla luce dei più recenti decisa giurisprudenziali*, in neldiritto.it., 1 Marzo 2011. Per le restrizioni del campo di operatività del concorso mediante omissione in un reato commissivo v. FIANDACA G., *Il reato commissivo mediante omissione*, Milano, 1979, p. 179 ss., nonché *contra* GRASSO G., *Il reato omissivo improprio*, Milano, 1983, p. 141 ss. Secondo l'autore escludere nel caso di concorso omissivo nel reato attivo le fattispecie di mera condotta è un'operazione priva di fondamento testuale e razionale: le limitazioni alla responsabilità omissiva potranno solamente fondarsi avendo riguardo alla posizione di garanzia. Il richiamo alla fattispecie causalmente orientata sarà quindi necessario solo in relazione alle ipotesi monosoggettive.

solo nel caso in cui - per particolari circostanze specificatamente rilevati - l'aggressore sia nella sfera di controllo del garante»[63].

Per parte della dottrina e della giurisprudenza[64] la responsabilità *per omissionem* dell'ISP incontra ostacoli insuperabili: la posizione di garanzia in questione non troverebbe base giuridica *de iure condito* e sarebbe per lo più necessariamente causativa di un obbligo "preventivo" di controllo dei contenuti trasmessi che si rivelerebbe *sempre* del tutto inesigibile per l'impossibilità materiale ed effettiva di gestione del flusso[65] e per l'inefficacia dell'intervento del *provider*[66]. Tale controllo, inoltre, violerebbe il divieto di assoggettare i *providers*

---

[63] Cfr. RISICATO L., *La partecipazione mediante omissione a reato commissivo*, cit., p. 1281.

[64] Cfr. in modo particolare le decisioni del caso *Google v. Vivi Down*: Tribunale di Milano, sent. 12 aprile 2010, n. 1972 con nota di ROSSELLO C., *Riflessioni de jure condendo in materia di responsabilità del provider*, in *Il Diritto dell'Informazione e dell'Informatica*, 2010, p. 617 ss.; PEZZELLA V., *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, in *Giurisprudenza di merito*, n. 9/2010, p. 2232 ss.; CAJANI F., *Quella Casa nella Prateria: gli Internet Service Providers americani alla prova del caso Google Video*, in PICOTTI L., RUGGIERI F. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Milano, 2012, p. 223 ss. Corte d'Appello di Milano, sent. 27 febbraio 2013, n. 8611 con nota di BASSOLI E., *Esclusa la responsabilità penale di Google per violazione di dati personali da parte di materiale multimediale immesso da terzi*, in *Rivista penale*, n. 5/2013, p. 558 ss.; RESTA F., *Libertà della rete e protezione dei dati personali: ancora sul caso Google-Vivi Down*, in *Il Diritto dell'Informazione e dell'Informatica*, 2013, p. 502 ss.; INGRASSIA A., *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali*, in penalecontemporaneo.it, 4 Marzo 2013. Cassazione penale, sent. 17 dicembre 2013, n. 5107, con nota di INGRASSIA A., *La sentenza della Cassazione sul caso Google*, in penalecontemporaneo.it, 6 Febbraio 2014.

[65] Si consideri inoltre che nel settore specifico della corrispondenza privata l'inesigibilità del controllo è connessa al fatto che lo stesso integrerebbe la fattispecie di cui all'art. 616 c.p. In tal senso cfr. COSTANZO P., *Aspetti evolutivi del regime giuridico di Intenet*, in *Il Diritto dell'Informazione e dell'Informatica*, 1996, p. 831 ss. V. inoltre SEMINARA S., *La pirateria su Internet e il diritto penale*, cit., p. 99 ss.; SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer*, cit., p. 1219 ss.

[66] Gli utenti possono, nella maggior parte dei casi, accedere ai medesimi contenuti tramite altri siti *web* o altri *server*. Cfr. CAMMARATA M., *Il diavolo nel sito e il provider diventa esorcista*, in interlex.it, 16 Luglio 1998: «Comunque tutto questo non eviterebbe che il diavolo esorcizzato

ad un obbligo generale di sorveglianza dei contenuti immessi dagli utenti di cui all'art. 15 della direttiva *e-Commerce*[67].

Con particolare riguardo ai reati di condotta che si consumano nel momento in cui i dati illeciti sono resi disponibili dall'utente, la partecipazione dell'intermediario non sarebbe ravvisabile né per l'omessa cancellazione né per il mantenimento degli stessi *on line*: trattandosi in entrambe i casi di condotte susseguenti la realizzazione del reato mancherebbe la necessaria sussistenza del nesso causale[68]. Non solo, nei reati di pura condotta, l'obbligo di impedire l'evento coinciderebbe con quello di impedire il reato, comportando un'inaccettabile equiparazione, attraverso un'interpretazione analogica *in malam partem*, tra *provider* e agenti di polizia, ai quali esclusivamente si riferisce l'art. 55 c.p.p.[69].

In linea generale, quindi, la responsabilità del fornitore di servizi in relazione agli illeciti realizzati dagli utenti sarebbe configurabile solamente nella forma del concorso commissivo. Inutile infatti il paradigma dell'omissione ove si sostenga che il contributo dell'ISP sia causalmente efficiente rispetto al fatto tipico qualora egli abbia la possibilità tecnica e giuridica di controllare preventivamente i contenuti immessi dai terzi e, pur essendo a conoscenza della loro illiceità, decida consapevolmente e volontariamente di non attivarsi: «è già l'azione di per sé neutra della fornitura del servizio, arricchita e qualificata dalla presenza del dolo, a costituire un contributo di partecipazione (attiva) rilevante per la commissione del reato»[70].

---

da un server possa immediatamente comparire su altri dieci o cento siti della Rete. Il che confermerebbe la visione di quelli che vedono Internet come un'invenzione diabolica, mentre si tratta solo del primo mezzo di comunicazione sul quale non può funzionare alcun tipo di censura». V. inoltre SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer*, cit., p. 1219.

[67] Cfr. MANNA A., *I soggetti in posizione di garanzia*, in *Il Diritto dell'Informazione e dell'Informatica*, 2010, p. 779.

[68] Cfr. SEMINARA S., *La responsabilità penale degli operatori su Internet*, cit., p. 766.

[69] Cfr. MANNA A., *I soggetti in posizione di garanzia*, cit., p. 790.

[70] Cfr. SPAGNOLETTI V., *La responsabilità del provider per i contenuti illeciti in internet*, cit. L'autrice sostiene inoltre che, eventualmente, in assenza dell'elemento dell'accordo tra compartecipi, potrà al più, ricorrendone gli ulteriori presupposti, configurarsi il reato di

Né infine si potrebbe trarre l'obbligo giuridico di attivarsi da una precedente attività svolta dal *provider*[71]: la stessa, consistente nell'offerta dei diversi servizi Internet, non può essere considerata pericolosa in sé, in quanto del tutto neutra e lecita per il diritto penale ed anzi essenziale all'esplicarsi di diritti costituzionalmente garantiti[72].

In realtà, la non ipotizzabilità in capo all'ISP di un generale obbligo di impedimento degli illeciti altrui e le argomentazioni richiamate, non sembrano essere in grado di escludere a priori che doveri specifici di collaborazione possano validamente fondare una sua responsabilità omissiva[73].

Come già in parte analizzato nei precedenti paragrafi, peculiari doveri di informazione, comunicazione e collaborazione con l'autorità giudiziaria o amministrativa sono stati introdotti non solo ai sensi degli artt. 14, 15, 16, 17 del d.lgs. n. 70/2003, ma anche nel campo della lotta alla pedopornografia[74], al

---

favoreggiamento *ex* art. 378 c.p., o d'inosservanza di un provvedimento dell'autorità *ex* art. 388 c.p.

[71] In giurisprudenza è pacifica l'ammissibilità di un obbligo di attivarsi gravante sull'agente originato dall'esercizio di attività pericolose (cfr. *ex multis* Cassazione penale, sent. n. 26239/2013). In senso critico rispetto a tale asserzione v. FIANDACA G., *Il reato commissivo mediante omissione*, cit., p. 204 ss.

[72] Cfr. SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer*, cit., p. 1211 ss. V. inoltre Tribunale di Milano, 25 febbraio 2004, n. 1993.

[73] In tal senso cfr. PICOTTI L., *Fondamento e limiti della responsabilità penale dei Service Providers*, cit.

p. 380 ss.; ID., *La responsabilità penale dei service-providers in Italia*, cit., p. 504 ss.; ID., *I diritti fondamentali nell'uso e abuso dei social network. Aspetti penali*, in *Giurisprudenza di merito*, n. 12/2012, p. 2543 ss.

[74] Art. 14 *ter* l. n. 269/1998 «1. I fornitori dei servizi resi attraverso reti di comunicazione elettronica sono obbligati, fermo restando quanto previsto da altre leggi o regolamenti di settore, a segnalare al Centro, qualora ne vengano a conoscenza, le imprese o i soggetti che, a qualunque titolo, diffondono, distribuiscono o fanno commercio, anche in via telematica, di materiale pedopornografico, nonché a comunicare senza indugio al Centro, che ne faccia richiesta, ogni informazione relativa ai contratti con tali imprese o soggetti. 2. I fornitori dei servizi per l'effetto della segnalazione di cui al comma 1 devono conservare il materiale oggetto della stessa per almeno quarantacinque giorni. 3. Salvo che il fatto costituisca reato, la violazione degli obblighi di

terrorismo[75], al gioco d'azzardo[76] nonché nell'ambito della tutela della *privacy*[77] e della *cyber*-sicurezza[78]. Sono altresì rinvenibili doveri di collaborazione tramite il

---

cui al comma 1 comporta una sanzione amministrativa pecuniaria da euro 50.000 a euro 250.000. All'irrogazione della sanzione provvede il Ministero delle comunicazioni. 4. Nel caso di violazione degli obblighi di cui al comma 1 non si applica il pagamento in misura ridotta di cui all'articolo 16 della legge 24 novembre 1981, n. 689».

Art. 14 *quater*: «1. I fornitori di connettività alla rete INTERNET, al fine di impedire l'accesso ai siti segnalati dal Centro, sono obbligati ad 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. Con il medesimo decreto viene altresì indicato il termine entro il quale i fornitori di connettività alla rete INTERNET devono dotarsi degli strumenti di filtraggio. 2. La violazione degli obblighi di cui al comma 1 è punita con una sanzione amministrativa pecuniaria da euro 50.000 a euro 250.000. All'irrogazione della sanzione provvede il Ministero delle comunicazioni. 3. Nel caso di violazione degli obblighi di cui al comma 1 non si applica il pagamento in misura ridotta di cui all'articolo 16 della legge 24 novembre 1981, n. 689».

[75] Art. 2, commi 3-4, d.l. n. 7/2015: «I fornitori di connettività, su richiesta dell'autorità giudiziaria procedente, inibiscono l'accesso ai siti inseriti nell'elenco di cui al comma 2, secondo le modalità, i tempi e le soluzioni tecniche individuate e definite con il decreto previsto dall'articolo 14*quater*, comma 1, della legge 3 agosto 1998, n. 269. 4. Quando si procede per i delitti di cui agli articoli 270 *bis*, 270 *ter*, 270 *quater* e 270 *quinquies* del codice penale commessi con le finalità di terrorismo di cui all'articolo 270 *sexies* del codice penale, e sussistono concreti elementi che consentano di ritenere che alcuno compia dette attività per via telematica, il pubblico ministero ordina, con decreto motivato, ai fornitori di servizi di cui all'articolo 16 del decreto legislativo 9 aprile 2003, n. 70, ovvero ai soggetti che comunque forniscono servizi di immissione e gestione, attraverso i quali il contenuto relativo alle medesime attività è reso accessibile al pubblico, di provvedere alla rimozione dello stesso. I destinatari adempiono all'ordine immediatamente e comunque non oltre quarantotto ore dal ricevimento della notifica. In caso di mancato adempimento, si dispone l'interdizione dell'accesso al dominio internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale».

[76] Art. 50 l. n. 296/2006: «In coerenza ai principi recati dall'articolo 38 del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248, ed al fine di contrastare la diffusione del gioco irregolare ed illegale, l'evasione e l'elusione fiscale nel settore del gioco, nonché di assicurare l'ordine pubblico e la tutela del giocatore, con uno o più provvedimenti del Ministero dell'economia e delle finanze - Amministrazione autonoma dei monopoli di Stato sono stabilite le modalità per procedere alla rimozione dell'offerta, attraverso le reti telematiche o di telecomunicazione, di giochi, scommesse o concorsi pronostici con vincite in

denaro in difetto di concessione, autorizzazione, licenza od altro titolo autorizzatorio o abilitativo o, comunque, in violazione delle norme di legge o di regolamento o delle prescrizioni definite dalla stessa Amministrazione. I provvedimenti di cui al presente comma sono adottati nel rispetto degli obblighi comunitari. L'inosservanza dei provvedimenti adottati in attuazione della presente disposizione comporta l'irrogazione, da parte dell'Amministrazione autonoma dei monopoli di Stato, di sanzioni amministrative pecuniarie da 30.000 euro a 180.000 curo per ciascuna violazione accertata».

[77] Art. 32 *bis* d.lgs. n. 196/2003 inserito con l. n. 69/2012: «1. In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione al Garante. 2. Quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona, il fornitore comunica anche agli stessi senza ritardo l'avvenuta violazione. 3. La comunicazione di cui al comma 2 non é dovuta se il fornitore ha dimostrato al Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione. 4. Ove il fornitore non vi abbia già provveduto, il Garante può, considerate le presumibili ripercussioni negative della violazione, obbligare lo stesso a comunicare al contraente o ad altra persona l'avvenuta violazione. 5. La comunicazione al contraente o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione al Garante descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio. 6. Il Garante può emanare, con proprio provvedimento, orientamenti e istruzioni in relazione alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione, tenuto conto delle eventuali misure tecniche di attuazione adottate dalla Commissione europea ai sensi dell'articolo 4, paragrafo 5, della direttiva 2002/58/CE, come modificata dalla direttiva 2009/136/CE.

7. I fornitori tengono un aggiornato inventario delle violazioni di dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in modo da consentire al Garante di verificare il rispetto delle disposizioni del presente articolo. Nell'inventario figurano unicamente le informazioni necessarie a tal fine. 8. Nel caso in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico affidi l'erogazione del predetto servizio ad altri soggetti, gli stessi sono tenuti a comunicare al fornitore senza indebito ritardo tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti di cui al presente articolo».

Ulteriori obblighi in merito alla conservazione e protezione dei dati erano già stati previsti grazie alle modifiche apportate dal d.lgs. n. 109/2008 all'art. 132 d.lgs. n. 196/2003: «1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, sono

conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. 1 *bis*. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni. 3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del giudice su istanza del pubblico ministero o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391 *quater* del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante. 4 *ter*. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi. 4 *quater*. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4 *ter* deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale. 4 *quinquies*. I provvedimenti adottati ai sensi del comma 4 *ter* sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia. 5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'art. 17, volti anche a: a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli

combinato disposto di specifiche violazioni penali e precipue procedure inibitorie nel settore dei diritti d'autore ed in quello della proprietà industriale[79].

E' necessario quindi valutare se tali doveri possano integrare altrettante posizioni di garanzia necessarie per l'applicazione del paradigma di cui all'art. 40, comma 2, c.p.

Come più volte chiarito da dottrina e giurisprudenza non qualsiasi obbligo di attivarsi rileva nell'ottica della responsabilità omissiva. E' pacificamente ammessa la possibilità che anche leggi extra-penali costituiscano fonti potenziali di posizione di garanzia, mentre, stante l'assenza di indicazioni precise nel codice penale, molto più complessa risulta l'individuazione dei criteri sostanziali onde selezionare i comandi rilevanti[80].

---

incaricati del trattamento di cui all'allegato b); d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2».

Per le violazioni del nuovo art. 132 d.lgs. n. 196/2003 sono state altresì introdotte sanzioni amministrative all'art. 162 bis.

[78] Art. 11 DPCM 24.01.13: «*Operatori privati* 1. Gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici, ivi comprese quelle individuate ai sensi dell'art. 1, comma 1, lett. d), del decreto del Ministro dell'interno 9 gennaio 2008, secondo quanto previsto dalla normativa vigente, ovvero previa apposita convenzione: a) comunicano al Nucleo per la sicurezza cibernetica, anche per il tramite dei soggetti istituzionalmente competenti a ricevere le relative comunicazioni ai sensi dell'art. 16 *bis*, comma 2, lett. b), del decreto legislativo n. 259/2003, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti; b) adottano le *best practices* e le misure finalizzate all'obiettivo della sicurezza cibernetica, definite ai sensi dell'art. 16 *bis*, comma 1, lett. a), del decreto legislativo n. 259/2003, e dell'art. 5, comma 3, lett. d), del presente decreto; c) forniscono informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza, nei casi previsti dalla legge n. 124/2007; d) collaborano alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti».

[79] V. artt. 156, 156 *bis* e 163 l. n. 633/1941; art. 131 d.lgs. n. 30/2005.

[80] Secondo la teoria c.d. formale la posizione di garanzia si identifica negli obblighi fissati dalla legge (penale o extra-penale), dalla consuetudine o dai contratti (non escludendo la *negotiorium gestio*). Pur discostandosi dal criterio formale, cui la teoria si ispira, chi aderisce a tale ricostruzione riconosce quale fonte qualificata anche la precedente azione pericolosa, che

Indipendentemente dalla riconducibilità nell'ambito delle posizioni di garanzia cd. *di protezione* ovvero in quelle di *controllo* o ancora nella discussa categoria delle posizioni di garanzia nascenti dal *dovere di impedire la commissione dei reati altrui*[81], che ha suscitato numerose problematiche e

---

imporrebbe di attivarsi per eliminare la situazione di pericolo creata. Il limite di tale orientamento è costituito dal fatto che, concentrandosi solamente sulla valutazione dell'aspetto della genesi formale dell'obbligo, si trascura completamente l'analisi della preordinata funzionalità a evitare l'evento.

Per far fronte a tale criticità è stata valorizzata da alcuni autori una ricostruzione c.d. funzionale, che, superando il dogma della giuridicità della fonte degli obblighi di garanzia, affida la selezione a criteri di natura materiale desumibili dalle specifiche funzioni in concreto svolte dall'agente, titolare di un potere di signoria sulle condizioni essenziali per il verificarsi dell'evento. La "copertura normativa" di tale teoria viene garantita da norme di contenuto generale, quali gli artt. 2 e 32 della Costituzione. Anche questa seconda impostazione non è comunque esente da critiche, stante il rischio di violazioni del principio di legalità e di determinatezza della fattispecie.

È stata infine elaborata un'ulteriore teoria che, integrando le due precedenti, valorizza sia il requisito formale che quello finalistico sancendo che la fonte dell'obbligo deve essere legislativamente determinata (salva la possibilità meramente integrativa della normazione secondaria) e l'obbligo destinato finalisticamente a proteggere ed impedire l'evento lesivo. In virtù dell'art. 1372 c.c., secondo il quale il contratto ha forza di legge tra le parti, si annovera tra le fonti qualificate anche il contratto. Spesso la giurisprudenza, aderendo a tale terza impostazione, ha ritenuto sufficiente a fondare l'esistenza di una posizione di garanzia la "presa in carico" del bene che ne accresca la possibilità di salvezza, ovvero l'assunzione volontaria ed unilaterale di compiti di tutela al di fuori di un preesistente obbligo giuridico (v. Cassazione penale, sent. 22 maggio 2007, n. 25527). L'assunzione di fatto di poteri inerenti agli obblighi di tutela è peraltro oggi normativamente prevista in tema di sicurezza sul lavoro, ai sensi dell'art. 299 del d.lgs. 9 aprile 2008, n. 81, nel caso di chi, pur sprovvisto di formale investiture, esercita in concreto i poteri giuridici riferiti al datore di lavoro, al dirigente e al preposto.

A fronte della totale assenza di indicazione precise nel codice penale non si può che condividere la valutazione negativa del paradigma di cui all'art. 40, comma 2, c.p., espressa da autorevole dottrina: «non soltanto non consente alcuna certezza, ma addirittura rappresenta uno dei casi più clamorosi di creazione giudiziale delle fattispecie penali», v. ROMANO M., *Commentario sistematico del codice penale I*, sub. *art. 40 c.p.*, cit., p. 364 ss.

[81] Per la definizione di tali categorie cfr. GRASSO G., *Il reato omissivo improprio*, cit., p. 291 ss.

soluzioni contradditorie, sembra potersi innanzitutto affermare che gli obblighi in esame appaiono sufficientemente "qualificati" e specificati.

Né si potrebbe obbiettare che tramite gli stessi i *providers* si trasformino da operatori tecnici a operatori giuridici, "controllori della rete" con compiti inquisitori e di polizia, senza avere peraltro specifiche competenze e con grave messa in pericolo della libera manifestazione del pensiero[82].

Un'attenta lettura delle norme richiamate, infatti, evidenzia come i doveri fissati siano innanzitutto di segnalazione/informazione e la rimozione dei contenuti o l'inibizione dell'accesso a determinati siti non sia basata sulla personale valutazione di merito del fornitore ma bensì solidamente ancorata alle indicazioni delle autorità competenti.

Confutabile anche la tesi dell'inesigibilità dell'intervento dell'intermediario che, data la caratteristica dinamicità del flusso dati nella rete delle reti, risponderebbe secondo il paradigma di una responsabilità oggettiva o di posizione: in pieno rispetto al principio di personalità della responsabilità penale, gli obblighi in esame sorgono con la "conoscenza" delle presunte attività illecite. E' inoltre evidente che l'ISP, stante l'attività svolta, è dotato dei poteri tecnici per agire[83] ma che, in relazione alle "censure", i provvedimenti delle autorità competenti devono individuare specificatamente le violazioni in relazione alle quali essi devono intervenire. Sarà infine sempre necessario vagliare il dominio

---

[82] Tali preoccupazioni sono state espresse anche dalla *Associazione per le libertà nella comunicazione elettronica interattiva* (ALCEI), *Provider e responsabilità nella legge comunitaria 2001*, in interlex.it, 19 Giugno 2002: «Il *provider* viene, di fatto, trasformato in un giudice-poliziotto, che per evitare di essere chiamato a rispondere in prima persona del comportamento illecito degli utenti, sarà costretto ad esercitare censure, filtraggi e controlli più o meno palesi su quanto accade nei propri server. E questo quando oramai, almeno in Italia, sembrava un dato acquisito (anche dalla giurisprudenza) che l'unica responsabilità ipotizzabile a carico del provider fosse quella fondata sul concorso nell'illecito».

[83] Sicuramente nel caso del *provider* professionale, che lucra tramite la raccolta pubblicitaria, sostenere l'incapacità di intervento sui dati immessi dagli utenti sembra inaccettabile: i profitti, infatti, sono strettamente connessi all'abilità tecnica di offrire agli internauti una pubblicità profilata sulle loro preferenze (ricavate dalle *queries* rivolte al motore di ricerca) e di abbinare determinati contenuti pubblicitari a quelli ospitati sul sito. In tal senso cfr. ROSSELLO C., *Riflessioni de jure condendo in materia di responsabilità del provider*, cit., p. 627.

tecnico-organizzativo nella situazione concreta e specifica secondo la lente del principio *ultra posse nemo tenetur*[84].

Sembra potersi abbracciare l'orientamento giurisprudenziale secondo il quale la posizione di garanzia richiede l'esistenza di poteri impeditivi che ben possono anche concretizzarsi in obblighi diversi e di minore efficacia rispetto a quelli direttamente e specificamente volti ad impedire il verificarsi dell'evento. Considerato perlopiù il fatto che nella maggior parte dei casi il garante non dispone in ogni situazione di tutti i poteri impeditivi che invece di volta in volta si modulano sulle situazioni concrete, sarà sufficiente che ad esso siano riservati mezzi idonei a sollecitare gli interventi necessari per evitare che l'evento dannoso venga cagionato, e che quindi, nel contesto di operatività di altri elementi condizionanti di natura dinamica, egli ponga in essere quelli da lui esigibili[85].

E' necessaria un'ulteriore puntualizzazione: si è sostenuto che gli obblighi in esame scatterebbero spesso in un momento successivo alla consumazione del reato, trattandosi nella maggior dei casi di reati a forma libera a consumazione istantanea[86]. In realtà, tale affermazione sembra non tener debitamente in considerazione le caratteristiche precipue della rete: come già più volte ribadito nel presente lavoro, la strutturale a-territorialità e a-materialità del *cyberspace* impongono una ripensamento dei concetti dogmatici tradizionalmente connessi

---

[84] Sul punto cfr. ampiamente SIEBER U., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di internet*, cit.

[85] Cfr. Corte di Cassazione, sent. n. 16761/2010; 38991/2010. Nelle pronunce in esame quindi non si condivide l'orientamento, espresso da parte della dottrina, in virtù del quale gli obblighi di garanzia andrebbero distinti dagli "obblighi di sorveglianza" o "di attivazione" per i quali non opererebbe la clausola di equivalenza dell'art. 40, comma 2, c.p., comportando per chi ne è onerato, solo un compito di vigilanza sulle situazioni di pericolo ma non un compito impeditivo dell'evento delittuoso, attesa la mancanza dei relativi poteri.

[86] Cfr. INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, cit., p. 33. L'autore in modo particolare sostiene questo a proposito dei reati di diffusione, divulgazione, pubblicizzazione di materiale pedopornografico, rilevanti con riguardo agli obblighi di cui all'art. 14 *ter-quater* della l. n. 269/1998. Sul punto v. inoltre DE NATALE D., *Responsabilità penale dell'Internet Service Provider per omesso impedimento e per concorso nel rato di pedopornografia*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, cit., p. 295.

alla dimensione spazio-temporale. In modo particolare l'"evento" *on-line* non può che subire forti distorsioni: nel caso di diffusione di contenuti illeciti o dei reati di manifestazione del pensiero realizzati via Internet, infatti, esso non solo si smaterializza ma «tende anche ad espandersi e riprodursi "automaticamente", quasi moltiplicandosi per il numero delle volte o delle possibilità di percezione da parte di terzi, pur in tempi successivi ed in territori (ed ordinamenti!) molto diversi»[87].

Nella rete quindi i reati istantanei assumerebbero la veste di reati istantanei ad effetti permanenti data la perdurante circolazione potenziale del dato e il protrarsi dell'interesse al rispetto delle prescrizioni esaminate, volte alla tutela di beni e diritti fondamentali quali il libero sviluppo psico-fisico del minore, la sicurezza nazionale, la proprietà intellettuale ed industriale, il buon funzionamento del mercato e l'ordine pubblico.

In tale contesto gli obblighi di segnalazione all'autorità o cessazione/impedimento dell'altrui condotta generano una posizione di garanzia per quanto avviene successivamente alla conoscenza dell'illeceità dell'attività realizzata dall'utente o del provvedimento dell'autorità e non possono che rendere causalmente rilevante il contributo omissivo dell'ISP.

E' infine essenziale evidenziare che il legislatore, fissando gli obblighi di segnalazione o rimozione esaminati, utilizza sovente i termini "violazioni" o "attività illecite" e non "reati": che le stesse si siano già verificate è presupposto necessario affinchè il *provider* si attivi ma ciò non significa che costituiscano un reato perfezionato[88].

---

[87] Così PICOTTI L., *Internet e responsabilità penali*, cit., p. 119.

[88] V. FLOR R., *Nuove tecnologie e giustizia penale in Europa, tra le esigenze di accertamento e prevenzione dei reati e quelle di tutela della riservatezza: il ruolo «propulsore» della Corte di Giustizia*, in *Studi in onore di Maurizio Pedrazza Gorlero*, Napoli, 2014 , pp. 247-286: «Si tratta comunque di attività che si svolgono sotto l'autorità o il controllo del *provider*, rispetto alle quali è dotato di un effettivo potere / dovere di interferenza - in quanto viene a conoscenza dell'illecito o è messo concretamente in grado di riconoscerlo, ossia in condizione di riconoscere la situazione di pericolo o di rischio - per impedire sia la prosecuzione delle violazioni dei diritti d'autore, che la realizzazione di reati, se le condizioni di rischio sono specificatamente individuate e definite dai provvedimenti ingiunzionali. Pertanto non è pacifica l'esclusione di una posizione di garanzia o di

Alla luce di quanto esposto sembra quindi potersi concludere che i citati precetti extra-penali fissati dal legislatore nazionale, senza disattendere il principio dell'assenza di un dovere generale di sorveglianza per i *provider*, costituiscono la fonte di quegli obblighi giuridici che, ai sensi dell'art. 40 cpv. c.p., sono idonei a fondare una responsabilità penale per omesso impedimento dell'evento[89]. D'altronde tutto ciò è pienamente in linea con la condotta virtuosa che, come previsto dal legislatore comunitario, gli stati membri possono richiedere agli intermediari della società dell'informazione[90].

Il contemperamento tra l'esigenza di garantire la libertà di comunicazione e la necessità di tutelare diritti fondamentali del nostro ordinamento non può, infatti, che comportare il superamento del paradigma del *provider* inerte o passivo non appena ricevuta la notizia dell'illecito commesso dai fruitori del suo servizio[91].

A sostegno di tale conclusione anche la ricostruzione dell'omissione *ex* art. 40 c.p. offerta da una parte della dottrina, in virtù della quale le posizioni di garanzia cd. di protezione, imponendo un rilevante sacrificio della libertà personale conseguente alla statuizione di obblighi d'agire penalmente rilevanti, sarebbero

---

un obbligo di impedimento dei reati realizzati dagli utenti della rete in capo al *provider*, la cui sussistenza deve essere valutata caso per caso anche rispetto agli obblighi previsti dalla disciplina extrapenale del "settore di riferimento" (pedopornografia, proprietà intellettuale, privacy ecc.)». Cfr. inoltre ID., *Social Networks e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Rivista trimestrale di diritto penale dell'economia*, n. 3/2012, p. 647.

[89] In tal senso cfr. PICOTTI L., *Commento Art. 600-ter, III comma, c. p. (Pornografia minorile)*, cit., p. 207 ss.; FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, cit., p. 448 ss.; SALVADORI I., *Presupposti della responsabilità penale del blogger per gli scritti offensivi pubblicati su un blog da lui gestito*, cit. In relazione alla precedente normativa in materia di *privacy* (l. n. 675/1996) v. PICOTTI L., *La responsabilità penale dei service-providers in Italia*, cit., p. 504 ss.

[90] Dir. 2000/31/CE, Considerando 48: «La presente direttiva non pregiudica la possibilità per gli Stati membri di chiedere ai prestatori di servizi, che detengono informazioni fornite dai destinatari del loro servizio, di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire taluni tipi di attività illecite».

[91] Cfr. Corte d'appello di Milano, sez. spec. in materia d'impresa, sent. 29/2015.

configurabili solo in riferimento a beni dotati di particolare valore[92]: come enunciato nelle conclusioni del precedente capitolo, non sembrerebbe infatti possibile escludere a priori l'esistenza di un bene giuridico superindividuale costituito da un "*cyberspace* sano" da proteggere da fonti di pericolo quali l'immissione di dati illeciti.

3. RESPONSABILITÀ *EX* ART. 57 C.P.

Onde configurare una responsabilità penale dell'ISP è stato proposto il ricorso al modello soggettivo del responsabile editoriale di una testata giornalistica.

Assimilando la carta stampata alle informazioni circolanti nel *web* si potrebbero, infatti, estendere le disposizioni sui reati commessi a mezzo stampa: il *provider* avrebbe l'obbligo di controllare i contenuti immessi mediante i propri *server* e diverrebbe imputabile per l'illecito realizzato dall'utente a titolo di *culpa in vigilando*.

L'operatività delle norme di cui agli artt. 57 ss. c.p. implica in primo luogo una riflessione su complesse questioni terminologiche. Le disposizioni in esame regolano, precisamente, la responsabilità penale del direttore di "stampe o stampati", categoria che ai sensi dell'art. 1 della legge 8 febbraio 1948, n. 47 è riferibile a «tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione»[93].

E' necessario quindi interrogarsi circa la sovrapponibilità della nozione di "stampa" alla fenomenologia dell'immissione di dati in rete.

---

[92] Cfr. SGUBBI F., *Responsabilità penale per omesso impedimento dell'evento*, Padova, 1975, p. 23 ss.; PULITANÒ D., *Il favoreggiamento personale tra diritto e procedura penale*, Milano, 1984, p. 158 ss. Da segnalare come a tale indirizzo, che limita fortemente l'applicazione dell'art. 40, comma 2, c.p., siano state avanzate obiezioni convincenti: la formula adottata dal legislatore non consentirebbe infatti una tale restrizione a priori. Cfr. in tal senso GRASSO G., *Il reato omissivo improprio*, p. 169 ss.

[93] Legge n. 47/1948, art. 1, *Definizione di stampa o stampato.*

Pur essendo entrambe strumenti attraverso i quali comunicare il pensiero, è evidente che l'elemento imprescindibile della nozione di stampa accolta dalla l. n. 47/1948 è la riproduzione attraverso mezzi tipografici[94].

Proprio in conformità a tale rilievo si è registrato, in dottrina e in giurisprudenza, un orientamento secondo il quale la configurabilità dei reati in materia di stampa nel *web* violerebbe il divieto di analogia di cui all'art. 14 delle disposizioni preliminari del codice civile, essendo la circolazione di contenuti in Internet totalmente svincolata dalla riproduzione stampata e pertanto sostanzialmente diversa dalla stampa[95].

In ossequio al principio di legalità, di cui il principio di tassatività e il divieto di analogia in *malam partem* sono estrinsecazioni, la definizione di stampa o stampato *ex* art. 1 della l. n. 47/1948, non sarebbe pertanto suscettibile di interpretazione analogica e/o estensiva nei confronti di altri mezzi e strumenti di comunicazione diversi ed eterogenei, ai fini dell'applicabilità delle connesse responsabilità penali[96].

---

[94] Già Nuvolone individuava quali elementi che contraddistinguono il concetto di stampa quello "statico", consistente nella riproduzione tipografica ottenuta con mezzi meccanici o fisico-chimici, e quello "dinamico" della destinazione alla pubblicazione. Cfr. NUVOLONE P., *Il diritto penale della stampa*, Padova, 1971, p. 11 ss.

[95] Cfr. in tal senso ZENO-ZENCOVICH V., *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/1998, p. 15 ss. In giurisprudenza tra le più risalenti v. Tribunale di Milano, sent. 12 maggio 2003, n. 4153 e sent. 25 febbraio 2004, n. 1993, (prima sentenza penale in materia di responsabilità per *linking*) con commento di CAVANNA E., *Le responsabilità dei providers alla luce della sentenza del Tribunale di Milano - Sezione V Penale in composizione collegiale - n. 1993 del 25 febbraio 2004*, in penale.it, 25 Febbraio 2004; RESTA F., *La responsabilità penale del provider: tra laissez faire ed obblighi di controllo*, in *Giurisprudenza di merito*, 2004, p. 1715 ss. e nota di CORRIAS LUCENTE. G., *Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che loro gestiscono?*, in *Giurisprudenza di merito*, 2004, p. 2523 ss.

[96] Cfr. Cassazione penale, sent. 3 febbraio 1989, n. 259, con la quale la Corte esclude che la videocassetta registrata sia assimilabile al concetto di stampato; v. inoltre Cassazione penale, sent. 27 febbraio 1996, n. 1291 e sent. 23 aprile 2008, n. 34717 con le quali, stante la diversità tra la stampa e la radiotelevisione si è negato l'applicabilità dell'art. 57 c.p. al direttore della testata televisiva.

Oltre a ragioni strutturali, legate all'assenza di un supporto fisico da distribuire, il divieto di estensione della disciplina in materia di stampa ad Internet è giustificato anche dalla necessità di non infrangere il principio di personalità della responsabilità penale di cui all'art. 27 Cost. L'enorme flusso di dati *on-line* rende infatti alquanto complicato, se non impossibile, un "controllo" manuale degli stessi e, come chiarito nel primo capitolo del presente lavoro, punire un'omissione quando il comportamento da tenere è inesigibile, rappresenta una violazione del principio di colpevolezza[97].

La figura del *provider* sarebbe perciò assimilabile eventualmente ad un *book store* o ad una biblioteca pubblica, più che al direttore o al vice-direttore responsabile, non sussistendo quindi alcun obbligo generale di sorveglianza, così come per lo più riconosciuto nella direttiva *e-Commerce*[98].

---

[97] In tali termini si è espressa anche la Corte di Cassazione, sent. 29 novembre 2011, n. 44126: «D'altronde, non vi è solamente una diversità strutturale tra i due mezzi di comunicazione (carta stampata e Internet), ma altresì la impossibilità per il direttore della testata di impedire la pubblicazione di commenti diffamatori, il che rende evidente che la norma contenuta nell'articolo 57 del codice penale non è stata pensata per queste situazioni, perché costringerebbe il direttore ad una attività impossibile, ovvero lo punirebbe automaticamente ed oggettivamente, senza dargli la possibilità di tenere una condotta lecita. E di ciò si rende conto anche la sentenza impugnata, laddove afferma che - non essendo possibile una censura preventiva, e dunque, non potendo "…imputarsi al direttore responsabile l'omesso controllo di ciò che, fino a quel momento, non poteva sapere venisse pubblicato…" - la H. avrebbe dovuto svolgere una verifica successiva delle inserzioni già avvenute, espungendo quelle a contenuto diffamatorio. Così facendo, però, il giudice di appello ha indebitamente modificato la fattispecie normativa prevista dall'articolo 57 del codice penale, sanzionando una condotta diversa da quella tipizzata dal legislatore». V. nota a questa sentenza di VIGEVANI G. E., *La «sentenza figlia» sul direttore del giornale telematico: il caso Hamaui*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2011, p. 798 ss.; TURCHETTI S., *Un secondo "alt" della Cassazione all'applicazione dell'art. 57 c.p. al direttore del periodico on line*, in penalecontemporaneo.it, 16 Dicembre 2011; CORRIAS LUCENTE. G., *Al direttore responsabile di un periodico on line non si applica il reato previsto dall'art. 57 del codice*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2012, p. 82 ss.

[98] Cfr. Tribunale di Roma, ord. 4 luglio 1998 (in *Dir. informazione e informatica*, 1998, p. 807 ss.), con la quale, prima dell'approvazione del d.lgs n. 70/2003, già si negava fermamente sia l'identità tra testata giornalistica e sito Internet sia l'esistenza di un obbligo di controllo sul

Nel corso degli anni, però, non sono mancate soluzioni giurisprudenziali alquanto eterogenee che hanno talvolta equiparato il gestore di un sito Internet ad un responsabile editoriale, attribuendogli l'obbligo di monitorare il materiale pubblicato sul proprio *server*[99].

In modo particolare, con riguardo allo specifico caso del direttore di un giornale *on-line,* dopo le modifiche apportate dalla legge 7 marzo 2001, n. 62,

---

materiale inserito dagli utenti da parte del *provider*. A commento v. CAMMARATA M., *Finalmente una decisione sulla responsabilità del provider*, in interlex.it, 20 Luglio 1998; FOGLIANI E., *Verso una irresponsabilità oggettiva del provider?*, in interlex.it, 24 Luglio 1998. Cfr. inoltre Cassazione penale, sent. 10 marzo 2009, n. 10535; Corte Costituzionale, ord. 12 dicembre 2011, n. 337. In termini comparatistici cfr. *United States District Court for the Southern District of New York*, sent. 29 ottobre 1991, *Cubby, Inc. v. CompuServe Inc.* Si tratta del primo caso statunitense relativo alla diffamazione in rete ed alla responsabilità degli ISP per i messaggi diffusi da terzi. Oggetto della causa i messaggi offensivi nei confronti della *Skuttlebut*, società controllata dalla *Cubby Inc.*, registrati all'interno di un «*Journalism Forum*», ospitato dalla società *CompuServe*. La Corte esclude che l'ISP potesse essere responsabile in qualità di *publisher*, secondo le normali regole di responsabilità editoriali, bocciando la presunta analogia tra i prestatori telematici e quelli dei servizi editoriali.

[99] Cfr. Tribunale di Aosta, sent. 26 maggio 2006, n. 553, con nota di SALVADORI I., *Presupposti della responsabilità penale del blogger per gli scritti offensivi pubblicati su un blog da lui gestito*, in *Giurisprudenza di merito*, n. 4/2007, p. 1069 ss. Seppur in sede civile v. inoltre Tribunale di Napoli, ord. 8 agosto 1996 (in *Dir. inf. e informatica*, 1997, p. 970 ss.). Nell'affermare la responsabilità extracontrattuale del *provider* il giudice adotta pienamente la teoria della *culpa in vigilando*, sull'assunto che un sito Internet, quale canale di comunicazione destinato a un pubblico di lettori, va assimilato ad un organo di stampa; v. inoltre Procura della Repubblica presso la Pretura Circondariale di Vicenza, Decreto di sequestro preventivo, 23 giugno 1998, a commento CAMMARATA M., *Internet, diritto e politica, non c'è da stare allegri*, in interlex.it, 2 Luglio 1998.

Nella giurisprudenza americana in modo particolare cfr. *U.S. New York Supreme Court,* 1995 WL 323710, *Stratton Oakmont, Inc. v. Prodigy Services Co.* Rispetto al precedente *Cubby v. CompuServe* sussiste un elemento differente: l'ISP che ospita il *forum* di discussione, infatti, utilizza un "filtro", ossia un *software* capace di rimuovere automaticamente i contenuti contraddistinti da un linguaggio offensivo. E' proprio tale filtro che permette alla Corte di affermare la responsabilità dell'ISP convenuto a titolo di *publisher.* A causa del controllo attivo dei contenuti il *provider* si trasforma quindi in un editore avente le stesse responsabilità previste per la stampa.

recante "Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla Legge 5 agosto 1981, n. 416", le pubblicazioni sul *web* sono state talora equiparate al "prodotto editoriale".

Si sono cioè registrate pronunce secondo le quali la l. n. 62/2001, inglobando nel concetto di prodotto editoriale quello realizzato su supporto informatico, «destinato alla pubblicazione o, comunque, alla diffusione d'informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva, con esclusione dei prodotti discografici o cinematografici»[100], avrebbe esteso anche alle pubblicazioni con il mezzo elettronico la disciplina sulla stampa ed i relativi obblighi fissati nella l. n. 47/1948, tra cui l'indicazione del direttore o del vice-direttore responsabile, ai quali quindi potrebbe applicarsi la responsabilità *ex* art. 57 c.p.[101].

[100] Legge 62/2001, art. 1, *Definizioni e disciplina del prodotto editoriale*: «1. Per «prodotto editoriale», ai fini della presente legge, si intende il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva, con esclusione dei prodotti discografici o cinematografici. 2. Non costituiscono prodotto editoriale i supporti che riproducono esclusivamente suoni e voci, le opere filmiche ed i prodotti destinati esclusivamente all'informazione aziendale sia ad uso interno sia presso il pubblico. Per «opera filmica» si intende lo spettacolo, con contenuto narrativo o documentaristico, realizzato su supporto di qualsiasi natura, purchè costituente opera dell'ingegno ai sensi della disciplina sul diritto d'autore, destinato originariamente, dal titolare dei diritti di utilizzazione economica, alla programmazione nelle sale cinematografiche ovvero alla diffusione al pubblico attraverso i mezzi audiovisivi. 3. Al prodotto editoriale si applicano le disposizioni di cui all' articolo 2 della legge 8 febbraio 1948, n. 47. Il prodotto editoriale diffuso al pubblico con periodicità regolare e contraddistinto da una testata, costituente elemento identificativo del prodotto, è sottoposto, altresì, agli obblighi previsti dall'articolo 5 della medesima legge n. 47 del 1948».

[101] Cfr. Tribunale di Firenze, sent. 13 febbraio 2009, n. 982: «Il sito internet, inteso come insieme di hardware e software attraverso cui si genera il prodotto telematico sotto forma di trasmissione di flussi di dati, in quanta prodotto editoriale, ai sensi della l. n. 62/2001, si deve *ritenere* sottoposto anche ai fini penali alla disciplina sulla stampa. Quanto ai periodici *on line*, essi rientrando in questo genus, sono soggetti anche alle indicazioni obbligatorie in tema di editoria previste per gli stampati e alla registrazione obbligatoria della testata (art. 1 co. 3). Quindi anche il giornale *on line* ha un suo direttore responsabile ed un editore che devono essere riportati sul sito web. Ragionando in questi termini, nel caso di diffamazione commessa con il mezzo di un

Aderendo a tale impostazione la legislazione penale in materia di stampa, grazie all'equiparazione introdotta dall'art. 1 della l. n. 62/2001, sarebbe per ciò solo applicabile a quanto divulgato non solo in forma cartacea ma anche telematica.

In realtà la correttezza di una tale ricostruzione è molto dubbia.

L'estensione della disciplina della stampa all'informazione diffusa tramite Internet sembra il frutto di una forzatura interpretativa del testo della legge n. 62/2001. Non si comprende, infatti, perché la semplice riferibilità del "prodotto editoriale" all'informazione telematica debba comportare l'estensione alla diffusione di dati in Internet della disciplina sulla stampa *tout court*, compresa quella penale, tanto più che proprio nell'art. 1, comma 1, l'inciso «ai fini della presente legge» circoscrive nettamente la portata della norma e che l'art 7, comma 3, d.lgs. n. 70/2003 ha precisato come l'obbligo di registrazione della testata editoriale telematica sussiste solamente in relazione a quelle attività per le quali i prestatori del servizio intendono avvalersi dei benefici previsti dalla l. n. 62/2001. I fini di quest'ultima sono appunto quelli di concedere agevolazioni quali ad esempio la possibilità di avere determinati contributi, erogati da un apposito fondo, oppure la possibilità di beneficiare del credito di imposta a vantaggio delle imprese editoriali che effettuano investimenti e programmi di ristrutturazione.

E' chiaro quindi che il legislatore ha previsto l'obbligo, o meglio l'onere, di registrazione e l'equiparabilità del prodotto editoriale ad Internet non

---

giornale telematico, non possono non richiamarsi le norme del codice penale in materia di stampa, ossia l'art. 595 co. 3 c.p. e l'art. 57 c.p. […] Conseguentemente risponde sicuramente del reato di diffamazione l'autore della pubblicazione, ove sia indicato. Ma anche il direttore responsabile della pubblicazione potrà rispondere sia di concorso nel medesimo reato sia autonomamente del reato di cui all'art. 57 c.p. Nel primo caso, occorrerà dimostrare che il direttore ha voluto la pubblicazione nella consapevolezza (dolo) del suo contenuto lesivo della dignità e dell'onore altrui, mentre nel secondo caso si tratterà di un reato autonomo punibile a titolo di colpa, che consiste nel mancato esercizio sul contenuto del periodico del controllo necessario ad impedire che con il mezzo della pubblicazione siano commessi reati». A commento di questa sentenza v. MELZI D'ERIL C., VIGEVANI G. E., *La responsabilità del direttore telematico, tra difficili equiparazioni e specificità di internet*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2010, p. 91 ss.

indistintamente, ma solamente per ragioni amministrative e perché possano essere estese anche al mezzo telematico gli interventi a sostegno del settore editoriale[102].

L'assimilazione è quindi inidonea, in mancanza di una previsione specifica sul punto, a fondare una responsabilità del *provider*.

E' questa la posizione assunta dalla Corte di Cassazione nella sentenza del 16 luglio 2010, n. 35511[103], con la quale, dopo aver ribadito che, per la sostanziale diversità tecnica tra le pubblicazioni cartacee e quelle effettuate in via telematica, è inammissibile l'estensione alle seconde della disciplina penale prevista per le prime, si è escluso fermamente l'eventuale rilevanza della registrazione della pubblicazione telematica ai fini dell'applicabilità di quanto disposto all'art. 57 c.p.

La decisione in esame sembra aver delineato una soluzione univoca grazie ad un interpretazione "costituzionalmente orientata" delle regole dell'informazione

---

[102] Cfr. in tal senso ZENO-ZENCOVICH V., *I «prodotti editoriali» elettronici nella l. 7 marzo 2001 n. 62 e il preteso obbligo di registrazione*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 2/2001, p. 153 ss.; PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, in *Il Diritto dell'Informazione e dell'Informatica*, cit., p. 302 ss.; MELZI D'ERIL C., VIGEVANI G. E., *La responsabilità del direttore telematico, tra difficili equiparazioni e specificità di internet*, cit., p. 99 ss.

[103] Il caso esaminato dalla Corte riguarda un commento anonimo diffamatorio inserito in una sezione dedicata agli interventi di una rivista *on-line* regolarmente registrata. Il direttore di quest'ultima è stato citato in giudizio, per omesso controllo *ex* art. 57 c.p., e condannato sia in primo che in secondo grado. La Cassazione infine ha annullato la sentenza impugnata perché il fatto contestato non è previsto dalla legge come reato. A commento della sentenza cfr. TURCHETTI S., *L'art. 57 c.p. non è applicabile al direttore del periodico online*, in penalecontemporaneo.it, 17 Novembre 2010; MELZI D'ERIL C., *Roma Locuta: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testate giornalistica on line*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2010, p. 895 ss.; ID., *La complessa individuazione dei limiti alla manifestazione del pensiero in Internet*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 4-5/2011, p. 571 ss.; BEVERE A., ZENO-ZENCOVICH V., *La rete e il diritto sanzionatorio: una visione d'insieme*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 3/2011, p. 375 ss.; BETZU M., *Anonimato e responsabilità in internet*, in costituzionalismo.it, n. 2/2011, 6 Ottobre 2011; DIOTALLEVI L., *Internet e Social Network tra "fisiologia" costituzionale e "patologia applicativa",* in *Giurisprudenza di merito*, n. 12/2012, p. 2507 ss.

telematica[104]: nessuno spazio esiste, *de iure condito*, per l'assimilazione della stampa ad Internet e per l'applicabilità alle condotte commesse in rete della disciplina dei reati commessi a mezzo stampa.

Nonostante tali principi siano stati ribaditi dalla Suprema Corte anche nella cd. "sentenza figlia" del 29 novembre 2011, n. 44126[105], negli ultimi anni non sono mancate pronunce di merito e voci in dottrina che hanno riproposto l'opzione assimilazionista, presentandola talora come il risultato di una mera deduzione interpretativa fondata sull'applicazione di un criterio storico sistematico[106], talaltra come operazione necessaria ai fini dell'applicazione al *web* delle garanzie costituzionali previste per gli stampati ai sensi dell'art. 21 Cost.[107].

---

[104] Così MELZI D'ERIL C., *Roma Locuta: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testate giornalistica on line*, cit., p. 900.

[105] V. nota 97.

[106] V. Tribunale di Varese, sent. 22 febbraio 2013, n. 116: «Dall'esame dei lavori preparatori, che come è noto risalgono all'Assemblea Costituente nella sua attività di legislazione ordinaria, emergono, nella seduta del 6 dicembre 1947, nell'ambito della discussione sull'art. 2 (attuale art. 1) della legge recante disposizioni sulla stampa, tre passaggi illuminanti: il presidente e relatore Cevolotto si preoccupa di richiamare – in termini di disciplina liberale da riacquistare - la L. 28 giugno 1906 n. 278, che limitava gli interventi repressivi "delle edizioni, degli stampati e di tutte le manifestazioni del pensiero"; lo stesso relatore segnala la modifica del testo nel senso di ritenere "stampa" qualsiasi riproduzione ottenuta non con "mezzi meccanico-fisici o chimici" bensì "meccanici o chimico-fisici"; il deputato Colitto chiede e ottiene che non si parli di "riproduzioni impresse" bensì, più largamente, "ottenute". Tutto ciò segnala la volontà del legislatore di prevedere, a ogni buon fine, una disciplina che potesse tenere conto del superamento della pura e semplice "impressione con mezzi meccanici" (tale era la primigenia espressione del progetto di legge) di gutenberghiana memoria, rispetto ai progressi della meccanica, della fisica, della chimica; questo progresso ha oggi prodotto una forma di editoria, quella su Internet, del tutto identica (e in alcuni casi anche sostitutiva, con quotidiani *on demand*, su *tablet*, editati a domicilio e così via) a quella che produce caratteri impressi su carta; e del resto, a ben vedere, l'informatica e la telematica altro non sono che applicazione combinata di mezzi (di variazioni di stato) meccanici, fisici, chimici; in questo quadro interpretativo la L. 7 marzo 2001, n. 62, non è fonte di "rilettura" della L. 8 febbraio 1948, n. 47, bensì sopravvenienza coerente (nella sua equiparazione tra più prodotti editoriali) con un concetto di stampa idoneo *ab origine* a ricomprendere la sopravvenienza dei quotidiani o periodici - ora normalmente registrati e oggetto di benefici - su Internet. Se questo è vero, compete peraltro all'interprete attribuire a un sito Internet, sulla base di

Alla luce delle incongruenze riscontrate non si può che auspicare un intervento legislativo che fissi con chiarezza una specifica disciplina per la regolamentazione dell'informazione diffusa via *web*, risultando inaccettabile che il tutto sia rimesso agli esiti per di più ondivaghi dei formanti giurisprudenziale e dottrinale.

In un recente progetto di legge in materia di diffamazione[108], sembra in realtà che il legislatore si stia muovendo verso il fronte opposto rispetto a quello

---

caratteristiche intrinseche e fenomeniche, nonché formali (la registrazione) la natura di "stampa"». Cfr. commento di ROSSETTI S., *Una sentenza di merito sembra eludere l'orientamento negativo della Cassazione in tema di responsabilità del blogger per le affermazioni diffamatorie provenienti dai frequentatori del sito*, in penalecontemporaneo.it, 11 Giugno 2013.

[107] Favorevole all'applicazione analogica alla rete della disciplina prevista dall'art. 21, comma 3, Cost. MELZI D'ERIL C., *La Cassazione esclude l'estensione ai siti internet delle garanzie costituzionali previste per il sequestro degli stampati*, in penalecontemporaneo.it, 25 Marzo 2014, che si pronuncia in termini critici nei confronti della Cassazione penale, sent. 5 novembre 2013, depositata il 5 marzo 2014, n. 10594 (V. nota alla sentenza di CORRIAS LUCENTE. G., *La Cassazione interviene ancora sull'equiparazione fra stampa e giornali telematici*, in medialaws.eu, 20 Marzo 2014). In dottrina perplessità in merito all'analogia in esame sono state sollevate da SEMINARA S., *Internet (diritto penale)*, in *Enciclopedia del diritto* – Annali vol. VII, 2014, p. 567, secondo cui «l'aspirazione a estendere a Internet i presidi in tema di sequestro previsti per la stampa ha finito tuttavia con l'ingenerare un movimento paradossale, che al fine di evitare ogni dilatazione della responsabilità penale ex artt. 57 ss. c.p. si diparte da una situazione di netta diversità e poi approda a una loro assimilazione allo scopo di giustificare l'ampliamento delle garanzie». In tema v. inoltre il recente contributo di PULVIRENTI A., *Sequestro e internet: un difficile binomio tra "vecchie" norme e "nuove" esigenze*, in *Processo penale e giustizia*, n. 1/2015, p. 111 ss. Cfr. infine sentenza Cass. pen., S.U., n. 31022/15. Secondo la Corte il giornale *on-line* al pari di quello cartaceo non può essere oggetto di sequestro preventivo, eccettuato i casi previsti dalla legge, dato che rientrando entrambi nel concetto ampio di "stampa", la diversità di disciplina comporterebbe un'indebita violazione del principio di uguaglianza sostanziale di cui all'art. 3 Cost. In commento v. MELZI D'ERIL C., VIGEVANI G. E., *Tra carta e online parificazione assai discutibile*, in medialaws.eu, 30 Luglio 2015.

[108] Disegno di legge C. 925-B, Proposta di legge: S. 1119. - COSTA: *"Modifiche alla legge 8 febbraio 1948, n. 47, al codice penale, al codice di procedura penale e al codice di procedura civile in materia di diffamazione, di diffamazione con il mezzo della stampa o con altro mezzo di*

tracciato nelle ultime sentenze della suprema Corte, prevedendo una riformulazione dell'art. 57 c.p. in tali termini:

Reati commessi con il mezzo della stampa, della diffusione radio-televisiva o con altri mezzi di diffusione

«Fatta salva la responsabilità dell'autore della pubblicazione, e fuori dei casi di concorso, il direttore o il vicedirettore responsabile del quotidiano, del periodico o della testata giornalistica, radiofonica o televisiva o della testata giornalistica *on line* registrata ai sensi dell'articolo 5 della legge 8 febbraio 1948, n. 47, limitatamente ai contenuti prodotti, pubblicati, trasmessi o messi in rete dalle stesse redazioni, risponde **a titolo di colpa** dei delitti commessi con il mezzo della stampa, della diffusione radiotelevisiva o con altri mezzi di diffusione se il delitto è conseguenza della violazione dei doveri di vigilanza sul contenuto della pubblicazione. La pena è in ogni caso ridotta di un terzo. Non si applica la pena accessoria dell'interdizione dalla professione di giornalista. Il direttore o il vicedirettore responsabile di cui al primo periodo, in relazione alle dimensioni organizzative e alla diffusione del quotidiano, del periodico o della testata giornalistica, radiofonica o televisiva o della testata giornalistica *on line* registrata ai sensi dell'articolo 5 della legge 8 febbraio 1948, n. 47, limitatamente ai contenuti prodotti, pubblicati, trasmessi o messi in rete dalle stesse redazioni, può delegare, con atto scritto avente data certa e accettato dal delegato, le funzioni di controllo a uno o più giornalisti professionisti idonei a svolgere le funzioni di vigilanza di cui al primo periodo.

Il direttore o il vicedirettore responsabile del quotidiano, del periodico o della testata giornalistica radiofonica o televisiva o della testata giornalistica *on line* risponde dei delitti commessi con il mezzo della stampa o della diffusione radiotelevisiva o con altri mezzi di diffusione nei casi di scritti o diffusioni non firmati»[109].

---

diffusione, di ingiuria e di condanna del querelante nonché di segreto professionale. Ulteriori disposizioni a tutela del soggetto diffamato, in camera.it. V. nota 13.

[109] D.d.l. C. 925-B. art. 2, comma 1. La parte in neretto rappresenta le modifiche apportate dal Senato.

E' proprio quest'ultima parte a suscitare non pochi interrogativi e a porsi in apparente contraddizione con le statuizioni che la precedono: il primo comma, infatti, fissa un regime di favore per i direttori delle testate giornalistiche registrate ai sensi dell'art. 5 della l. n. 47/1947, giacché gli stessi rispondono "limitatamente ai contenuti prodotti, pubblicati, trasmessi o messi in rete dalle stesse redazioni"[110], mentre l'ultimo, prevedendo una responsabilità per gli scritti anonimi, sembrerebbe potersi applicare solamente in assenza della registrazione.

A conferma di questo presunto duplice regime differenziato anche la modifica al d.d.l., introdotta dal Senato, concernete l'art 13, comma 1, della l. 47/1948 il quale recita:

Pene per la diffamazione

«1. Nel caso di diffamazione commessa con il mezzo della stampa**, di testate giornalistiche on line registrate ai sensi dell'articolo 5** o della radiotelevisione, si applica la pena della multa **fino a** 10.000 euro. Se l'offesa consiste nell'attribuzione di un fatto determinato falso, la cui diffusione sia avvenuta con la consapevolezza della sua falsità, si applica la pena della multa da **10.000** euro a **50.000** euro»[111].

Lecito quindi chiedersi: che né stato del rispetto del principio di colpevolezza di cui all'art. 27 Cost. nel preciso profilo dell'esigibilità della condotta quale elemento essenziale affinché il rimprovero penale possa dirsi effettivamente personale?[112]

---

[110] L'art. 1 del disegno di legge in questione, prevede in tal senso che all'art. 1 della l. 47/1948 venga aggiunto il seguente comma: «Le disposizioni della presente legge si applicano, altresì, alle testate giornalistiche *on line* registrate ai sensi dell'articolo 5, limitatamente ai contenuti prodotti, pubblicati, trasmessi o messi in rete dalle stesse redazioni, nonché alle testate giornalistiche radiotelevisive».

[111] Ddl C. 925-B. art. 1, comma 5. La parte in neretto rappresenta le modifiche apportate dal Senato.

[112] Purtroppo in tal senso smentite le considerazione di MELZI D'ERIL C., *Roma Locuta: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testate giornalistica on line*, cit., p. 905: «Il Parlamento italiano non pare tra i più solerti nell'accogliere gli stimoli provenienti dalle discussioni nate dal dibattito giuridico a cui danno vita dottrina e giurisprudenza, preferendo − di massima − agire sotto la spinta di episodi che, secondo alcuni, dimostrano emergenze che

Davvero nonostante la specificità della rete, di cui si è ampliamente discusso nel secondo capitolo, l'opzione migliore è *"new wines in old bottles"*?[113]

Una risposta negativa sembra ancor più necessaria se si considera le profonde critiche che, come sottolineato nel primo capitolo del presente lavoro, l'art. 57 c.p. ha da sempre suscitato in ordine al requisito della colpa. In rete, dato l'enorme afflusso di dati e la loro mobilità, tali problematiche si acuiscono e colorano di rinnovato vigore, rendendo drammaticamente attuali vecchi timori: «Come dovrà e potrà esplicarsi tale controllo da parte del direttore o vice-direttore responsabile? Basterà che egli si accerti che il reato non sia rilevabile *ictu oculi* o dovrà risalire alla fonte di tutte le informazioni di cui si dà notizia nel periodico e accertarne personalmente la veridicità? È ovvio che un controllo di tale genere sarebbe sostanzialmente impossibile, almeno nella maggior parte dei casi: onde il rischio che si finisca per ripiegare, nell'applicazione pratica, su un criterio di colpa presunta, ritornando inevitabilmente nel campo della responsabilità oggettiva»[114].

---

sfuggono ai più. Tuttavia, nel caso in cui il potere legislativo intendesse intervenire in materia − intervento che tuttavia oggi pare meno urgente, se la rigorosa impostazione offerta dalla Corte sarà seguita con puntualità − dovrebbe essere lecito confidare per una volta nell'attenzione e nella lungimiranza di quest'ultimo, affinché abbia presente le riflessioni del Supremo collegio e della dottrina. Tenuto conto di come si sta evolvendo l'editoria on line, imporre in capo al direttore di un periodico telematico un obbligo di controllo nel merito di tutto quanto viene diffuso, assistito da una sanzione penale, pone un serio problema di esigibilità della condotta. In questo contesto, probabilmente la scelta peggiore e più miope sarebbe quella di approvare una legge che si limiti a estendere la previsione dell'art. 57 c.p. al prodotto editoriale e, con esso, alla informazione via *web*».

[113] Utile riportare le parole pronunciate dalla Suprema Corte nella sent. n. 35511/10: «Sul piano pratico, poi, non va trascurato che la c.d. interattività (la possibilità di interferire sui testi che si leggono e si utilizzano) renderebbe, probabilmente, vano -o comunque estremamente gravoso- il compito di controllo del direttore di un giornale *on line*. Dunque, accanto all'argomento di tipo sistematico (non assimilabilità normativamente determinata del giornale telematica a quello stampato e inapplicabilità nel settore penale del procedimento analogico *in malam partem*), andrebbe considerata anche la problematica esigibilità della ipotetica condotta di controllo del direttore (con quel che potrebbe significare sul piano della effettiva individuazione di profili di colpa)».

[114] PISAPIA G. D., *La nuova disciplina della responsabilità per reati commessi a mezzo stampa*, cit., p. 321.

4. ERMENEUTICHE GIURISPRUDENZIALI DELLA CORTE EUROPEA DEI DIRITTI DELL'UOMO E DELLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

Occasioni di ripensamento sui rilievi penalistici fin qui esposti sono offerte da alcune delle numerose pronunce registrate nello scenario europeo[115].

Iniziando quest'analisi dall'approccio della Corte europea dei diritti dell'uomo, sembra in primo luogo trovare conferma nelle parole della stessa la non assimilabilità di Internet alla stampa. Il *reasoning* della Corte si fonda sulla particolare diffusività dei contenuti in seguito alla loro immissione nella rete: coinvolgendo milioni di utenti in tutto in mondo, Internet non può essere oggetto delle medesime regole previste per gli altri strumenti di comunicazione e necessita di una disciplina *ad hoc*[116].

---

[115] Cfr. VAN EECKE P., *Online service providers and liability: A plea for a balanced approach*, in *Common Market Law Review*, n. 48/2011, p. 1455 ss.; D'AMBROSIO L., *Responsabilità degli Internet provider e Corte di Giustizia dell'Unione Europea: quali spunti per il sistema penale italiano?*, in LUPARIA L. (a cura di), *Internet Provider e Giustizia Penale*, cit., p. 67 ss.; POLLICINO O., *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, cit.; STAMATOUDI I., TORREMANS P. (eds.), *EU Copyright Law: A Commentary*, Cheltenham-Northampton, 2014, p. 884 ss.

[116] Cfr. Corte europea dei diritti dell'uomo, 5 maggio 2011, n. 33014/05, *Editorial Board of Pravoye Delo e Shtekel c. Ucraina*, § 63: «*the Internet is an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information. The electronic network, serving billions of users world-wide, is not and potentially will never be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned*». La Corte per tale motivo non ha interpretato estensivamente le norme che in base al *Press Act* in vigore in Ucraina disciplinavano l'esonero dei giornalisti dalla responsabilità civile nel caso di riproduzione letterale di materiale pubblicato su stampa.

Attraverso il prisma dell'elaborazione della Corte di Strasburgo le misure adottate nei confronti degli ISPs nel caso di pubblicazioni illegali appaiono innanzitutto subordinate alla tutela della libertà di accesso alla rete. Basti considerare a tal riguardo la sentenza del 18 dicembre 2012 nel caso *Yildrim v. Turchia*[117] con la quale la Corte ha dichiarato il contrasto con l'articolo 10 della Convenzione europea per i diritti dell'uomo (CEDU)[118], in materia di libertà di

[117] Ahmet Yildirim, cittadino turco, è un ricercatore del dipartimento di Ingegneria Informatica all'Università Boğaziçi in Turchia. Appassionato d'informatica, ha creato un sito su *Google Sites* ove pubblica il proprio lavoro accademico nonché personali opinioni in merito a svariate tematiche. Il 24 giugno 2009, tale *blog* venne improvvisamente bloccato: a causa di una presunta pubblicazione di materiale offensivo e denigratorio di Kemal Atatürk, l'eroe nazionale turco fondatore e primo presidente della Repubblica Turca, il tribunale distrettuale di Denizli emise un provvedimento ai sensi dell'art. 8 § 1, lettera b) della legge n. 5651 sulla regolamentazione delle pubblicazioni in Internet, mediante il quale si bloccò l'accesso al *blog*. Il provvedimento, secondo procedura, venne quindi notificato alla Presidenza delle telecomunicazioni e informatica (PTI), che il giorno seguente ordinò il blocco dell'intero *Google Sites*, essendo questa l'unica modalità per impedire totalmente la visualizzazione e l'accesso al *blog*. Dopo che il ricorso avverso tale provvedimento venne respinto dal tribunale, Ahmet Yildirim si rivolse alla Corte europea dei diritti dell'uomo lamentando la violazione dell'art. 10 CEDU. Cfr. PROTO F. R., *Turchia: la censura governativa colpisce ingiustamente il blog di un ricercatore universitario*, in dirittieuropa.it, 9 Gennaio 2013. V. inoltre *Dossier n. 39/0* della Camera dei Deputati: *La tutela del diritto d'autore sulle reti di comunicazione elettroniche*, in documenti.camera.it, 9 Luglio 2013.

[118] Art. 10 CEDU: «**Libertà di espressione** 1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive. 2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario». V. BARTOLE S., DE SENA P., ZAGREBELSKY V., *Commentario breve alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012, p. 397; GRABENWARTER C., *European Convention on Human Rights*, München, 2014, p. 251 ss.

espressione, del provvedimento giurisdizionale turco che, per violazione della legge in materia di diffamazione, aveva inibito l'accesso ad un intero sito Internet[119]. Il caso è di fondamentale importanza perchè affiora in esso una nuova

sfumatura della libertà di espressione ovvero il diritto di accesso illimitato ad Internet[120].

---

[119] In particolare la Corte ha ritenuto che le basi legali offerte dalla legge turca per il blocco del sito, vale a dire l'esistenza di "sufficienti elementi" per "sospettare" che la pubblicazione su Internet contenesse contenuti illegali, rappresentasse una cornice eccessivamente fragile per giustificare la restrizione alla luce dell'art. 10 della Convenzione. Purtroppo recentemente, mascherate da azioni necessarie per la tutela dei minori e per difesa della *privacy* e dei diritti individuali, sono state apportate modifiche alla regolamentazione di Internet che consentono al TIB (autorità governativa nell'ambito delle telecomunicazioni) controlli sempre più invasivi e maggiore possibilità di blocco e censura di pagine *Web* senza la necessità di un ordine del tribunale. Yaman Akdeniz, professore di diritto presso la *Istanbul's Bilgi University* ed importante giurista, ha affermato che: «*It is not just about censorship or control of content, but they are introducing certain mechanisms that I call an Orwellian nightmare (...) I was a little optimistic when the European Court of Human Rights delivered its judgment on the application of a PhD student, Ahmet Yıldırım, with regard to access being blocked to Google sites. It ruled in December 2012 that Law 5651 was incompatible with the European Convention on Human Rights. I was then expecting some positive amendments, but the government disregarded the ruling. On the one hand, I know that some of these measures will be overcome, but at the same time I am concerned that it will have a chilling effect on political discourse. The media has already been forced to self-censorship, and now it will start with the people. People will know these measures exist, so they'll be much more careful*». V. l'interessante intervista "*Turkey's new Internet law is the first step toward surveillance society", says cyberlaw expert*, in hurriyetdailynews.com, 24 Febbraio 2014. V. inoltre RICCI I., *Turchia: la legge bavaglio approda sul Web*, in articolo21.org, 12 Febbraio 2014; VENTURI R., *Turchia: promulgata legge-censura su Internet*, in ilreferendum.it, 21 Febbraio 2014;

Numerosi sono stati i blocchi ordinati a seguito dell'approvazione di tali riforme: da *twitter* a *youtube*. V. *news: La Turchia blocca anche YouTube*, in archivio.internazionale.it, 27 Marzo 2014.

Nell'ottobre 2014 la Coste Costituzionale turca ha dichiarato l'incostituzionalità di tali misure ma nuove proposte di legge tentano un loro rafforzamento. V. *News: Turchia: nuova stretta su Web, a premier e ministri potere di chiudere siti*, in adnkronos.com, 20 Gennaio 2015. Puntuale quindi la nuova pronuncia di condanna della Corte EDU per violazione dell'art. 10 CEDU con sentenza 1 dicembre 2015, n. 376/15, *Cengiz and Others v. Turkey***,** (C-48226/10; C-14027/11).

Le restrizioni all'accesso di contenuti *on-line* sono considerate lecite e rispettose dell'art. 10 CEDU solo nella misura in cui riguardino contenuti specifici e non piattaforme intere o comunque altri contenuti estranei a quelli accusati di violazione.

D'altro canto non si tratta dell'unico diritto tutelato dalla CEDU che grazie all'intervento della Corte viene esteso alle nuove tecnologie: l'art. 8 CEDU[121] in tema di vita privata e corrispondenza nè è tipico esempio. Emblema di questa interpretazione evolutiva che caratterizza l'Organo da più di 50 anni e che mira a potenziare la tutela dei diritti umani in Europa, l'affermazione contenuta in una pronuncia che risale agli inizi degli anni novanta: «*The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle.*

---

[120] Ricordiamo come anche in ambito nazionale non mancano proposte di un *addendum* all'art. 21 Cost. che sancisca l'eguale diritto di tutti i cittadini ad accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale. V. RODOTA' S., *Verso una Dichiarazione dei diritti di Internet*, in camera.it. V. inoltre *news* RE GARBAGNATI E., *Stefano Rodotà: Internet è un diritto costituzionale*, in tomshw.it, 1 Dicembre 2010; DI CORINTO A., *Una Costituzione per la Rete, ecco la bozza punto per punto*, in repubblica.it, 13 Ottobre 2014. Cfr. inoltre FROSINI T. E., A*ccess to internet as a fundamental right*, in *Italian journal of Public Law*, Vol. 5, Issue 2/2013, p. 226; ID., *Libertè, Egalitè, Internet*, in *Percorsi costituzionali*, n. 1/2014, p. 1. MELZI D'ERIL C., VIGEVANI G. E., *Ancora sulla Dichiarazione dei diritti di Internet. Riflessioni sparse in tema di anonimato*, in medialaws.eu, 11 Febbraio 2015.

[121] Art. 8 CEDU: «**Diritto al rispetto della vita privata e familiare** 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». V. BARTOLE S., DE SENA P., ZAGREBELSKY V., *Commentario breve alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, cit., p. 297; GRABENWARTER C., *European Convention on Human Rights*, München, 2014, p. 183.

Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world»[122]. E' proprio questo l'argomento essenziale utilizzato per includere nell'ambito della tutela dell'art. 8 CEDU anche il trattamento automatizzato dei dati personali[123] nonché la posta elettronica[124].

Focalizzando l'attenzione sulla tematica della pubblicazione di contenuti illeciti tramite la rete da segnalare come la Corte di Strasburgo abbia affrontato i diversi casi ponendo quale premessa essenziale delle proprie pronunce l'ormai consolidata teoria del carattere non assoluto delle libertà tutelate dalla CEDU[125].

I bilanciamenti degli interessi contrapposti operati dalla Corte non sono sempre stati esenti da critiche: ad esempio ha suscitato il disappunto di parte della

---

[122] Corte europea dei diritti dell'uomo, 16 dicembre 1992, n. 13710/88, *Niemietz c. Germania.*

[123] Corte europea dei diritti dell'uomo, 4 maggio 2000, *Rotaru v. Romania*; 26 marzo 1987, *Leander v. Sweden*; 6 giugno 2006, *Segerstedt-Wiberg v. Sweden*; 18 novembre 2008, *Cemalettin Canli v. Turkey*. V. inoltre BASILICO A. E., *Tra giurisprudenza inglese e diritti europei: quattro sentenze della nuova Supreme Court*, in rivistaaic.it, 2 Luglio 2010.

[124] Corte europea dei diritti dell'uomo, 3 aprile 2007, n. 62617/00, *Copland c. Regno Unito.*

[125] Cfr. *ex multis* Corte europea dei diritti dell'uomo, 2 dicembre 2008, n. 2872/02, *KU c. Finlandia*: «*Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others*». Con riguardo al bilanciamento tra la libertà di condividere contenuti in Internet o permettere ad altri di farlo, tutelata dal diritto di ricevere e trasmettere informazioni previsto dall'art. 10 CEDU, ed il contrapposto diritto d'autore v. Corte europea dei diritti dell'uomo, 10 gennaio 2013, n. 36769/08, *Ashby Donald e altri c. Francia*; Corte europea dei diritti dell'uomo, 13 marzo 2013, n. 40397/12, *Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) c. Svezia* (con nota di GULINO L., *Svezia: Anche la Corte Europea condanna il sito Pirate Bay*, in dirittieuropa.it, 18 Marzo 2013).

dottrina il caso *Delfi c. Estonia*[126], in relazione al quale non è stata rilevata nei confronti dell'Estonia la violazione dell'art. 10 CEDU sebbene, sulla base della legge nazionale la *Delfi AS*, noto portale e sito di informazione estone, sia stata considerata responsabile dei commenti diffamatori anonimi comparsi sulla propria pagine *web* e per questo condannata per diffamazione, secondo la legge sull'editoria nazionale[127]. L'interferenza dello stato sulla libertà di espressione è stata ritenuta dalla Corte proporzionata e necessaria in una società democratica al fine di proteggere la reputazione e i diritti degli altri consociati[128].

Le polemiche che hanno accompagnato questa pronuncia paiono in realtà inappropriate[129]: la Corte infatti non si è pronunciata sull'applicabilità o meno al caso di specie dei *safe harbours* europei o sulla portata della direttiva *e-Commerce*, essendo tale valutazione di competenza dei giudici nazionali ed eventualmente della Corte di Giustizia. Avvallando l'interpretazione offerta dai giudici estoni il *provider* nel caso specifico risponde per i commenti anonimi ma ciò non significa che la Corte abbia in tal modo scardinato il sistema di tutele

[126] Corte europea dei diritti dell'uomo, 10 ottobre 2013, n. 64569/09, *Delfi c. Estonia*, con commento di GULINO L., *I siti online sono responsabili per i commenti degli utenti. Fine della libertà d'espressione?*, in dirittieuropa.it, 14 Febbraio 2013; VECCHIO M., *Anonimato online? Non per l'editoria digitale*, in punto-informatico.it, 11 Ottobre 2013. La Grande Camera della Corte di Strasburgo ha confermato la sentenza il 16 Giugno 2015 (v. testo in udoc.echr.coe.int). Per un commento v. TAMBURRINO C., *Diritti umani, siti responsabili dei commenti anonimi*, in punto-informatico.it, 18 Giugno 2015.

[127] Alla base della vicenda la pubblicazione sul portale d'informazione di un articolo avente ad oggetto le discutibili scelte operate dalla compagnia di navigazione *Saaremaa Shipping Company* di distruggere le "*Ice roads*", strade di ghiaccio che collegano la terraferma alle numerose isole presenti nel Mar Baltico. I lettori reagirono postando commenti anonimi estremamente offensivi.

[128] Il diritto alla tutela della reputazione è tutelato quale espressione del diritto al rispetto della vita privata di cui all'art. 8 CEDU (v. *ex multis* Corte europea dei diritti dell'uomo, 21 settembre 2010, n. 34147/2006, *Polanco Torres, Movilla Polanco c. Spagna*, § 40).

[129] Tra i commenti che, a parere di chi scrive, offrono un'erronea lettura della sentenza in esame cfr. BIANCHI D., *Post anonimi, la responsabilità è del sito*, in corrierecomunicazioni.it, 11 Ottobre 2013.

previsto a livello comunitario dalla direttiva *e-Commerce*. Il parametro utilizzato dalla Corte, infatti, è solo ed esclusivamente l'art. 10 CEDU[130].

[130] E' la stessa Corte ad affermarlo chiaramente nella sentenza in esame: «*As regards the applicant company's argument that its liability was limited under the EU Directive on Electronic Commerce and the Information Society Services Act, the Court notes that the domestic courts found that the applicant company's activities did not fall within the scope of these acts. The Court reiterates in this context that it is not its task to take the place of the domestic courts. It is primarily for the national authorities, notably the courts, to resolve problems of interpretation of domestic legislation. The Court's role is confined to ascertaining whether the effects of such an interpretation are compatible with the Convention (see, among others, Pérez de Rada Cavanilles v. Spain, 28 October 1998, § 43, Reports of Judgments and Decisions 1998‑VIII*) […] *The fundamental principles concerning the question whether an interference with freedom of expression is "necessary in a democratic society" are well established in the Court's case-law and have been summarised as follows (see, among other authorities, Hertel v. Switzerland, 25 August 1998, § 46, Reports of Judgments and Decisions 1998‑VI; Steel and Morris v. the United Kingdom, no. 68416/01, § 87, ECHR 2005‑II; Mouvement raëlien suisse v. Switzerland [GC], no. 16354/06, § 48, ECHR 2012 (extracts)); and Animal Defenders International v. the United Kingdom [GC], no. 48876/08, § 100, 22 April 2013:*

"(i) Freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment. Subject to paragraph 2 of Article 10, it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness without which there is no 'democratic society'. As set forth in Article 10, this freedom is subject to exceptions, which must, however, be construed strictly, and the need for any restrictions must be established convincingly .

(ii) The adjective 'necessary', within the meaning of Article 10 § 2, implies the existence of a 'pressing social need'. The Contracting States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with European supervision, embracing both the legislation and the decisions applying it, even those given by an independent court. The Court is therefore empowered to give the final ruling on whether a 'restriction' is reconcilable with freedom of expression as protected by Article 10.

(iii) The Court's task, in exercising its supervisory jurisdiction, is not to take the place of the competent national authorities but rather to review under Article 10 the decisions they delivered pursuant to their power of appreciation. This does not mean that the supervision is limited to ascertaining whether the respondent State exercised its discretion reasonably, carefully and in good faith; what the Court has to do is to look at the interference complained of in the light of the case as a whole and determine whether it was 'proportionate to the legitimate aim pursued' and

In merito al problematico contemperamento tra il diritto alla vita privata e la libertà d'espressione anche la decisione *Wegrzynowski e Smolczewski c. Polonia*[131], nella quale la Corte si è trovata a dover valutare se, a seguito della dichiarata diffamatorietà di un articolo di stampa da parte dell'autorità giudiziaria, la sua immissione nell'archivio *on-line* del relativo quotidiano, rendendolo accessibile agli utenti della rete ed indicizzato in tutti i motori di ricerca, sia lesiva dell'art. 8 CEDU.

In primo luogo i Giudici di Strasburgo riconducono gli archivi *on-line* al campo di applicazione dell'art. 10 CEDU precisando che la loro finalità precipua è di assicurare un valido strumento educativo e di ricerca storica[132]. Quindi individuano il punto di equilibro tra la necessità di tutelare anche nel *cyberspace* l'identità personale da attacchi diffamatori e la libera costituzione di archivi *on-line*, non nell'eliminazione dell'articolo, bensì nell'eventuale pubblicazione di una nota che dia conto dell'accertamento giudiziale del carattere diffamatorio[133].

---

whether the reasons adduced by the national authorities to justify it are 'relevant and sufficient'. In doing so, the Court has to satisfy itself that the national authorities applied standards which were in conformity with the principles embodied in Article 10 and, moreover, that they relied on an acceptable assessment of the relevant facts» § 74, § 78.

[131] Corte europea dei diritti dell'uomo, 16 luglio 2013, n. 33846/07, *Wegrzynowski e Smolczewski c. Polonia.* V. commento di DE GRAZIA L., *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso internet: argomenti comparativi*, in rivistaaic.it, 29 Ottobre 2013; NANNIPIERI L., *Il mantenimento di contenuti diffamatori negli archivi online dei quotidiani e la pretesa alla conservazione dell'identità digitale in una recente sentenza della Corte Europea dei Diritti dell'Uomo*, in medialaws.eu, 6 Dicembre 2013.

[132] *Ivi*, § 59: «*Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free*».

[133] Da segnalare come la Corte di Cassazione italiana avesse già manifestato tale orientamento nell'ambito di una causa civile avente ad oggetto la richiesta di aggiornamento di un articolo presente nell'archivio *on-line* di un giornale, in cui veniva narrato dell'arresto del ricorrente, senza la menzione del successivo proscioglimento: sent. 5 marzo 2012, n. 5525, con nota di IASELLI M., *Diritto all'oblio: Cassazione ne conferma il riconoscimento*, in altalex.com, 16 Aprile 2012. In modo particolare la Suprema Corte, che nell'ampia ed articolata motivazione ripercorre l'evoluzione del concetto di *privacy* e ne evidenzia la dimensione dinamica in rapporto alla cronaca giudiziaria ed alle specifiche peculiarità di Internet, afferma che: «Se l'interesse pubblico sotteso al diritto all'informazione (art. 21 Cost.) costituisce un limite al diritto

La tematica è strettamente connessa al cd. diritto all'oblio, inteso quale diritto ad ottenere la rimozione dai motori di ricerca di notizie riguardanti la propria persona o meglio, in senso ampio, a vedersi rappresentati in modo da riflettere la propria attuale dimensione personale e sociale[134], oggetto anche della recentissima

---

fondamentale alla riservatezza (artt. 21 e 2 Cost.), al soggetto cui i dati pertengono è correlativamente attribuito il diritto all'oblio (v. Cass., 9/4/1998, n. 3679), e cioè a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino ormai dimenticate o ignote alla generalità dei consociati […] Il soggetto cui l'informazione oggetto di trattamento si riferisce ha in particolare diritto al rispetto della propria identità personale o morale, a non vedere cioè "travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale" (v. Cass., 22/6/1985, n. 7769), e pertanto alla verità della propria immagine nel momento storico attuale. Rispetto all'interesse del soggetto a non vedere ulteriormente divulgate notizie di cronaca che lo riguardano si pone peraltro l'ipotesi che sussista o subentri l'interesse pubblico alla relativa conoscenza o divulgazione per particolari esigenze di carattere storico, didattico, culturale o più in generale deponenti per il persistente interesse sociale riguardo ad esse. **Un fatto di cronaca può, a tale stregua, assumere rilevanza quale fatto storico,** il che può giustificare la permanenza del dato mediante la conservazione in archivi altri e diversi (es., archivio storico) da quello in cui esso è stato originariamente collocato. […] Atteso che come sopra indicato il principio di finalità costituisce un vero e proprio limite intrinseco del trattamento lecito dei dati personali, emerge allora la necessità, a salvaguardia dell'attuale identità sociale del soggetto cui la stessa afferisce, **di garantire al medesimo la contestualizzazione e l'aggiornamento della notizia già di cronaca che lo riguarda,** e cioè **il collegamento della notizia ad altre informazioni successivamente pubblicat**e concernenti l'evoluzione della vicenda, che possano completare o financo radicalmente mutare il quadro evincentesi dalla notizia originaria, a fortiori se trattasi di fatti oggetto di vicenda giudiziaria, che costituisce anzi emblematico e paradigmatico esempio al riguardo».

[134] Cfr. FROSINI T. E., *Diritto all'oblio e Internet*, in federalismi.it, 10 Giugno 2014: «Il diritto all'oblio (*right to be forgotten*), può ben essere considerato una sorta di reviviscenza del vecchio "diritto a essere lasciati soli" (*right to be left alone*), e quindi un diritto che appartiene <<alle ragioni e alle regioni del diritto alla riservatezza>> (G.B. Ferri), ovvero come <<pretesa a riappropriarsi della propria storia personale>> (C. Chiola), e quindi una sorta di diritto all'autodeterminazione informativa, altrimenti come <<mezzo per ricostruire la dimensione sociale dell'individuo, evitando che la vita passata possa costituire un ostacolo per la vita presente>> (M. Mezzanotte)». In dottrina v. MEZZANOTTE M., *Il diritto all'oblio: contributo allo studio della privacy storica*, Napoli, 2009; MANNA L., *Internet e diritto "all'oblio": una recente sentenza del Tribunale di Milano*, ilsole24ore.com, 29 Luglio 2013; FROSINI T. E., *Internet come ordinamento giuridico*, in *Percorsi costituzionali*, n. 1/2014, p. 13 ss.; FINOCCHIARO G.*, Il diritto all'oblio nel*

pronuncia della Corte di Giustizia dell'Unione europea nel cd. caso *Google/Spagna*[135]. La Corte di Lussemburgo per argomentare il riconoscimento

quadro dei diritti della personalità, in *Il diritto dell'Informazione e dell'Informatica*, 2014, p. 591 ss.; PETTI R., *La protezione dei dati personali e il caso Google Spain*, in dimt.it, 20 Marzo 2015; SENOR M., *Le tensioni del diritto all'oblio*, in medialaws.eu, 21 Aprile 2015; PECORA C., *Diritto all'oblio: il problema della estensione extraeuropea della deindicizzazione tra effettività della rimozione e libertà di informazione*, in medialaws.eu, 18 Settembre 2015. Per l'elaborazione giurisprudenziale italiana del diritto all'oblio v. Cassazione, sent. n. 7769/85; n. 3679/98; n. 5525/12. Interessante infine anche il punto di vista di uno dei più famosi *provider* sul tema: *Report of the Advisory Committee to Google on the Right to be Forgotten*, in rive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view, 6 Febbraio 2015.

[135] Corte di Giustizia dell'Unione europea, 13 maggio 2014, C-131/12, *Google Spain SL,Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* «Dati personali – Tutela delle persone fisiche con riguardo al trattamento di tali dati – Direttiva 95/46/CE – Articoli 2, 4, 12 e 14 – Ambito di applicazione materiale e territoriale – Motori di ricerca su Internet – Trattamento dei dati contenuti in siti web – Ricerca, indicizzazione e memorizzazione di tali dati – Responsabilità del gestore del motore di ricerca – Stabilimento nel territorio di uno Stato membro – Portata degli obblighi di tale gestore e dei diritti della persona interessata – Carta dei diritti fondamentali dell'Unione europea – Articoli 7 e 8». La vicenda inizia nel 1998 quando un quotidiano spagnolo pubblica anche nella sua versione *on-line* la notizia relativa alla vendita tramite asta di alcuni immobili appartenenti al Sig. González, stabilita in seguito ad un procedimento esecutivo per debiti contratti con il sistema previdenziale. Undici anni dopo, nel 2009, il diretto interessato contatta l'editore della testata, chiedendo la cancellazione dell'articolo in quanto, nonostante il pignoramento effettuato nei suoi confronti fosse già stato interamente definito da svariati anni, cercando il proprio nome su *Google* tra i primi *link* indicizzati compaiono proprio quelli riguardanti la vicenda. La richiesta viene respinta pertanto il Sig. González si rivolge direttamente alla divisione spagnola del motore di ricerca, che chiama in causa la sede californiana in quanto fornitrice del servizio. A metà 2010 il direttore dell'AEPD (*Agencia Española de Protección de Datos*) ordina a *Google Spain* e *Google Inc.* la rimozione dei dati in questione dalle SERP (pagine dei risultati), ma il motore di ricerca chiede l'annullamento della sentenza impugnandola dinanzi al giudice. Si arriva così alla decisione della Corte di Giustizia con la quale viene riconosciuto a González il diritto alla cancellazione dei *link* considerati lesivi per la propria reputazione. La portata innovativa della pronuncia si rinviene anche sotto l'aspetto dell'ampliamento dell'ambito applicativo della direttiva europea in materia di *privacy*. I giudici comunitari hanno infatti stabilito che l'applicazione della direttiva «non esige che il trattamento di dati personali in questione venga effettuato "dallo" stesso stabilimento interessato, bensì soltanto che venga effettuato "nel contesto delle attività" di quest'ultimo». Cfr. *News* di BOTTA' G., *UE: Google sia arbitro dell'oblio*, in punto-informatico.it, 13 Maggio 2014.

del diritto all'oblio ed attuare il corretto bilanciamento tra lo stesso ed il diritto all'informazione, utilizza il criterio della "finalità del trattamento" e del "tempo trascorso"[136]. Posto che il gestore di un motore di ricerca esplorando Internet in modo automatizzato, costante e sistematico per il rintracciamento di informazioni nonché raccogliendo dati, estraendoli, registrandoli e organizzandoli nell'ambito di programmi di indicizzazione[137] deve essere qualificato come «responsabile del trattamento di dati personali» ai sensi dell'art. 2 della direttiva 95/46/CE del Parlamento europeo e del Consiglio[138], i Giudici di Lussemburgo ne hanno

---

V. commenti di FLOR R., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, in *Il Diritto dell'Informazione e dell'Informatica*, 2014, p. 775 ss.; ID., *Nuove tecnologie e giustizia penale in Europa, tra le esigenze di accertamento e prevenzione dei reati e quelle di tutela della riservatezza: il ruolo «propulsore» della Corte di Giustizia*, cit.; SICA S., D'ANTONIO V., *La procedura di de-indicizzazione*, in *Il Diritto dell'Informazione e dell'Informatica*, 2014, p. 703 ss.; PASTENA R., *Internet e privacy: una relazione complicata (A margine della sentenza della Corte di Giustizia del 13 maggio 2014)*, in osservatorioaic.it, Luglio 2014; RICCIO M. G., *Diritto all'oblio e responsabilità dei motori di ricerca*, in *Diritto dell'Informazione e dell'Informatica,* 2014, p. 753 ss.

[136] Come specificato dalla Corte qualora la conservazione dei dati si imponga per motivi storici, statistici o scientifici, il concetto di tempo come limite alla finalità lecita di un trattamento legittimo non troverà applicazione in ossequio all'art. 6 lett. b) della direttiva sulla *privacy*. V. par. 72 e 92 CGUE 13.05.14, C-131/12.

[137] Il *software "crawler"* (detto anche *web crawler*, *spider* o *robot*), che analizza i contenuti della rete in un modo metodico e automatizzato per conto del motore di ricerca *Google* è denominato *"googlebot"*. Quest'ultimo perlustra *Internet* in modo costante e sistematico, acquisisce una copia testuale di tutti i documenti visitati ed infine li inserisce in un indice. Il complesso algoritmo di ricerca di *Google* valuta inoltre la rilevanza dei risultati della ricerca. Ai fini dell'indicizzazione e della visualizzazione dei risultati, la copia delle pagine viene registrata nella memoria *cache* del motore di ricerca. Cfr. voci *Googlebot* e *Crawler* in wikipedia.org.

[138] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, *"Relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"*, pubblicata sulla G.U. del 23.11.1995. La direttiva costituisce il testo di riferimento, a livello europeo, in materia di protezione dei dati personali e fissa limiti precisi per la raccolta e l'utilizzazione degli stessi. Ai sensi dell'art. 2 per *dati personali* si intende «qualsiasi informazione concernente una persona fisica identificata o identificabile», per *trattamento di dati personali* invece «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di

dichiarato l'obbligo**,** in determinate condizioni, di sopprimere, dall'elenco dei risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, *link* verso pagine *web* pubblicate da terzi contenenti informazioni relative a tale soggetto. Alla base di tale affermazione la costatazione del fatto che qualsiasi utente, digitando il nome di una persona fisica ottiene, grazie all'elenco di risultati forniti dal motore di ricerca, una visione complessiva strutturata delle svariate informazioni ad essa riferibili pubblicate in Internet. Questa sorta di tracciamento del profilo di un soggetto sarebbe impossibile o per lo meno molto difficoltosa senza l'attività del *provider*, che pertanto detiene un forte potere d'ingerenza sui diritti fondamentali alla vita privata e alla protezione dei dati personali[139]. Quest'ultimi, a parere della Corte, devono prevalere sull'interesse economico del gestore del motore di ricerca ma anche sull'interesse del pubblico ad avere accesso alle medesime informazioni fatta eccezione per i casi in cui, viceversa, l'ingerenza sia giustificata da ragioni particolari, quale ad esempio il ruolo ricoperto da tale persona nella vita pubblica. Pertanto, qualora i dati risultino inadeguati, non pertinenti o non più pertinenti ovvero eccessivi in rapporto alle finalità per le quali sono stati trattati il soggetto ha il diritto di richiedere, al gestore prima, e alle autorità competenti poi, che dei *link* verso pagine *web* siano cancellati dall'elenco offerto dai motori di ricerca. Le informazioni quindi

---

processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione». E*x* art. 2 lett. d) il *responsabile del trattamento* viene definito come «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario».

[139] «L'effetto dell'ingerenza nei suddetti diritti della persona interessata risulta moltiplicato in ragione del ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono alle informazioni contenute in un siffatto elenco di risultati carattere ubiquitario (v., in tal senso, sentenza eDate Advertising e a., C-509/09 e C-161/10, EU:C:2011:685, punto 45)». CGUE 13.05.14, C-131/12, punto 80.

sopravvivono al *delisting*, il quale non incide sull'esistenza della notizia, bensì sulla sua "visibilità", complicandone il reperimento da parte degli utenti[140] .

Gli ISPs, nella specifica attività di motori di ricerca, avrebbero l'obbligo di garantire *"the righ to be forgotten"* degli utenti o meglio il loro diritto ad essere derubricati/de-indicizzati[141]. La sentenza in esame si discosta nettamente dall'orientamento giurisprudenziale espresso dalla Corte di Cassazione italiana[142] secondo la quale l'eventuale richiesta di cancellazione, rimozione ovvero di modifica dei dati dovrebbe essere rivolta ai siti sorgente e non al gestore del

[140] «Gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, al fine di rispettare i diritti previsti da tali disposizioni, e sempre che le condizioni da queste fissate siano effettivamente soddisfatte, il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita». *Ivi*, dispositivo punto 3.

[141] Dopo la pronuncia esaminata *Google* ha reso disponibile sul web un *form* attraverso cui chiedere la rimozione dei *link* ritenuti inadeguati o non più pertinenti, e istituito al suo interno l'*Advisory Council on The Right to be forgotten*, comitato direttivo di dieci esperti deputato a vagliare le singole richieste, e dunque a stabilire i criteri di applicazione del diritto all'oblio. Le autorità europee che si occupano di tutela della *privacy*, radunate nel gruppo di lavoro *"Article 29"*, hanno cercato di specificare in alcune linee guida i criteri della "non rilevanza" e "non attualità" sulla base dei quali i *providers*, a seguito della richiesta dei soggetti interessati, dovrebbero procedere alla de-indicizzazione dei *link*. Il documento, rivolto alle autorità nazionali, afferma che se un operatore attraverso le sue controllate offre servizi in più Paesi membri dell'Unione la deindicizzazione dovrebbe avvenire su tutti i domini rilevanti, inclusi i ".com". Al momento, invece, *Google* e gli altri motori di ricerca applicano la disciplina europea solo alle versioni nazionali europee dei propri siti. V. Article 29 Data Protection Working Party, *"Guidelines on the implementation of the Court of Justice of the European Union judgment on Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/121"*, WP 225, 26 Novembre 2014.

[142] Cassazione civile, sent. 5 Marzo 2012, n. 5525 con nota di IASELLI M., *Diritto all'oblio: Cassazione ne conferma il riconoscimento*, in altalex.com, 16 Aprile 2012; DI MINCIO S., *Diritto all'oblio e la sentenza della Corte di Giustizia dell'UE del 31 Maggio 2014*, in *Il Documento Digitale*, n. 2/2014.

motore di ricerca in quanto quest'ultimo, ad eccezione delle ipotesi in cui compia un'attività di trasformazione degli stessi, è intermediario telematico, mero *database* che assolve la funzione di semplice trasporto delle informazioni. La Corte di Giustizia, al contrario, rileva la violazione del diritto all'oblio proprio in ragione dell'indicizzazione dei dati compiuta dal motore di ricerca, il quale, mediante tale attività, crea un'immagine sociale dell'individuo distorta, o comunque non più attuale.

Nonostante la questione sia stata sollevata nell'ambito di procedimenti civili, la decisione comunitaria è essenziale per il ripensamento dell'eventuale configurabilità di una responsabilità anche penale dell'ISP: il ruolo del motore di ricerca quale "responsabile del trattamento dati" viene infatti notevolmente accresciuto in vista di una maggiore tutela dell'utente, superando il principio della neutralità di cui alla direttiva *e-Commerce.*

Quanto mai corrette allora, alla luce di tali considerazioni, le doglianze della Procura Generale della Repubblica che, nell'impugnare la sentenza del Tribunale di Milano nel famoso caso *Google v. Vivi Down*[143], riteneva sussistente la penale

[143] V. nota 64 per i riferimenti giurisprudenziali e dottrinali. Come noto, il processo ha inizio nel 2006 con la pubblicazione su *Google Video* di un video che mostra alcuni ragazzini in un edificio scolastico umiliare un compagno affetto dalla sindrome di Down e insultare l'associazione. Il video in questione viene rimosso due mesi dopo, in seguito a numerose segnalazioni degli utenti e ril'intervento della polizia postale.

Tre *manager* di *Google* venivano imputati dei reati di cui agli artt. 40 cpv. e 595 c.p., per omesso impedimento del delitto di diffamazione nei confronti del minore e dell'associazione, e di cui all'art. 167 d.lgs. 196/2003, per trattamento illecito dei dati personali riguardanti lo stato di salute del ragazzo. In primo grado il Tribunale di Milano assolveva i *manager* dal concorso omissivo nel delitto di diffamazione, data l'inesistenza di un obbligo per i *providers* di prevenire i reati dei propri utenti nonché l'impossibilità tecnica di un tale controllo, mentre riteneva integrato il reato di illecito trattamento dei dati, in quanto *Google* non aveva preventivamente avvisato i propri utenti riguardo agli obblighi previsti in materia di dati sensibili secondo il disposto di cui all'art. 13 del Codice *privacy*. In sede di gravame, la Corte d'Appello di Milano, confermava l'assenza dell'obbligo giuridico in capo a *Google* di impedire eventuali reati da parte dei propri utenti, e annullava la condanna per la seconda accusa sostenendo che nell'attività di offerta di servizi di *upload* il *provider* non "tratta dati" e può ben beneficiare delle limitazioni di responsabilità previste dagli artt. 16 e 17 del d.lgs. 70/2003. Secondo la Corte, inoltre, alcun dovere potrebbe trarsi dal combinato disposto dell'art. 167 con l'art. 13 del Codice *privacy*, alla

responsabilità del noto *provider* per il reato di cui all'art. 167 d.lgs. 196/2003[144], in quanto nell'ambito del servizio *Google Video* non si limitava ad offrire un mero spazio per l'*upload* di video, ma eseguiva una indicizzazione e catalogazione del materiale caricato[145], effettuando quindi il trattamento dei dati personali del minore disabile ripreso nel video riconducibile all'art. 4, comma 1, lett. a) del Codice *privacy*[146]. E' lo stesso d.lgs. 70/03 a prevedere l'esclusione della sua

---

cui violazione è per lo più connessa una mera sanzione amministrativa *ex* art. 161. Infine la Suprema Corte, chiamata a pronunciarsi sulla questione, ribadendo l'assenza di una previsione normativa che imponga all'*host provider* un generale obbligo di impedire condotte illecite degli utenti, negava la possibilità di riconoscere in capo a *Google* un effettivo trattamento dei dati contenuti nel video caricato, dato che nella figura tipizzata del "titolare del trattamento dati" non può essere ricompreso qualsiasi soggetto che materialmente svolge l'attività stessa ma solo colui che ne determina gli scopi, i modi ed i mezzi. Nel caso di specie quindi si riconosce al *provider* la possibilità di godere dei *safe harbours* fissati nella direttiva *e-Commerce*, essendosi limitato a memorizzare contenuti senza intervenire in alcun modo su essi ed avendo provveduto alla loro rimozione non appena avvisato dall'autorità circa la loro illiceità.

[144] Ex art. 167 d.lgs. 196/03: «1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni». Secondo la pubblica accusa pur richiedendo l'art. 167 del Codice *privacy* la finalità di profitto, è sufficiente che il lucro sia perseguito e non effettivamente percepito: il reato in esame sarebbe configurabile dato che gli imputati, in sostanza, avrebbero volontariamente violato gli obblighi fissati dal Codice *privacy* in modo tale da riuscire ad ottenere dalla sua permanenza in rete un introito economico attraverso l'inserimento di *link* pubblicitari.

[145] Il video è stato "lavorato" dal *provider* giacché è stato inserito tra i video più divertenti e più visti: c'è quindi un *quid pluris* rispetto alla semplice tolleranza all'inserimento del contenuto da parte degli utenti e alla mancata rimozione. A parere di chi scrive, sussistono i presupposti per l'applicazione non solo del reato di illecito trattamento di dati personali, ma anche del concorso dell'ISP nel reato di diffamazione.

[146] *Ex* art. 4, comma 1, d.lgs. 196/03 il "trattamento" si identifica con «qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la

applicabilità nella materia specifica della tutela della riservatezza[147] e, forse, data la differenza dei beni giuridici protetti dalle disposizioni in esame ovvero la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico per quanto riguarda il decreto attuativo della direttiva *e-Commerce*, e della vita privata con riguardo al trattamento dei dati personali nel caso del Codice *privacy*, una distinta configurabilità delle responsabilità degli ISPs pare non solo rigorosamente logica ed in linea con i principi cardine del diritto penale sostanziale, quali il principio di proporzionalità ed adeguatezza, ma per lo più di buon senso.

Nell'ottica di una tutela differenziata e rafforzata dei diritti fondamentali delle persone, ed in modo particolare della protezione dei dati, si pone anche l'ulteriore recente sentenza della Corte di Giustizia nel cd. caso *Facebook*[148], con la quale si

---

raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati».

[147] Ai sensi dell'art. 1, comma 2, lett. b), d.lgs. 70/03 non rientrano nel campo d'applicazione dello stesso: «le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675 e al decreto legislativo 13 maggio 1998, n. 171 e successive modifiche e integrazioni».

[148] Corte di Giustizia dell'Unione europea, 6 ottobre 2015, C-362/14, *Maximillian Schrems/Data Protection Commissioner*, «Rinvio pregiudiziale – Dati personali – Protezione delle persone fisiche con riguardo al trattamento di tali dati – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 47 – Direttiva 95/46/CE – Articoli 25 e 28 – Trasferimento di dati personali verso paesi terzi – Decisione 2000/520/CE – Trasferimento di dati personali verso gli Stati Uniti – Livello di protezione inadeguato – Validità – Denuncia di una persona fisica i cui dati sono stati trasferiti dall'Unione europea verso gli Stati Uniti – Poteri delle autorità nazionali di controllo». Il caso di specie trae origine dalla denuncia presentata dall'attivista austriaco Maximilian Schrems alla autorità irlandese concernente l'inadeguatezza della tutela apprestata dal diritto americano contro la sorveglianza di massa operata tramite trasferimento dei dati. Quale utente del famoso *social-network Facebook* dal 2008, Schrems, alla luce delle rivelazioni fatte nel 2013 dal sig. Edward Snowden in merito alle attività dei servizi di *intelligence* negli Stati Uniti (in particolare della *National Security Agency*), esprime dubbi sulla validità della decisione 2000/520/CE con la quale la Commissione Europea ha ritenuto che, nel contesto del cosiddetto

sancisce l'inammissibilità di una sua compromissione attraverso forme di sorveglianza generalizzate realizzate da parte di autorità di Paesi terzi. La tutela si estende quindi anche al di fuori dei confini europei. In linea con quanto già affermato dall'Avvocato Generale Yves Bot[149] la Corte riconosce che nel diritto dell'Unione non può essere considerata accettabile una normativa che autorizza la conservazione generalizzata dei dati personali trasferiti dall'Unione verso gli Stati Uniti senza la fissazione precisa e specifica di limitazioni o eccezioni funzionali dell'obiettivo perseguito, nonchè di criteri oggettivi che circoscrivano l'accesso e l'utilizzazione dei dati da parte delle autorità pubbliche[150]. Sulla base del

---

regime di "approdo sicuro" (*Safe Harbor*), gli Stati Uniti garantiscano un livello adeguato di protezione dei dati personali trasferiti. L'autorità irlandese respinge la denuncia, e, in seguito la *High Court of Ireland* (Alta Corte di giustizia irlandese), investita della causa, si rivolge alla Corte di Giustizia al fine di sapere se la decisione della Commissione impedisca ad un'autorità nazionale di controllo di indagare su una denuncia con cui si lamenta che un Paese terzo non assicura un livello di protezione adeguato e, se necessario, di sospendere il trasferimento di dati contestato. In commento v. *Facebook: dichiarazione di Antonello Soro sulla sentenza della Corte di Giustizia Europea*, in garanteprivacy.it, 6 Ottobre 2015; BOTTA' G., *Safe Harbor, le garanzie non bastano*, in punto-informatico.it, 6 Ottobre 2015; IASELLI M., *Caso Facebook, il "Safe harbor" si può disapplicare: una svolta epocale?*, in altalex.com, 18 Ottobre 2015, UNGARO S., MAIO E., *Ma la "sentenza Facebook" non invalida il safe harbour: ecco perché*, in agendadigitale.eu, 18 Ottobre 2015. Per una visione complessiva del sistema *Safe Harbour* v. voce *U.S.-EU Safe Harbor* in export.gov. Da segnalare come, con l'adesione a tale accordo, le aziende statunitensi si vincolano al rispetto di sette principi ovvero: informare l'interessato circa le modalità di raccolta e utilizzo dei dati; consentire all'interessato di rifiutare il trasferimento dei dati a terzi; vincolare i terzi cui siano trasferiti i dati ad applicare adeguate misure di protezione; garantire la protezione dei dati contro perdite, intrusioni, alterazioni; utilizzare i dati per le sole finalità per cui sono stati raccolti; consentire agli interessati l'accesso e la correzione o cancellazione dei dati; attivare meccanismi di verifica della conformità dei sistema di raccolta a questi principi.

[149] V. Conclusioni dell'avvocato generale Yves Bot presentate il 23 settembre 2015 in curia.europa.eu; Cfr. inoltre *Facebook, avvocato generale Corte di Giustizia: "Stati possono impedire trasferimento dati degli iscritti verso Usa"*, in dimt.it, 23 Settembre 2015.

[150] La Corte non verifica nemmeno se il sistema americano di "approdo sicuro" garantisca o meno un livello di protezione sostanzialmente equivalente a quello assicurato nell'Unione, stante la sua applicazione alle sole imprese americane che lo sottoscrivono e non alle autorità pubbliche degli Stati Uniti. Inoltre la Corte precisa che, in conformità all'allegato I, quarto comma, della decisione 2000/520, le esigenze afferenti alla sicurezza nazionale, al pubblico interesse e

dispositivo della sentenza in questione, pur essendo solo la Corte competente a dichiarare invalido un atto dell'Unione, le autorità nazionali di controllo investite di relativa richiesta, anche se esiste una decisione della Commissione come nel caso di specie, potranno valutare in piena indipendenza se il trasferimento dei dati di una persona verso un Paese terzo rispetta i requisiti della normativa dell'Unione sulla protezione di tali dati (fatta salva la possibilità di adire i giudici nazionali affinché procedano ad un rinvio pregiudiziale). L'esistenza di una decisione della Commissione che dichiara che un Paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei diritti fondamentali dell'Unione europea e della direttiva 95/46/CE.

La pronuncia in esame quindi costituisce sicuramente un forte incoraggiamento verso una regolamentazione più attenta del trattamento dei dati dei cittadini europei da parte degli ISPs. Un invito esplicito ad un confronto tra istituzioni e aziende europee e americane che porti alla elaborazione di un nuovo accordo rispettoso dei diritti fondamentali è stato raccomandato anche dal Gruppo di Lavoro "*Article 29*". Secondo quanto stabilito nella relativa decisione dei garanti della *privacy* europei riuniti *"If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions"*[151].

---

all'osservanza delle leggi statunitensi prevalgono sul regime dell'approdo sicuro, cosicché le imprese americane sono tenute a disapplicare, senza limiti, le norme di tutela previste dal regime laddove queste ultime entrino in conflitto con tali esigenze, rendendo possibili ingerenze da parte delle autorità pubbliche americane nei diritti fondamentali delle persone senza che nella decisione della Commissione vi sia menzione circa l'esistenza, negli Stati Uniti, di norme intese a limitare queste eventuali ingerenze, né l'esistenza di una tutela giuridica efficace contro le stesse. Cfr. sent. in esame punti 82 e ss.

[151] V. *Statement of the Article 29 Working Party*, in ec.europa.eu, 16 Ottobre 2015. Cfr. *News* di BOTTA', *Privacy UE, tre mesi per un nuovo Safe Harbor*, in punto-informatico.it, 20 Ottobre 2015.

Venendo ora ad esaminare il preciso ambito di applicazione della direttiva *e-Commerce*, la Corte di Giustizia in più occasioni ha evidenziato come l'esonero dalla responsabilità per i contenuti caricati dagli utenti si applica al prestatore di un servizio *on-line* che li ospita qualora non abbia svolto un ruolo attivo che gli permetta di avere conoscenza o controllo circa i dati memorizzati, ovvero, in assenza di tale ruolo salvo che, abbia prontamente rimosso i contenuti non appena venuto a conoscenza della natura illecita degli stessi. Così ad esempio si è espressa la Corte di Giustizia nella sentenza del 12 luglio 2011[152] sulla controversia sorta tra l'azienda *L'Orèal SA* ed il noto portale *eBay*: pur essendo pacifico che il gestore del mercato *on-line* memorizza sul proprio *server* dati forniti dai suoi clienti e riscuote una percentuale sulle operazioni di compra-vendita effettuate, solo laddove detto gestore abbia prestato un'assistenza consistente segnatamente nell'ottimizzare la presentazione delle offerte in vendita di cui trattasi e nel promuoverle, non potrà essere considerato in posizione "neutrale" e quindi non potrà avvalersi della deroga in materia di responsabilità di cui all'art. 14 della direttiva 2000/31.

[152] Corte di Giustizia dell'Unione europea, 12 luglio 2011, causa C-324/09, *L'Orèal SA/eBay*, «Marchi – Internet – Offerta in vendita, in un mercato online destinato ai consumatori nell'Unione, di prodotti contrassegnati da un marchio destinati, dal titolare, ad essere venduti negli Stati terzi – Eliminazione dell'imballaggio di detti prodotti – Direttiva 89/104/CEE – Regolamento (CE) n. 40/94 – Responsabilità del gestore del mercato online – Direttiva 2000/31/CE ("direttiva sul commercio elettronico") – Ingiunzioni giudiziarie nei confronti di tale gestore – Direttiva 2004/48/CE ("direttiva sul rispetto dei diritti di proprietà intellettuale")». La vicenda trae origine da alcune aste nelle quali utenti di *eBay*, senza il consenso di *L'Oréal*, avevano messo in vendita prodotti di quest'ultima. In due casi gli articoli erano per lo più contraffatti. Nelle altre aste, invece, emergevano profili di incompatibilità con il diritto di proprietà intellettuale della società francese, avendo le stesse ad oggetto beni non destinati alla vendita o al mercato europeo. La questione della responsabilità del *provider* sarebbe connessa non solo al far comparire, sul sito del gestore di un mercato *on-line*, segni identici o simili a marchi, ma anche al fatto che, nell'ambito del servizio di posizionamento *AdWords* di Google, digitando le parole chiave "*L'Oréal"*, era possibile raggiungere i prodotti in questione per mezzo di *link* pubblicitario verso il sito www.ebay.co.uk, accompagnato da un messaggio commerciale vertente sulla possibilità di acquistare prodotti della marca attraverso il suddetto sito.

La Corte rimette quindi al giudice nazionale la difficile valutazione circa il ruolo svolto dal *provider* e la sussistenza della conoscenza della natura illecita dei dati o delle attività degli utenti[153].

In modo particolare a parere di chi scrive se, così come affermato dalla Corte di Appello di Milano nella recente sentenza *Yahoo!/RTI*, la semplice funzione di indicizzazione automatica dei contenuti ospitati non può essere considerata come elaborazione degli stessi che travolge elidendolo il carattere neutrale dell'*hosting provider*, ad identica conclusione non potrebbe giungersi con riguardo all'uso pubblicitario di parole chiave e *link* sponsorizzati contenenti riferimenti a prodotti la cui originalità non è garantita. Il *provider* infatti che seleziona presso il gestore del motore di ricerca parole chiave, facendo comparire, dall'inserimento ad opera degli utenti Internet in tale motore di ricerca di una richiesta contenente dette parole chiave, *link* pubblicitari verso il proprio sito accompagnato da messaggi commerciali non può che essere considerato come un'inserzionista e "utilizzatore" del marchio ai sensi dell'art. 5, n. 1, lett. a), della direttiva 89/104 e dell'art. 9, n. 1, lett. a), del regolamento n. 40/94 in relazione a prodotti in commercio sul mercato allorché utilizza un segno identico ad un marchio nella

[153] Ad analoga conclusione era giunta la Corte anche in una precedente sentenza concernente il servizio di *Adwords* offerto da *Google*: Corte di Giustizia dell'Unione europea, 23 marzo 2010, causa C-236/08, *Google France SARL e Google Inc./Louis Vuitton Malletier* riunita con causa C-237/08, *Google France SARL/Viaticum SA e Luteciel SARL* e C-238/08 e *Google France SARL/Centre national de recherche en relations humaines (CNRRH) SARL* e altri. La Corte, dopo aver fissato alcune indicazioni di principio fondamentali quali la riconducibilità del prestatore di un servizio di posizionamento su Internet che memorizza come parola chiave un segno identico a un marchio e organizza, a partire da quest'ultima, la visualizzazione di annunci, alla categoria dell'*hosting provider* e non a quella di "utilizzatore" del marchio ai sensi dell'art. 5, nn. 1 e 2, della direttiva 89/104 o dell'art. 9, n. 1, del regolamento n. 40/94, afferma che spetta quindi al giudice nazionale, che meglio può conoscere le modalità concrete della fornitura del servizio nel caso specifico, valutare se il ruolo svolto dal *provider*, in particolare nella redazione del messaggio commerciale che accompagna il *link* pubblicitario o nella determinazione o selezione di tali parole chiave, sia "attivo" ovvero atto a conferirgli la conoscenza o il controllo dei dati memorizzati. In realtà nella maggior parte dei casi le controversie di questo tipo si concludono mediante accordi tra le stesse aziende. V. ad esempio *News "ebay scende a patti con lvmh: basta falsi vuitton"*, in rainews.it, 17 luglio 2014.

propria pubblicità[154]. Sembrerebbe quindi che tale attività ben potrebbe rientrare in quella tipologia di "ottimizzazione" dell'offerta ed elaborazione dati incompatibile con la funzione di *hosting* per la quale è prevista l'esenzione di responsabilità di cui all'art. 14 della direttiva *e-Commerce*.

La Corte di Giustizia, come poc'anzi ricordato, non entra comunque nel merito e sancisce la competenza dell'autorità nazionale nel garantire un giusto equilibrio tra la tutela del marchio e il libero esercizio da parte degli ISP della propria attività commerciale.

Alla stessa conclusione la Corte approda anche nel successivo caso *Scarlet/Sabam*[155] in tema di proprietà intellettuale e diritto d'autore con l'ulteriore

[154] Cfr. Conclusioni dell'avvocato generale Niilo Jääskinen presentate il 9 dicembre 2010, Causa C‑324/09, punti 89 e 103 e ss.: «Come giustamente osservato dalla Commissione in relazione all'uso, sul sito Internet del gestore di un mercato online, di un segno identico ad un marchio protetto, tale sito Internet presenta un certo contenuto, vale a dire il testo delle offerte fornite dai venditori, che sono i destinatari del servizio, e memorizzate su loro richiesta. Laddove gli annunci vengano caricati dagli utenti senza che il gestore del mercato online effettui ispezioni o controlli preliminari che implicano un'interazione tra persone fisiche che rappresentano il gestore e l'utente , siamo in presenza di una memorizzazione di informazioni fornite dal destinatario del servizio. In tali circostanze, il gestore di un mercato online non è effettivamente al corrente dell'attività o dell'informazione illecite. E neppure sarebbe al corrente di fatti o circostanze che rendano manifesta l'illiceità dell'attività o dell'informazione. Di conseguenza, non sussisterebbero le condizioni della deroga in materia di responsabilità per l'hosting, quali definite all'art. 14 della direttiva 2000/31. Tuttavia, per quanto riguarda un servizio di posizionamento a pagamento su Internet e l'uso di un segno identico ad un marchio protetto nei link sponsorizzati del gestore di un mercato online, l'informazione non viene memorizzata da tale gestore, che agisce in tal caso come un inserzionista, ma piuttosto dal prestatore del servizio di posizionamento su Internet che gestisce il motore di ricerca. Pertanto, le condizioni dell'hosting, quali definite all'art. 14 della direttiva 2000/31, non sono soddisfatte a tal riguardo con riferimento al gestore del mercato online […] Dall'argomento sopra esposto risulta che il gestore continua a beneficiare della deroga relativa alle attività rientranti nell'ambito di applicazione dell'art. 14, n. 1, della direttiva 2000/31. Tuttavia, egli non fruisce della deroga per le attività che ne sono escluse. Tale situazione deve essere valutata sulla base delle disposizioni e dei principi pertinenti di diritto nazionale, in particolare per quanto riguarda la concessione del risarcimento dei danni o di altre compensazioni economiche per le attività cui non è applicabile alcuna deroga».

[155] Corte di Giustizia dell'Unione europea, 24 novembre 2011, C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, «Società

essenziale precisazione che, il diritto dell'Unione, ed in modo particolare l'art. 15 n. 1) della direttiva *e-Commerce*, vieta un'ingiunzione di un giudice nazionale diretta ad imporre ad un *provider* di predisporre un sistema di filtraggio generalizzato[156] per prevenire gli scaricamenti illegali di *file*. La sorveglianza in questione oltre ad essere contraria alle condizioni stabilite dall'art. 3, n. 1, della direttiva 2004/48, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose, violerebbe i diritti fondamentali degli utenti alla tutela dei dati personali e alla libertà di ricevere o di comunicare informazioni, tutelati dalla Carta dei diritti fondamentali dell'Unione europea agli artt. 8 e 11[157]. Tale tipologia di

---

dell'informazione – Diritto d'autore – Internet – Programmi "peer-to-peer" – Fornitori di accesso a Internet – Predisposizione di un sistema di filtraggio delle comunicazioni elettroniche al fine di impedire gli scambi dei file che ledono i diritti d'autore – Assenza di un obbligo generale di sorvegliare le informazioni trasmesse». Questa causa è scaturita da una controversia tra l'ISP Scarlet Extended SAe la SABAM, società di gestione belga incaricata di autorizzare l'utilizzo da parte di terzi di determinate opere musicali. Dopo aver scoperto che, avvalendosi dei servizi della *Scarlet* gli utenti scaricavano da Internet, senza autorizzazione e senza pagarne i diritti, opere contenute nel suo catalogo, utilizzando reti di condivisione *peer-to-peer*, la *Sabam* presentava relativa istanza al il presidente del Tribunal de première instance de Bruxelles ottenendo un'ingiunzione che, a pena di ammenda, imponeva alla Scarlet, di far cessare tali violazioni del diritto d'autore, rendendo impossibile ai suoi clienti qualsiasi forma di condivisione dei *file*. In sede d'appello il *provider* asseriva la non conformità di detta ingiunzione al diritto dell'Unione imponendole, *de facto*, un obbligo generale di sorveglianza sulle comunicazioni che transitano sulla sua rete. La *Cour d'appel* richiedeva pertanto intervento della Corte di giustizia. Per un commento in ottica comparatistica v. VIOLA DE AZEVEDO CUNHA M., MARIN L., SARTOR G., *Peer-to-Peer Privacy Violations and ISP Liability: Data protection in the user-generated web*, in *International Data Privacy Law*, vol. 2, n. 2, 2012, p. 50 ss.

[156] Per "filtraggio generalizzato" si intende una sorveglianza applicata indistintamente a tutti gli utenti, a titolo preventivo, a totale costo dell'ISP, senza limiti di tempo e che sia idonea ad identificare nella rete di tale fornitore la circolazione di *file* contenenti un'opera musicale, cinematografica o audiovisiva rispetto alla quale il richiedente affermi di vantare diritti di proprietà intellettuale, onde bloccare il trasferimento di file il cui scambio pregiudichi il diritto d'autore. Cfr. sent. in esame punti 29 e ss.

[157] Tale principio è stato confermato anche nella successiva sentenza della Corte di Giustizia dell'Unione europea, 16 febbraio 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM)/Netlog NV*, «Società dell'informazione – Diritti di proprietà

ingiunzione, infatti, implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'individuazione degli indirizzi IP degli utenti che effettuano l'invio dei contenuti illeciti sulla rete, i quali costituiscono sicuramente dati personali in quanto ne consentono la relativa identificazione[158].

Ancora una volta la Corte quindi pone in primo piano la necessità di una tutela rafforzata della *privacy*, che nelle sue diverse accezione sembra l'interesse privilegiato nella risoluzione del difficile giudizio di bilanciamento. D'altra parte tale soluzione si appalesa come l'unica pienamente rispettosa del principio di legalità il quale richiede che gli interventi di pubblici poteri nella sfera di attività

---

intellettuale – Direttiva 2004/48/CE – Diritto d'autore e diritti connessi – Direttiva 2001/29/CE – Scaricamento illecito di file su Internet – Scambio di file mediante software "*peer to peer*" – Sistema di filtraggio delle comunicazioni elettroniche – Meccanismo di blocco dei file scambiati in violazione di diritti di proprietà intellettuale – Diritto al rispetto della vita privata – Protezione dei dati personali – Artt. 7 e 8 della Carta – Art. 8 della CEDU – Direttiva 95/46/CE – Direttiva 2002/58/CE – Riservatezza delle comunicazioni – Diritto alla libertà di espressione – Art. 11 della Carta – Art. 10 della CEDU – Responsabilità dei prestatori intermediari di servizi – Obbligo generale di controllo delle informazioni – Direttiva 2000/31/CE – Stato di diritto – Limitazione dei diritti e delle libertà "prevista dalla legge" – Qualità della legge – Preminenza del diritto». Interessante notare come, soprattutto nelle conclusioni dell'avvocato generale Pedro Cruz Villalòn presentate il 14 aprile 2011, emerga la corrispondenza fra Carta europea e Convenzione EDU. Sulla base di tale corrispondenza l'avvocato generale propone la riformulazione della questione sostituendo il riferimento agli artt. 8 e 10 CEDU con quello agli artt. 7, 8,11 della Carta, in combinato disposto con l'art. 52, n. 1, della stessa, come interpretati, ove necessario, alla luce degli artt. 8 e 10 della CEDU. V. punti 29-34 delle conclusioni dell'avvocato generale Pedro Cruz Villalòn, Causa C-70/10.

[158] Circa l'equiparazione degli indirizzi IP ai dati personali dell'art. 2, lett. a) della direttiva 95/46 e l'interferenza nella sfera della vita privata e della corrispondenza nel caso di controllo del comportamento degli utenti di Internet sommato alla raccolta dei loro indirizzi IP v. *Parere del Garante Europeo della protezione dei dati*, 22 febbraio 2010, in merito ai negoziati ACTA, GU C 147, pag. 1, punto 24; *Parere del Garante Europeo della protezione dei dati*, 10 maggio 2010, sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pedopornografia, che abroga la decisione quadro 2004/68/GAI, GU C 323, pag. 6, punto 11; Article 29 Data Protection Working Party, Parere 4/2007 WP 136, in ec.europa.eu, 20 Giugno 2007.

privata di ogni persona, fisica o giuridica, siano fondati sulla legge in modo tassativo e determinato secondo i canoni di ragionevolezza e proporzionalità[159].

[159] Il principio in esame è stato oggetto anche di numerose sentenze della Corte Europea dei diritti dell'uomo, v. *ex multis* sent. *Klass e a./Germania*, 6 settembre 1978, *§* 55; sent. *Kopp/Svizzera,* 25 maggio 1998, *§* 55; sent. *Valenzuela Contreras/Spagna*, 30 luglio 1998, § 46. V. inoltre in tal senso anche Corte di Giustizia dell'Unione europea, 29 gennaio 2008, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*. Il rinvio pregiudiziale è scaturito dalla richiesta giudiziale dell'associazione di produttori ed editori di registrazioni musicali e audiovisive *Promusicae* di imporre alla *Telefónica* la rivelazione dell'identità e dell'indirizzo fisico di alcuni utenti che, attraverso connessioni *peer to peer* condividevano fonogrammi i cui diritti patrimoniali di utilizzo spettano ai soci della *Promusicae*. La Corte conclude affermando che la normativa europea in materia non impone agli Stati membri di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile, ma in sede di trasposizione delle direttive e di attuazione delle relative misure di recepimento le autorità e i giudici nazionali devono optare per interpretazioni conformi anche ai principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità. Molto più decise le conclusioni dell'Avvocato generale, che per chiarezza meritano di essere riportate per esteso: «La tutela dei dati ha per fondamento il diritto fondamentale al rispetto della vita privata e familiare, come discende segnatamente dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (in prosieguo: la «CEDU»), siglata a Roma il 4 novembre 1950 (23). La Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza il 7 dicembre 2000 (in prosieguo: la «Carta»), ha confermato tale diritto fondamentale all'art. 7 e ha sottolineato, in particolare, all'art. 8, il diritto fondamentale alla protezione dei dati di carattere personale, inclusi gli importanti principi fondamentali da applicarsi a tale protezione. La comunicazione di dati personali ad un terzo arreca quindi pregiudizio al diritto al rispetto della vita privata degli interessati, quale che sia l'ulteriore utilizzazione delle informazioni così comunicate, e presenta il carattere di un'ingerenza ai sensi dell'art. 8 della CEDU. Una siffatta ingerenza viola l'art. 8 della CEDU, salvo quando è «prevista dalla legge». L'articolo che la prevede deve essere pertanto redatto in modo sufficientemente preciso, conformemente al requisito di prevedibilità, in modo da consentire ai destinatari della legge di regolare la loro condotta . Il requisito della prevedibilità ha trovato particolare espressione nel diritto della tutela dei dati personali grazie al vincolo di finalità, espressamente menzionato all'art. 8, n. 2, della Carta. Il vincolo di finalità viene concretizzato dall'art. 6, n. 1, della direttiva 95/46/CE, ai sensi del quale i dati personali possono essere rilevati esclusivamente per determinate finalità univoche e legittime e non possono essere successivamente trattati in modo incompatibile con tali finalità. Inoltre, l'ingerenza nella sfera privata, ossia il trattamento di dati personali, deve rispondere al requisito di proporzionalità rispetto agli obiettivi perseguiti. Deve pertanto sussistere un'esigenza sociale imperativa e i provvedimenti devono essere proporzionati alla finalità

E' questa la linea seguita anche in materia di *data retention*[160]. La Corte infatti con sentenza dell'8 aprile 2014 ha dichiarato non valida la direttiva europea

---

legittima perseguita. Nella fattispecie, nell'ambito delle finalità lecite occorre tener conto dei diritti fondamentali coinvolti dei titolari dei diritti d'autore, nello specifico la tutela della proprietà e il diritto ad un'effettiva tutela giurisdizionale. Anche questi due diritti fondamentali, per giurisprudenza costante, fanno parte dei principi generali del diritto comunitario. Ciò è stato confermato dagli artt. 17 e 47 della Carta. L'art. 17, n. 2, della Carta sottolinea che anche la proprietà intellettuale rientra nella sfera di tutela del diritto fondamentale di proprietà […] Un'interpretazione dell'art. 6, n. 6, della direttiva 2002/58/CE che consenta la comunicazione dei dati sul traffico alla potenziale controparte semplicemente in forza di un loro uso in un procedimento contenzioso sarebbe, per insufficienza di elementi a sostegno nel testo, incompatibile con il principio di prevedibilità che deve essere osservato quando si giustificano per legge ingerenze nella sfera della vita privata e nella tutela dei dati. Oltre alle eccezioni di cui all'art. 6, nn. 2, 3 e 5, chiaramente indicate e circoscritte all'art. 6, n. 1, nonché ai sensi dell'art. 15, n. 1, si introdurrebbe una deroga quasi illimitata. Considerato il tenore dell'art. 6, non è tuttavia concepibile che l'utente di servizi di comunicazione elettronica si debba confrontare con una siffatta deroga. Tale deroga avrebbe allo stesso tempo una portata assai estesa, fatto per cui non potrebbe essere ritenuta proporzionale alla luce delle finalità perseguite. In linea di principio, l'utente dovrebbe sempre aspettarsi, e non solamente in seguito ad una violazione dei diritti d'autore, che i suoi dati sul traffico siano trasmessi a terzi che, per un qualsivoglia motivo, vogliono intentargli causa. È da escludere che siffatte controversie si fondino in tutti i casi su un'esigenza sociale imperativa ai sensi della giurisprudenza concernente l'art. 8 CEDU». Conclusioni dell'avvocato generale Juliane Kokott presentate il 18 luglio 2007, Causa C‑275/06, punti 51 e ss.

In una più recente pronuncia la Corte di Giustizia ha dichiarato la legittimità di un'ingiunzione del giudice ad un *provider* che, senza specificare le precise misure da adottare, vieti allo stesso di concedere ai suoi abbonati l'accesso ad un sito Internet che metta a disposizione materiali in violazione del diritto d'autore e al contempo permetta al fornitore d'accesso di evitare sanzioni per la violazione di tale ingiunzione dimostrando di avere adottato tutte le misure ragionevoli. Sarà poi il giudice nazionale a valutare la sussistenza della "ragionevolezza" delle misure adottate nel caso specifico (Corte di giustizia dell'Unione europea, 27 marzo 2014, C-314/12, *UPC Telekabel Wien GmbH / Constantin Film Verleih GmbH e Wega Filmsproduktionsgesellschaft mbH*).

[160] Per *data retention* si intende la conservazione dei dati di traffico telefonico e telematico per finalità che possono essere imposte dalla legge, da esigenze tecniche, o imprenditoriali. Cfr. VACIAGO G., *La disciplina normativa sulla data ritention e il ruolo degli internet service provider*, in LUPARIA L. (a cura di), *Internet Provider e Giustizia Penale*, cit., p. 141 ss.

2006/24/CE[161] che impone agli operatori di telefonia di memorizzare i dati di traffico per un periodo che va dai 6 mesi ai 2 anni e consente alle competenti autorità di potervi accedere, proprio per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza[162]. Anche il settore del contrasto al crimine quindi, pur

[161] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE. Essa ha per obiettivo principale l'armonizzazione delle disposizioni degli Stati membri sulla conservazione di determinati dati generati o trattati dai fornitori di servizino nonchè la disponibilità di tali dati a fini di indagine, accertamento e perseguimento di reati gravi, come in particolare i reati legati alla criminalità organizzata e al terrorismo. In tal senso, la direttiva dispone che i suddetti fornitori debbano conservare i dati relativi al traffico, i dati relativi all'ubicazione ed i dati connessi necessari per identificare l'abbonato o l'utente. La direttiva non autorizza, invece, la conservazione del contenuto della comunicazione e delle informazioni consultate. In relazione alla direttiva v. IP/11/484, Bruxelles, 18 aprile 2011, *La Commissione valuta la direttiva sulla conservazione dei dati relativi alle telecomunicazioni*, in europa.eu. Prima della pronuncia della Corte di Giustizia in esame, già alcune Corti costituzionali europee si erano espresse circa l'incostituzionalità delle leggi attuative della direttiva in questione. Per approfondito commento alle stesse v. FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Rivista trimestrale di diritto penale dell'economia*, n. 3/2009, p. 695 ss., Id., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention*, in *Ciberspazio e diritto*, 2010, p. 359 ss.; Id., *Le recenti sentenze del Bundesverfassungsgericht e della Curtea Constituţională sul data retention*, in unicam.it, *Atti del Convegno- Ascoli Piceno*, 5-7 Marzo 2010.

[162] Corte di Giustizia dell'Unione europea, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e altri; Kärntner Landesregierung e altri*, «Comunicazioni elettroniche – Direttiva 2006/24/CE – Servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione – Conservazione di dati generati o trattati nell'ambito della fornitura di tali servizi – Validità – Articoli 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione europea». La violazione del principio di proporzionalità deriverebbe, secondo la Corte, dall'avere la direttiva: 1) previsto le misure di conservazione dei dati come applicabili in via indifferenziata e generalizzata all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che

ammettendo in astratto per esigenze di interesse generale connesse alla pubblica sicurezza maggiori limitazioni alle libertà individuali, non sfugge al controllo di proporzionalità: le restrizioni dei diritti fondamentali non possono essere previste in maniera indifferenziata rispetto a qualsiasi reato ma richiedono l'autorizzazione dell'autorità giudiziaria sulla base di una previsione legislativa che le disciplini in modo differenziato in base al tipo di delitto, alle esigenze investigative, al tipo di dato e di mezzo di comunicazione utilizzato.

Gli obblighi di archiviazione e di controllo dei dati di traffico telematico e telefonico, pur non permettendo l'accesso al contenuto delle conversazioni, forniscono comunque indicazioni importanti sulle comunicazioni intrattenute che comportano una forte ingerenza nella vita privata dei cittadini e, avvenendo la conservazione e il successivo utilizzo dei dati a loro saputa, «ingenerano la sensazione che la loro vita privata sia oggetto di costante sorveglianza»[163].

La Corte di giustizia dell'Unione europea quindi sottolinea la non neutralità dei dati di traffico e la pericolosità cui è esposta la vita privata nel caso di una

---

venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi; 2) omesso di prevedere alcun criterio oggettivo che limiti l'accesso a tali dati per sole esigenze di accertamento di reati sufficientemente gravi da giustificare una simile ingerenza, ben oltre - dunque - il generico rinvio ai reati gravi definiti da ciascuno Stato membro; 3) omesso di sancire i presupposti sostanziali e procedurali ai quali subordinare l'accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell'autorità giudiziaria o di un'autorità amministrativa indipendente; 4) omesso di prevedere criteri necessari a differenziare la durata della conservazione dei dati, limitandosi a stabilirne i soli termini minimi e massimi; 5) omesso di imporre che i dati così acquisiti siano conservati nel solo territorio della Ue.

In commento v. FLOR R., *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in penalecontemporaneo.it, 28 Aprile 2015; ID., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, cit.; v. inoltre SENOR M., *Un altro "tango down" in tema di data retention*, in medialaws.eu, 22 Luglio 2015.

[163] CGUE 8.04.14, C-293/12 e C-594/12, punto 37.

indifferenziata conservazione di questi dati per periodi molto lunghi, rafforzando la tutela della riservatezza[164].

Alla luce dei casi esaminati è palese come le decisioni della Corte di Lussemburgo e della Corte di Strasburgo si inseriscano nel vivace dibattito in tema di responsabilità del *provider*, cristallizzando *standard* di comportamento in riferimento ai quali possono o meno operare i *safe harbours* previsti nella direttiva europea, nonché adeguando il dato normativo vigente al nuovo scenario tecnologico[165].

In modo particolare il divieto per gli Stati membri di introdurre sistemi di filtraggio, conservazione e sorveglianza generalizzati, fissato nella direttiva *e-Commerce* e più volte specificato nelle pronunce della Corte di Lussemburgo, rappresenta sostanziale contropartita della tutela di valori fondamentali della CEDU, la cui portata è stata illustrata anche dalla Corte di Strasburgo. Tale divieto ha come diretta conseguenza l'inconfigurabilità di una generale

[164] Certo, come evidenziato dal dott. Flor, le decisioni nel caso *Google /Spain* e nel caso cd. *data retention* «se, da un lato, forzano la tutela della riservatezza, dall'altro segnano uno strappo epocale nell'odierna società di Internet, ponendo dei limiti decisi all'uso delle tecnologie della rete, che non sempre possono produrre effetti positivi rispetto alla tutela di rilevanti contro interessi di natura generale e collettiva […] Le sfide lanciate da nuovi fini fenomeni illeciti o di natura criminosa, nonchè l'esigenza di prevenzione di accertamento dei reati, richiedono un percorso di scelte che non è paragonabile al viaggio di Raffaele Itlodeo nell'isola di *Utopia*, una *societas perfecta*. Sarebbe utopistico, infatti, credere che l'utente medio del nuovo millennio non utilizzi le opportunità offerte dall'evoluzione-rivoluzione informatica. Sarebbe altrettanto utopistico credere di contrastare con finalità anche grave senza ricorrere alle stesse opportunità offerte dalla evoluzione-rivoluzione informatica». V. FLOR R., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, cit.

[165] Le pronunce europee, come visto, rappresentano in realtà solamente un "traguardo intermedio" e non "destinazione raggiunta", rimettendo poi al giudice nazionale il contemperamento degli interessi in gioco nel caso specifico. Sul complesso dialogo tra giudici nazionali e europei in materia penale cfr. MANES V., *Metodo e limiti dell'interpretazione conforme alle fonti sovranazionali in materia penale*, in penalecontemporaneo.it, 9 Luglio 2012; VIGANÒ F., *L'adeguamento del sistema penale italiano al "diritto europeo" tra giurisdizione ordinaria e costituzionale*, in penalecontemporaneo.it, 14 Febbraio 2014.

responsabilità penale omissiva dei *providers* per mancato impedimento degli illeciti commessi dai propri utenti. Ma, il fatto che non gravi sul fornitore un obbligo generico di attivarsi per sorvegliare la rete e proteggere i diritti degli internauti, non esclude la sussistenza di specifiche posizioni di garanzia, individuate caso per caso secondo le disposizioni specifiche del settore di riferimento, sulle quali poter fondare anche una responsabilità ex art 40 cpv. c.p.

Le sentenze della Corte Superiori non possono che essere lette come dimostrazione e al contempo linee guida di tale orientamento. Certo pure la tutela penale dovrà adeguarsi al richiamato giudizio di proporzionalità utilizzando quali parametri nel bilanciamento le scelte di protezione di beni giuridici operate dalle istituzioni europee[166].

In modo particolare, proprio per garantire il rispetto del principio di proporzionalità la valutazione circa l'effettiva conoscenza dell'illeceità dell'attività realizzata dall'utente richiamata in sede civile dalla Corte di Giustizia in riferimento all'applicabilità dell'esenzione di responsabilità *ex* art. 14 della direttiva *e-Commerce*, dovrebbe, in ambito penale, escludere dall'alveo dell'elemento soggettivo il dolo eventuale.

Al termine di questa breve analisi appare opportuno rilevare che il dialogo tra le Corti sovranazionali e nazionali, pur svolgendo il compito essenziale di sagomare l'ottimale bilanciamento dei diritti fondamentali coinvolti in funzione della particolarità del caso concreto, non può sostituirsi all'intervento legislativo che risulta ancor più di vitale importanza ove si considerino le sfumature che gli stessi acquisiscono grazie all'utilizzo delle nuove tecnologie: solo una normativa *ad hoc* può infatti offrire «indicazioni essenziali, idonee a tracciare il solco entro il quale può impiantarsi e svolgersi il "diritto vivente", per quindi rimettersi a soluzioni non meramente applicative bensì attuative e, se del caso, integrative dei

[166] Basti a tal riguardo richiamare, ad esempio, la direttiva 2011/93/CE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, attuata in Italia con d.lgs. 38/2014, dalla quale emerge chiaramente che l'interesse superiore del minore deve essere considerato preminente. In modo particolare nella direttiva si prevedono quali strumenti di contrasto il blocco dell'accesso a siti e la rimozione delle pagine contenenti immagini pedopornografiche.

giudici, che dalle leggi stesse ricevano perciò la "delega" per quelle operazioni di bilanciamento in concreto degli interessi meritevoli di tutela che solo nelle sedi giudiziali e in ragione dei casi possono essere a modo fatte»[167].

[167] Così si esprime il prof. Ruggeri in un interessantissimo saggio avente ad oggetto il ruolo dei giudici nazionali ed internazionali nella tutela dei diritti fondamentali: RUGGERI A., *"Dialogo" tra le Corti e tecniche decisorie, a tutela dei diritti fondamentali*, in diritticomparati.it, 19 Novembre 2013.

CONSIDERAZIONI CONCLUSIVE

Nel confronto tra una domanda di tutela sempre più accentuata e avvertita come urgente dalla società digitale, ed un dato normativo europeo e nazionale obsolescente e per molteplici versi carente, la risposta giurisprudenziale non può che risultare come poco soddisfacente, correndo il pericolo di risolversi, per certi versi, in un arbitrio.

I rischi connessi alle innovazioni tecnologiche non possono più godere di una sorta di franchigia sociale, connessa ad esimenti ideologiche[1]. Il richiamo, ad esempio, alla *freedom of speech*, non può trasformarsi in uno scudo protettivo dell'irresponsabilità dei *providers*.

Vi è chi, aderendo alla concezione del *web* come luogo di massima espressione di libertà del singolo, onde evitarne la compressione o negazione, avversa ogni intervento legislativo che propenda per qualche controllo.

I *digital libertarians* dovrebbero forse rammentare però che, come precisato dal prof. Rodotà quasi un ventennio orsono, «la libertà ha sempre bisogno di un quadro istituzionale non che la protegga, ma che consenta ad essa di rimanere al riparo dai molti attacchi che alla libertà possono essere portati anche senza una volontà censoria. E nel momento in cui Internet evolve come grande luogo di interessi economici, tendenza che non può e sarebbe sbagliato contrastare, dobbiamo però tenere conto della necessità di salvaguardare in rete i diritti e le dinamiche della libertà»[2].

Internet è uno spazio sociale, politico, economico ed i fornitori di servizi ne sono i protagonisti, non solo in quanto potrebbero essere coinvolti nella

---

[1] Cfr. SORO A., *Persona vulnerabile. La protezione dei dati nella società digitale. Discorso del Presidente. Relazione 2014*, Roma, 23 Giugno 2015: «Gli scenari della società digitale disegnano un quadro di grandi sfide che abbiamo il dovere di affrontare senza rassegnata subalternità e senza inutile ostilità. Dobbiamo rimuovere la tentazione tecnofobica, il timore dell'innovazione, senza rinunciare a contrastarne le distorsioni, a ricercare una qualche regolazione dei processi e, più in generale, a vivere responsabilmente il nostro tempo».

[2] Cfr. RODOTÀ S., *Relazione introduttiva: Libertà, opportunità, democrazia, informazione*, Convegno *Internet e privacy – Quali regole?*, cit.

realizzazione di reati (a titolo di autoria, concorso commissivo od omissivo), ma anche perché svolgono un ruolo di natura pubblica ed indispensabile nell'ambito delle attività investigative.

Penso che prevedere precipui obblighi di attivazione per gli ISPs, distinguendo tra le diverse fasi ed attività, e fondare su di essi anche eventuali responsabilità penali, sia la scelta migliore in vista della ricerca di un equilibrio in rete tra libertà, sicurezza e tutela dei diritti coinvolti. Ovviamente ciò richiede anche la fissazione di una specifica procedura di *notice and take down*, d'ispirazione americana, che permetta il contraddittorio tra le parti ed il coinvolgimento delle autorità specifiche del settore (ad es. AGCOM, CISR, DIS, Centro nazionale per il contrasto della pedo-pornografia sulla rete Internet, etc.). In tal modo si eviterebbe il rischio di trasformazione degli ISPs in incontrollati censori della rete, e si conformerebbe l'ordinamento all'indicazione della Corte di Giustizia, secondo cui l'intermediario non può che essere considerato responsabile degli illeciti commessi in rete qualora sussista la *knowledge*[3].

E' nel quadro forte dei principi cardine del nostro sistema, quali il principio di personalità, colpevolezza e «del potere agire diversamente»[4], che troverà posto il corretto bilanciamento degli interessi valorizzando le specificità del caso concreto, e si eviterà il pericolo che Internet si trasformi in una «sconfinata prateria dove tutto è permesso e niente può essere vietato»[5].

Nonostante, come illustrato, esistano già norme penali suscettibili di applicazione per contrastare la criminalità in Internet, senza una tipizzazione chiara e un intervento legislativo che delimiti con precisione i diritti ed i confini

---

[3] Cfr. RESTA F., *Libertà della rete e protezione dei dati personali*, cit., p. 502 ss.: « […] È necessario prevedere - adeguatamente bilanciando i vari interessi in gioco - specifici obblighi di attivazione del *provider*. Il quale, informato dell'illiceità dei contenuti trasmessi e su richiesta dell'interessato o dell'autorità giudiziaria, sia tenuto a rimuovere le informazioni contestate, pena un suo concorso nel reato sottostante, indubbi essendo, a questo punto, non solo il contributo agevolativo fornito sul piano soggettivo, ma anche la consapevolezza del carattere illecito dell'altrui condotta favorita».

[4] Cfr. PULITANÒ D., *L'errore di diritto nella teoria del reato*, cit., p. 563 ss.

[5] L'espressione è stata utilizzata dal giudice Oscar Magi nella sentenza Tribunale di Milano, sent. 12 aprile 2010, n. 1972.

della responsabilità dell'ISP, il "caso" assurge a vero ed unico soggetto della decisione[6] ponendosi, evidentemente, come regola e segno stesso di impossibilità di una regola *in action*, e aumentando il senso di incertezza e vertigine che già di per sé la rete delle reti, per la sua intrinseca a-materialità e la caratteristica specifica di non luogo privo di confini e distanza, trasmette.

Un coinvolgimento del *provider* che lo renda, seppur in modo limitato e condizionato, garante della sorveglianza e sicurezza della rete, sembra non solo inverare la previsione di cui all'art. 41 Cost., secondo la quale la libertà d'iniziativa economica può subire limitazioni per ragioni determinate dall'interesse pubblico od in vista di un'utilità sociale, ma anche risposta necessitata dinnanzi ad un sistema costituzionale che ha posto la persona umana al vertice della scala dei valori[7]. Quanto mai attuali risuonano allora le parole del prof. Vassalli che, già agli inizi degli anni sessanta, riflettendo sulla protezione della personalità o della sfera individuale di fronte ai problemi posti dal progresso tecnico, affermava: «lo sviluppo della tecnica, che pur porta per sua tendenza, come ogni progresso, ad un potenziamento della personalità individuale, deve trovare un argine in nome della stessa personalità umana, destinata a restare nelle sue manifestazioni più alte e più sacre, il metro di tutte le cose; senza di che rischieremo un giorno di perire tutti per opera nostra […] Tutti gli aspetti della personalità, dalla vita alla salute, dal lavoro alla dignità e alla riservatezza, dalla libertà morale all'onore, meritano oggi una tutela più attenta ed efficace che per il passato di fronte ai pericolo connessi con il progresso tecnologico: al quale tuttavia la personalità individuale è debitrice dei suoi maggiori arricchimenti e delle sue maggiori garanzie»[8].

---

[6] Cfr. RODOTÀ S., *La vita e le regole. Tra diritti e non diritto*, Milano, 2006, p. 159.

[7] Cfr. per tutti PALAZZO F. C., *Il problema dell'ignoranza della legge penale nelle prospettive di riforma*, cit., p. 777 ss. e Corte Costituzionale, sent. n. 364 del 1988.

[8] VASSALLI G., *La protezione della sfera della personalità nell'era della tecnica*, in *Studi in onore di Emilio Betti*, vol. V, Milano, 1962, p. 675.

I fenomeni illeciti, nel *cyberspace*, presentano una dimensione sovranazionale, pertanto richiedono di essere contrastati su basi comuni nei diversi ordinamenti. E' auspicabile, quindi, una presa di posizione del legislatore europeo che, in virtù della nuova competenza in materia penale di cui all'art. 83 TFUE e procedura penale ex art. 82 TUFE, chiarisca le responsabilità dell'operatore del sistema, introducendo obblighi d'incriminazione penale per contrastare reati di violazione del "*cyberspace* sano" e risolvere anche potenziali conflitti di giurisdizione.

L'economia digitale ha favorito la creazione di piattaforme tecnologiche, con poteri sempre più influenti a livello internazionale. Per la struttura organizzata delle imprese che esercitano l'attività di *Intenet service provision*, a fronte dell'insufficienza dei tradizionali strumenti di prevenzione e contrasto ancorati al paradigma tradizionale della responsabilità penale delle singole persone fisiche e ad un sistema di prevenzione sostanzialmente interno o settoriale, sarebbe quanto mai opportuna la previsione di una responsabilità da reato degli enti[9], che superi il modello italiano disciplinato dal D.Lgs. 231/2001[10] e che tenga conto delle attività concretamente svolte dagli intermediari, del ruolo che essi rivestono nei processi di circolazione delle informazioni, dell'esigibilità del loro intervento e della proporzione tra gravità oggettiva dell'illecito ed entità della sanzione, secondo le indicazioni delle Corti Superiori europee.

La sfida del ripensamento delle categorie penalistiche esige una risposta globale e, propendere per una maggiore responsabilizzazione dei *providers*, è

[9] E per far ciò ancora essenziali risultano le riflessioni di Bricola e Marinucci che, sebbene attenti al volto costituzionale dell'illecito penale, già negli anni '70, si preoccuparono degli effetti negativi del mantenimento del dogma *societas delinquere non potest*, evidenziandone l'inconsistenza (cfr. MARINUCCI G., *Il reato come "azione". Critica di un dogma*, cit.), nonché il costo in termini di efficienza punitiva e di tutela effettiva dei beni giuridici di fronte alle nuove forme di aggressione nel settore dell'attività d'impresa (cfr. BRICOLA F., *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, cit., p. 951 ss.).

[10] Cfr. pag. 30 e ss.

forse scelta indispensabile per migliorare la qualità della cd. *Infosfera*[11], entro cui si svolge la personalità di ciascuno.

Se, oltre a determinati beni personali (quali l'intangibilità della sfera sessuale del minore, la *privacy*, il diritto d'autore, ecc.), consideriamo il "*cyberspace* sano", inteso come nuovo ambiente in cui si sviluppa la nostre esistenza, quale un interesse meritevole di protezione, ed il diritto penale come strumento di giusta tutela, così come è stato in materia ambientale[12], la necessità del punire non può costituire solo un limite all'intervento del legislatore, ma anche legittimazione positiva di risposte che, nel rispetto del principio di proporzionalità, evitino comunque l'eccesso e l'iperpenalizzazione[13].

Il contemperamento tra esigenza che i fenomeni criminosi commessi nella rete e attraverso la rete non restino impuniti, anche solo per la mancata conoscenza dell'autore materiale, e necessità del rispetto del principio di personalità della responsabilità penale, nonché tra libertà di espressione e tutela degli interessi che possono essere offesi, dovrebbe comportare la previsione di reati omissivi propri, contraddistinti da cornici edittali abbastanza ampie per poter parametrare le risposte sanzionatorie alla gravità del fatto ed alle sue conseguenze, eliminando in tal modo anche il rischio di introdurre ipotesi di responsabilità oggettiva lesive del principio *ad impossibilia nemo tenetur*, e di riproporre una fattispecie critica e criticabile come quella di cui all'art. 57 c.p.[14].

---

[11] Così il presidente dell'Autorità garante per la protezione dei dati personali definisce il "pianeta connesso" in cui tutti siamo immersi. V. SORO A., *Persona vulnerabile*, cit.

[12] Per la definizione dei beni giuridici "ambiente" ed "ecosistema", tutelati grazie all'introduzione nel c.p. dei nuovi delitti contro l'ambiente, v. MASERA L., *I nuovi delitti contro l'ambiente - voce per il "libro dell'anno del diritto Treccani 2016*, in penalecontemporaneo.it, 17 Dicembre 2015. Per una riflessione approfondita sulle novità introdotte dalla legge n. 68/2015, v., inoltre, RUGA RIVA C., *I nuovi ecoreati, Commento alla legge 22 maggio 2015, n. 68*, Torino, 2015.

[13] Cfr. in tal senso le riflessioni del prof. Pulitanò sul tema del possibile dialogo fra scienza e legislazione penale: PULITANÒ D., *La cultura giuridica e la fabbrica delle leggi*, in penalecontemporaneo.it, 28 Ottobre 2015.

[14] Già Pisapia nel 1958, suggeriva ciò con riguardo ai reati commessi a mezzo stampa. Cfr. PISAPIA G. D., *La nuova disciplina della responsabilità per i reati commessi a mezzo stampa*, cit., p. 322 ss. L'esigenza di un trattamento differenziato della stampa rispetto ad Intenet, sostenuta nei

Pur non disconoscendo la centralità della risposta civile quale via naturale per ottenere il risarcimento del danno da fatti illeciti, e dell'adozione di codici di autodisciplina essenziali anche per un ripensamento dell'elemento soggettivo della colpa, il diritto penale non sembra, quindi, poter svolgere una funzione secondaria ma appare come pietra d'angolo per un'efficace disciplina che regoli l'inarrestabile sviluppo della rete.

---

precedenti capitoli, non elimina le analogie ed i parallelismi che caratterizzano questi due mezzi di comunicazione, i quali rendono coerenti, quindi, anche riflessioni comuni per la fissazione delle discipline di ciascun settore. In modo particolare ritroviamo spunti essenziali anche nella proposta di creazione di un "testo unico della stampa" di Nuvolone (NUVOLONE P., *I reati di stampa*, cit., p. 199 ss.).

BIBLIOGRAFIA

ABDEL-KHALIK J., *Is eBay counterfeiting?*, in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, London, 2013.

ADORNATO C., *Il momento consumativo del reato*, Milano, 1966.

AHLERT C., MARSDEN C., YUNG C., *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation*, in ox.ac.uk, 1 Maggio 2004.

ALESSANDRI A. (a cura di), *Il nuovo diritto penale delle società*, Milano, 2002.

ALESSANDRI A., *Art. 27*, in BRANCA G., PIZZORUSSO A., *Commentario della Costituzione*, Bologna-Roma, 1991.

ALESSANDRI A., *Note penalistiche sulla nuova responsabilità delle persone giuridiche*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 33 ss.

AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Matelica, 2006.

ANTOLISEI F., *Manuale di diritto penale. Parte generale*, Quindicesima Edizione integrata e aggiornata da L. Conti, Milano, 2000.

ANTOLISEI F., *Manuale di diritto penale. Parte speciale, II*, Quindicesima Edizione integrata e aggiornata a cura di C. F. Grosso, Milano, 2008.

ANTONINI A., *La tutela giuridica del nome di dominio*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2001, p. 813 ss.

AZZALI G., *Concorso di persone nel reato. La prospettiva causale*, in DOLCINI E., PALIERO C. E. (a cura di), *Studi in onore di Giorgio Marinucci*, Tomo II, Milano, 2006.

BAISTROCCHI P., *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in *Santa Clara High Techology Law Journal*, Volume 19, Issue 1, Article 3, 2002, p. 111 ss.

BALLON I. C., *Secondary trademark liability for internet and mobile sites and services and other intermediaries*, LAIPLA (Los Angeles Intellectual Property Law Association) spring seminar, Ojai, California, 6-8 Giugno 2014.

BALSAMO A., *Decreto antiterrorismo e riforma del sistema delle misure di prevenzione*, in penalecontemporaneo.it, 2 Marzo 2015.

BARFIELD C. E., HEIDUK G., WELFENS P.J.J. (eds.), *Internet, Economic Growth and Globalization – Perspectives on the New Economy in Europe, Japan and the US*, Berlin et al., 2003.

BARTOLE S. CONFORTI B., RAIMONDI G., (a cura di), *Commentario della Convenzione europea dei diritti dell'uomo*, Padova, 2001.

BARTOLE S., DE SENA P., ZAGREBELSKY V., *Commentario breve alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012.

BARTOW A., *Barnes v. Yahoo! And Section 230 ISP immunity*, in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, London, 2013.

BASILICO A. E., *Tra giurisprudenza inglese e diritti europei: quattro sentenze della nuova Supreme Court*, in rivistaaic.it, 2 Luglio 2010.

BASSINI M., POLLICINO O., *Evoluto, ma non attivo. La Corte d'appello di Milano travolge la più recente giurisprudenza sull'hosting*, in diritto24.ilsole24ore.com, 27 Gennaio 2015.

BASSOLI E., *Esclusa la responsabilità penale di Google per violazione di dati personali da parte di materiale multimediale immesso da terzi*, in *Rivista penale*, n. 5/2013, p. 558 ss.

BELLEZZA M., *Yahoo! Vs RTI: a new era for ISP's liability in Italy?*, in medialaws.eu, 26 Gennaio 2015.

BELLUTA H., *Cybercrime e responsabilità degli enti*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l.18 marzo 2008, n.48)*, Milano, 2009.

BERNARDI A., *All'indomani di Lisbona: note sul principio europeo di legalità penale*, in *Quaderni Costituzionali*, n. 1/2009, p. 37 ss.

BERNARDI A., *Art. 7. "Nessuna pena senza legge"*, in BARTOLE S. CONFORTI B., RAIMONDI G., (a cura di), *Commentario della Convenzione europea dei diritti dell'uomo*, Padova, 2001.

BERNARDI A., *L'armonizzazione delle sanzioni in Europa: linee ricostruttive*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008.

BETTIOL G., *Diritto penale*, Padova, 1969.

BETZU M., *Anonimato e responsabilità in internet*, in costituzionalismo.it, n. 2/2011, 6 Ottobre 2011.

BEVERE A., ZENO-ZENCOVICH V., *La rete e il diritto sanzionatorio: una visione d'insieme*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 3/2011, p. 375 ss.

BIANCHI M., *Concorso di persone e reati accessori*, Torino, 2013.

BRIAT M., SIEBER U., (eds.) *Computer Related Criminality: Analysis of Legal Policy in the OECD- Area*, Parigi, 1986.

BRICOLA F., *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Rivista italiana di diritto e procedura penale*, 1983, p. 951 ss.

BRICOLA F., *La discrezionalità nel diritto penale*, Milano, 1965.

BRICOLA F., voce *Teoria generale del reato,* in *Novissimo Digesto Italiano*, 1973, p. 7 ss.

BRUNST P., SIEBER U., *Cybercrime Legislation in Germany* in BASEDOW J., KISCHEL U., SIEBER U., (eds.), *German National Reports to the XVIII International Congress of Comparative Law*, 2010.

BUGIOLACCHI L., *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet Provider. Una sintesi di diritto comparato*, in *Il Diritto dell'Informazione e dell'Informatica*, 2000, p. 836 ss.

CADOPPI A. (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006.

CAJANI F., *Quella Casa nella Prateria: gli Internet Service Providers americani alla prova del caso Google Video*, in PICOTTI L., RUGGIERI F. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Milano, 2012.

CAMALDO L. (a cura di), *La circolazione e il contrabbando di prodotti contraffatti o pericolosi. La tutela degli interessi finanziari dell'Unione Europea e la protezione dei consumatori*. *Atti del Convegno europeo svoltosi a Milano il 31 maggio 2012, organizzato dal Centro Studi di diritto penale europeo, in stretta collaborazione con OLAF (Ufficio europeo per la lotta antifrode) e con UAE (Unione degli Avvocati Europei)*, Torino, 2013.

CAMMARATA M., *Finalmente una decisione sulla responsabilità del provider*, in interlex.it, 20 Luglio 1998.

CAMMARATA M., *Il diavolo nel sito e il provider diventa esorcista*, in interlex.it, 16 Luglio 1998.

CAMMARATA M., *Internet, diritto e politica, non c'è da stare allegri*, in interlex.it, 2 Luglio 1998.

CANESTRARI S., voce *Responsabilità oggettiva*, in *Digesto delle discipline penalistiche*, 1997, p. 107 ss.

CANNON R., *The Legacy of the Federal Communications Commission's Computer Inquiries*, in *Federal Communication Law Journal*, n. 55/2003, p. 167 ss.

CANNON R., *The Legislative History of Senator Exon's Communications Decency Act:*

Regulating Barbarians on the Information Superhighway, in *Federal Communications Law Journal*, Volume 49-Issue 1, Article 3, 1996.

CASETTA E., *Manuale di diritto amministrativo*, Milano, 2012.

CASSANO G. - BUFFA F., *Responsabilità del content provider e dell'host provider*, in altalex.com, 14 Febbraio 2003.

CASSANO G., *Cybersquatting*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2001, p. 83 ss.

CASSANO G., *Una «giurisprudenza toscana» sui nomi a dominio?*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 3/2001, p. 511 ss.

CASTELLANA A. M., *Diritto penale dell'Unione europea e principio «societas delinquere non potest»*, in *Rivista trimestrale di diritto penale dell'economia*, 1996, p. 747 ss.

CAVANNA E., *Le responsabilità dei providers alla luce della sentenza del Tribunale di Milano - Sezione V Penale in composizione collegiale - n. 1993 del 25 febbraio 2004*, in penale.it, 25 Febbraio 2004.

CIPOLLA P., *Social network, furto di identità e reati contro il patrimonio*, in *Giurisprudenza di merito*, n. 12/2012, p. 2672 ss.

CODIGLIONE G. G., *Indirizzo IP, reti Wi-Fi e responsabilità per illeciti commessi da terzi*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2013, p. 107 ss.

COMANDE' G., *Al via l'attuazione della direttiva sul commercio elettronico, ma… serve maggiore coordinamento*, in *Danno e Responsabilità*, n. 8-9/2003, p. 809 ss.

COMER D. E., *Internetworking con TCP/IP. Principles, Protocols and Architecture*, New York, 2006.

CONIGLIARO S. C., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della nuova direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in penalecontemporaneo.it, 30 Ottobre 2013.

CORRIAS LUCENTE G., *In tema di competenza territoriale per la pubblicazione su Facebook, in violazione del diritto alla privacy*, in medialaws.eu, 4 Maggio 2015.

CORRIAS LUCENTE. G., *Al direttore responsabile di un periodico on line non si applica il reato previsto dall'art. 57 del codice*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2012, p. 82 ss.

CORRIAS LUCENTE. G., *La Cassazione interviene ancora sull'equiparazione fra stampa e giornali telematici*, in medialaws.eu, 20 Marzo 2014.

CORRIAS LUCENTE. G., *Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che loro gestiscono?*, in *Giurisprudenza di merito*, 2004, p. 2523 ss.

COSTANZO P., *Aspetti evolutivi del regime giuridico di Intenet*, in *Il Diritto dell'Informazione e dell'Informatica*, 1996, p. 831 ss.

COTTU E., *Il Consiglio europeo adotta i nuovi orientamenti strategici per lo spazio di libertà, sicurezza e giustizia per il quinquennio 2015-2020*, in penalecontemporaneo.it, 22 Luglio 2014.

D'ALESSANDRO F., *art. 40 c.p.: B) L'equivalenza tra azione ed omissione*, in DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato*, Terza Edizione, Milano, 2011.

D'AMBROSIO L., *Responsabilità degli Internet provider e Corte di Giustizia dell'Unione Europea: quali spunti per il sistema penale italiano?*, in LUPARIA L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012.

DE CATA M., *La responsabilità civile dell'Internet service provider*. *Collana Università degli studi di Milano - Bicocca dip. dir. Economia*, 2010.

DE GRAZIA L., *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso internet: argomenti comparativi*, in rivistaaic.it, 29 Ottobre 2013.

DE MAGLIE C., *Principi generali e criteri di attribuzione della responsabilità*, in *Diritto Penale e Processo*, n. 11/2001, p. 1348 ss.

DE MARTINO P., *Le innovazioni introdotte nel codice di rito dal decreto legge sulla violenza di genere, alla luce della Direttiva 2012/29/UE*, , in penalecontemporaneo.it, 8 Ottobre 2013.

DE NATALE D., *Attività di contrasto alla pedopornografia on line: aspetti problematici della responsabilità delle persone fisiche e degli enti (parte seconda)*, in *Rivista trimestrale di diritto penale dell'economia*, n. 23/2010, p. 1 ss.

DE NATALE D., *Attività di contrasto alla pedopornografia online: aspetti problematici della responsabilità delle persone fisiche e degli enti*, in *Rivista trimestrale di diritto penale dell'economia*, n. 22/2009, p. 793 ss.

DE NATALE D., *Responsabilità penale dell'Internet Service Provider per omesso impedimento e per concorso nel rato di pedopornografia*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

DE SIMONE G., *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione, in* penalecontemporaneo.it, 28 Ottobre 2012.

DE SIMONE G., *Persone giuridiche e responsabilità da reato. Profili storici, dogmatici e comparatistici, Pisa, 2012.*

DE VERO G., *Corso di diritto penale*, Torino, 2012.

DE VERO G., *La responsabilità penale delle persone giuridiche*, Milano, 2008.

DELITALA G., voce *Diritto penale*, in *Enciclopedia del diritto*, 1964, p. 1095 ss.

DI MINCIO S., *Diritto all'oblio e la sentenza della Corte di Giustizia dell'UE del 31 Maggio 2014*, in *Il Documento Digitale*, n. 2/2014.

DIOTALLEVI L., *Internet e Social Network tra "fisiologia" costituzionale e "patologia applicativa",* in *Giurisprudenza di merito*, n. 12/2012, p. 2507 ss.

DIXON A. N., *Liability of users and third parties for copyright infringements on the Internet: overview of international developments*, in STROWEL A. (ed.), *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham, 2009.

DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato*, Terza Edizione, Milano, 2011.

DOLCINI E., PALIERO C. E. (a cura di), *Studi in onore di Giorgio Marinucci*, Milano, 2006.

DOLCINI E., *Principi costituzionali e diritto penale alle soglie del nuovo millennio*, in *Rivista italiana di diritto e procedura penale*, 1999, p. 10 ss.

DONINI M., *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in penalecontemporaneo.it, 20 Settembre 2013.

DONINI M., *La partecipazione al reato tra responsabilità per fatto proprio e responsabilità per fatto altru*i, in *Rivista italiana di diritto e procedura penale*, 1984, p. 175 ss.

DONINI M., voce *Teoria del reato*, in *Digesto delle discipline penalistiche*, 1999, p. 221 ss.

DÖRR D., JANICH S., *The criminal responsibility of Internet Service Providers in Germany*, in *Mississippi Law Journal*; v. 80, n. 4, 2011, p. 1247 ss.

DOUGLAS M. F., *Reno v. ACLU*, in PARKER R. A., *Free speech on trial*, Tuscaloosa, 2003.

DOUGLAS M. F., TUMAN J. S., *Freedom of Expression in the Marketplace of Ideas*, California, 2010.

ECONOMIDES N., *The Telecommunications Act of 1996 and its impact*, in nyu.edu, Settembre 1998.

EDWARDS L., *Role and responsibility of internet intermediaries in the field of copyright and related rights*, in wipo.int, 22 Giugno 2011.

FALETTI E., *La responsabilità dell'Internet Provider in Diritto Comparato per materiale pubblicato da terzi*, in *Diritto dell'Internet*, n. 2/2007, p. 137 ss.

FERRI E., *Principio di diritto criminale*, Torino, 1928.

FERRUA P., *Le insanabili contraddizioni nella responsabilità dell'impresa*, in *Diritto e Giustizia*, n. 29/2001, p. 79 ss.

FIANDACA G., DI CHIARA G., *Introduzione al sistema penale per una lettura costituzionalmente orientata*, Napoli, 2003.

FIANDACA G., *Il reato commissivo mediante omissione*, Milano, 1979.

FIANDACA G., MUSCO E., *Diritto penale. Parte generale*, Sesta Edizione, Bologna, 2009.

FINOCCHIARO G.*, Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'Informazione e dell'Informatica*, 2014, p. 591 ss.

FINOCCHIARO G.*, Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'Informazione e dell'Informatica*, 2014, p. 591 ss.

FIORELLA A., voce *Reato in generale*, in *Enciclopedia del diritto*, 1987, p. 770 ss.

FIORELLA A., voce *Responsabilità penale*, in *Enciclopedia del diritto*, 1988, p. 1289 ss.

FLICK C., AMBRIOLA V., *Dati nelle nuvole: aspetti giuridici del Cloud computing e applicazione alle amministrazioni pubbliche*, in federalismi.it, 20 marzo 2013.

FLICK M. G., *Problemi attuali e profili costituzionali del diritto penale d'impresa*, in *Rivista italiana di diritto e procedura penale*, 1983, p. 433 ss.

FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Rivista trimestrale di diritto penale dell'economia*, n. 3/2009, p. 695 ss.

FLOR R., *Concezione dualistica dei diritti d'autore e tutela penale: quali prospettive per la rivalutazione della componente personalistico?*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013.

FLOR R., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, in *Il Diritto dell'Informazione e dell'Informatica,* 2014, p. 775 ss.

FLOR R., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention*, in *Ciberspazio e diritto*, 2010, p. 359 ss.

FLOR R., *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in penalecontemporaneo.it, 28 Aprile 2015.

FLOR R., *La rilevanza penale dell'immissione abusiva in un sistema di reti telematiche di un'opera dell'ingegno protetta: bene iudicat qui beni distinguit?*, in *Il Diritto*

dell'Informazione e dell'Informatica, n. 3/2007, p. 557 ss.

FLOR R., *La tutela penale della proprietà intellettuale ed il contrasto alla commercializzazione ed alla circolazione in Internet di opere o prodotti con segni falsi o alterati*, in CAMALDO L. (a cura di), *La circolazione e il contrabbando di prodotti contraffatti o pericolosi. La tutela degli interessi finanziari dell'Unione Europea e la protezione dei consumatori*. *Atti del Convegno europeo svoltosi a Milano il 31 maggio 2012, organizzato dal Centro Studi di diritto penale europeo, in stretta collaborazione con OLAF (Ufficio europeo per la lotta antifrode) e con UAE (Unione degli Avvocati Europei)*, Torino, 2013.

FLOR R., *Le recenti sentenze del Bundesverfassungsgericht e della Curtea Constituţională sul data retention*, in unicam.it, *Atti del Convegno - Ascoli Piceno*, 5-7 Marzo 2010.

FLOR R., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, in penalecontemporaneo.it, 20 Settembre 2012.

FLOR R., *Misure tecnologiche di protezione ed anticipazione della punibilità nel sistema di tutela penale dei diritti d'autore e connessi in Europa*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

FLOR R., *Nuove tecnologie e giustizia penale in Europa, tra le esigenze di accertamento e prevenzione dei reati e quelle di tutela della riservatezza: il ruolo «propulsore» della Corte di Giustizia*, in *Studi in onore di Maurizio Pedrazza Gorlero*, Napoli, 2014.

FLOR R., *Phishing, identity theft* e *identity abuse*: *le prospettive applicative del diritto penale vigente*, in *Rivista italiana di diritto e procedura penale*, 2007, p. 899 ss.

FLOR R., *Sequestro preventivo di siti web e abusiva trasmissione telematica di programmi televisivi. Nota a G.i.p. Trib. Milano (ord.), 07.1.2013, Giud. Ghinetti*, in penalecontemporaneo.it, 15 Marzo 2013.

FLOR R., *Social Networks e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Rivista trimestrale di diritto penale dell'economia*, n. 3/2012 , p. 647 ss.

FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale,* Padova, 2010.

FOGLIANI E., *Verso una irresponsabilità oggettiva del provider?*, in interlex.it, 24 Luglio 1998. MONTANARI M., *Il Senato approva il ddl. in materia di diffamazione*, in penalecontemporaneo.it, 11 Novembre 2014.

FORNASARI G., *Il ruolo della esigibilità nella definizione della responsabilità penale del*

Provider, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

FROSINI T. E., A*ccess to internet as a fundamental right*, in *Italian journal of Public Law*, Vol. 5, Issue 2/2013, p. 226 ss.

FROSINI T. E., *Diritto all'oblio e Internet*, in federalismi.it, 10 Giugno 2014.

FROSINI T. E., *Internet come ordinamento giuridico*, in *Percorsi costituzionali*, n. 1/2014, p. 13 ss.

FROSINI T. E., *Liberté, Egalité, Internet*, in *Percorsi costituzionali*, n. 1/2014, p. 1 ss.

GALDIERI P., *Il trattamento illecito del dato nei social network*, in *Giurisprudenza di merito*, n. 12/2012, p. 2697 ss.

GALGANO F., *Delle persone giuridiche*, in *Commentario del Codice Civile Scialoja – Branca*, Bologna, Roma, 2006, p. 3 ss.

GALLI C., voce *Marchio e altri segni distintivi*, in treccani.it.

GALLI L., *L'art. 57, n. 1, c.p. e l'art. 27 della Costituzione*, in *Giustizia Penale*, 1950, p. 770 ss. CARNELUTTI F., *Teoria generale del reato*, Padova, 1933.

GALLO M., *L'elemento oggettivo del reato*, Torino, 1969.

GALLO M., voce *Capacità penale*, in *Novissimo Digesto Italiano*, 1958, p. 885 ss.

GAMBULI M., *La responsabilità penale del provider per i reati commessi in internet*, in altalex.com, 24 Ottobre 2005.

GATTA G. L., *Protezione dei minori contro lo sfruttamento e l'abuso sessuale: ratificata la Convenzione di Lanzarote del 2007 (e attuata una mini-riforma nell'ambito dei delitti contro la persona),* in penalecontemporaneo.it, 20 Settembre 2012.

GATTEI C., *Considerazioni sulla responsabilità dell'Internet provider*, in interlex.it, 23 Novembre 1998.

GIOVANELLA F., *La responsabilità per linking a files audiovisivi contraffatti e l'incerta natura del motore di ricerca*, in *Danno e Responsabilità*, n. 8-9/2011, p. 847 ss.

GRABENWARTER C., *European Convention on Human Rights*, München, 2014.

GRASSO G., *Il reato omissivo improprio*, Milano, 1983.

GRASSO G., *La «competenza penale» dell'Unione Europea nel quadro del Trattato di Lisbona*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

GRASSO G., SICURELLA R. (a cura di), *Lezioni di diritto penale europeo*, Milano, 2007.

GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo. Esigenze di*

tutela degli interessi comunitari e nuove strategie di integrazione penale, Milano, 2008.

GRISPIGNI F., *Diritto Penale Italiano*, Milano, 1947.

GROSSO C. F., *L'errore sulle scriminanti*, Milano, 1961.

GROSSO C. F., voce *Responsabilità penale*, in *Novissimo Digesto Italiano*, 1968, p. 707 ss.

GUARNERI G., *La responsabilità anomala per i delitti commessi a mezzo della stampa e il principio costituzionale della personalità della responsabilità penale*, in *Giurisprudenza Italiana*, 1950, p. 12 ss.

HAGGERTY R. K., ERICSON V. R., *The surveillant assemblage*, in *British Journal of Sociology*, n. 51/2000, p. 605 ss.

HASSANABADI A., *Red flags of "piracy" online*, in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, London, 2013.

HAZLETT T. V., *Economic and Political Consequences of the 1996 Telecommunications Act*, in *Hastings Law Journal*, 50-1998/1999, p. 1359 ss.

HOEREN T., in *MMR*, 3/2004, p. 168 ss.

HOEREN T., *Liability for Online Services in Germany*, in *German Law Journal*, v. 10, n. 5, 2009, p. 561 ss.

IANNI V., *La responsabilità in sede penale dell'internet service provider alla luce dei più recenti decisa giurisprudenziali*, in neldiritto.it., 1 Marzo 2011.

IASELLI M., *Caso Facebook, il "Safe harbor" si può disapplicare: una svolta epocale?*, in altalex.com, 18 Ottobre 2015.

IASELLI M., *Diritto all'oblio: Cassazione ne conferma il riconoscimento*, in altalex.com, 16 Aprile 2012.

INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, in LUPARIA L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012.

INGRASSIA A., *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali*, in penalecontemporaneo.it, 4 Marzo 2013.

INGRASSIA A., *La sentenza della Cassazione sul caso Google*, in penalecontemporaneo.it, 6 Febbraio 2014.

KNIEPS G., *Competition in Telecommunication and the Internet Services. A Dynamic Perspective*, in BARFIELD C. E., HEIDUK G., WELFENS P.J.J. (eds.), *Internet, Economic Growth and Globalization – Perspectives on the New Economy in Europe, Japan and the US*, Berlin et al., 2003.

KOELMAN K., HUGENHOLTZ B., *Online Services Provider Liability for Copyright*

Infringement, WIPO Workshop on Service Provider Liability, Geneva, 9 dicembre 1999.

KOOPS B., PRINCE C., HIJAMANS H, *ICT Law and Internationalisation: A Survey of Government Views*, The Hague, 2000.

LANGDON R. T., *The Communications Decency Act § 230: Make Sense? Or Nonsense?-A Private Person's Inability to Recover if Defamed in Cyberspace*, in *St. John's Law Review*, Volume 73-Issue 3, Article 11, 1999.

LUPARIA L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012.

LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processuali*; in *Diritto penale e processo*, n. 6/2008, p. 717 ss.

MAGGIORE G., *Diritto Penale*, Bologna, 1951.

MAGLI S., SPOLIDORO M. S., *La responsabilità degli operatori in Internet: profili interni e internazionali*, in *Il Diritto dell'Informazione e dell'Informatica*, 1997, p. 61 ss.

MAIELLO V., *La natura (formalmente amministrativa, ma sostanzialmente penale) della responsabilità degli enti nel D. Lgs. N. 231/2001: una truffa di etichette davvero innocua?*, *in Rivista trimestrale di diritto penale dell'economia*, 2002, p. 879 ss.

MAMBRIANI A., *art. 57 c.p.*, in DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato*, Terza Edizione, Milano, 2011.

MANES V., *Il principio di offensività nel diritto penale*, Torino, 2005.

MANES V., *Metodo e limiti dell'interpretazione conforme alle fonti sovranazionali in materia penale*, in penalecontemporaneo.it, 9 Luglio 2012.

MANES V., ZAGREBELSKY V., (a cura di), *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011.

MANNA A., *I soggetti in posizione di garanzia*, in *Il Diritto dell'Informazione e dell'Informatica*, 2010, p. 779 ss.

MANNA A., *La c.d. responsabilità amministrativa delle persone giuridiche: un primo sguardo d'insieme*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 501 ss.

MANNA L., *Internet e diritto "all'oblio": una recente sentenza del Tribunale di Milano*, ilsole24ore.com, 29 Luglio 2013.

MANTOVANI F., *Diritto penale. Parte generale*, Ottava Edizione, Padova, 2013.

MANZONI I., voce *Illecito amministrativo tributario*, in *Enciclopedia del diritto*, 2007, p. 717 ss.

MARINI G., DI LA MONICA M., MAZZA L., *Commentario al Codice Penale*, Torino, 2002.

MARINUCCI G., *Il reato come "azione". Critica di un dogma*, Milano, 1971.

MARSDEN C. T., *Internet Co-Regulation: European Law, Regulatory Governance and*

Legitimacy in Cyberspace, Cambridge, 2011.

MARUCCIA A., *Net neutrality USA, le nuove regole*, in punto-informatico.it, 27 Febbraio 2015.

MASERA L., *I nuovi delitti contro l'ambiente - voce per il "libro dell'anno del diritto Treccani 2016*, in penalecontemporaneo.it, 17 Dicembre 2015.

MAUGERI A. M., *I principi fondamentali del sistema punitivo comunitario: la giurisprudenza della Corte di Giustizia e della Corte europea dei diritti dell'uomo*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008.

MAUGERI A. M., *Il principio di proporzione nelle scelte punitive del legislatore europeo. L'alternativa delle sanzioni amministrative comunitarie*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

MAUGERI A. M., *Il sistema sanzionatorio comunitario dopo la Carta europea dei diritti fondamentali*, in GRASSO G., SICURELLA R. (a cura di), *Lezioni di diritto penale europeo*, Milano, 2007.

MELZI D'ERIL C., *La Cassazione esclude l'estensione ai siti internet delle garanzie costituzionali previste per il sequestro degli stampati*, in penalecontemporaneo.it, 25 Marzo 2014.

MELZI D'ERIL C., *La complessa individuazione dei limiti alla manifestazione del pensiero in Internet*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 4-5/2011, p. 571 ss.

MELZI D'ERIL C., *Roma Locuta: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testate giornalistica on line*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2010, p. 895 ss.

MELZI D'ERIL C., VIGEVANI G. E., *Ancora sulla Dichiarazione dei diritti di Internet. Riflessioni sparse in tema di anonimato*, in medialaws.eu, 11 Febbraio 2015.

MELZI D'ERIL C., VIGEVANI G. E., *La responsabilità del direttore telematico, tra difficili equiparazioni e specificità di internet*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/2010, p. 91 ss.

MELZI D'ERIL C., VIGEVANI G. E., *Tra carta e online parificazione assai discutibile*, in medialaws.eu, 30 Luglio 2015.

MEZZANOTTE M., *Il diritto all'oblio: contributo allo studio della privacy storica*, Napoli, 2009.

MILITELLO V., *L'identità della scienza giuridica penale nell'ordinamento multilivello*, in *Rivista italiana di diritto e procedura penale*, n. 1/2014, p. 106 ss.

MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Rivista trimestrale di diritto penale dell'economia*, 1992, p. 372 ss.

MINOTTI D., *Responsabilità penale: il provider è tenuto ad "attivarsi"?*, in interlex.it, 5 Maggio 2003.

MONTARI M., *L'attuazione italiana della direttiva 2011/36/UE: una nuova mini-riforma dei delitti di riduzione in schiavitù e di tratta di persone*, in penalecontemporaneo.it, 20 Marzo 2014.

MORALES G. O., *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul Cyber*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

MOSCA A., *Una breve scheda sullo stato dell'arte della normativa europea sui diritti di proprietà intellettuale*, in alessiamosca.it, 22 Marzo 2015.

NAGEL D., *I fornitori di servizi internet in Germania tra forme di responsabilità e doveri di collaborazione,* in LUPARIA L. (a cura di), *Internet provider e giustizia penale*, *Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012.

NANNIPIERI L., *Il mantenimento di contenuti diffamatori negli archivi online dei quotidiani e la pretesa alla conservazione dell'identità digitale in una recente sentenza della Corte Europea dei Diritti dell'Uomo*, in medialaws.eu, 6 Dicembre 2013.

NATALE D., *Attività di contrasto alla pedopornografia on line: aspetti problematici della responsabilità delle persone fisiche e degli enti (parte seconda)*, in *Rivista trimestrale di diritto penale dell'economia*, n. 23/2010, p. 1 ss.

NATALE D., *Attività di contrasto alla pedopornografia online: aspetti problematici della responsabilità delle persone fisiche e degli enti*, in *Rivista trimestrale di diritto penale dell'economia*, n. 22/2009, p. 793 ss.

NATOLI R., *La tutela dell'onore e della reputazione in internet: il caso della diffamazione anonima*, in *Europa e diritto privato*, n. 2/2001, p. 441 ss.

NICOSIA E., *Convenzione europea dei diritti dell'uomo e diritto penale*, Torino, 2006.

NIVARRA L. - RICCIUTO V. (a cura di), *Internet e il diritto dei privati*, Torino, 2002.

NUVOLONE P., *I reati di stampa*, Milano, 1951.

NUVOLONE P., *Il diritto penale della stampa*, Padova, 1971.

NUVOLONE P., *Le leggi penali e la Costituzione*, Milano, 1953.

NUVOLONE P., voce *Pena (diritto penale)*, in *Enciclopedia del diritto*, 1982, p. 787 ss.

PAGLIARO A., *Il fatto di reato*, Palermo, 1960.

PALAZZO F. C., *Ignorantia legis*: *vecchi limiti ed orizzonti nuovi della colpevolezza*, in *Rivista italiana di diritto e procedura penale*, 1988, p. 920 ss.

PALAZZO F. C., *Il problema dell'ignoranza della legge penale nelle prospettive di riforma*, in *Rivista italiana di diritto e procedura penale*, 1975, p. 777 ss.

PALIERO C. E., *"Materia penale" e illecito amministrativo secondo la Corte Europea dei Diritti dell'Uomo: una questione "classica" a una svolta radicale*, in *Rivista italiana di diritto e procedura penale*, 1985, p. 894 ss.

PALIERO C. E., TRAVI A., *La sanzione amministrativa. Profili sistematici*, Milano, 1988.

PALIERO C.E., *La responsabilità delle persone giuridiche: profili generali e criteri di imputazioni, in* ALESSANDRI A. (a cura di), *Il nuovo diritto penale delle società*, Milano, 2002.

PALIERO C. E. (a cura di), *Studi in onoore di Giorgio Marinucci*, Tomo II, Milano, 2006.

PALIERO C.E., *Le sanzioni comunitarie quale modello di disciplina per la responsabilità da reato delle persone giuridiche*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008.

PARKER R. A., *Free speech on trial*, Tuscaloosa, 2003.

PASCUZZI G. (a cura di), *Diritto e informatica*, Milano, 2002.

PASCUZZI G. (a cura di), *Diritto e informatica: l'avvocato di fronte alle tecnologie digitali*, Milano, 2002.

PASTENA R., *Internet e privacy: una relazione complicata (A margine della sentenza della Corte di Giustizia del 13 maggio 2014)*, in osservatorioaic.it, Luglio 2014.

PATERNITI C., voce *Economia pubblica (delitti contro)*, in *Enciclopedia Giuridica Treccani*, 1989, p. 1 ss.

PATRONO P., *Problematiche attuali dell'errore nel diritto penale dell'economia*, in *Rivista trimestrale di diritto penale dell'economia*, 1988, p. 87 ss.

PATRONO P., *Verso la soggettività penale degli enti, in Rivista trimestrale di diritto penale dell'economia*, 2002, p. 183 ss.

PATTINAVIA A. (ed.), *Information Technology and the Criminal Justice System*, Thousand Oaks, Califronia, 1995.

PAVICH G., *Le novità del decreto legge sulla violenza di genere: cosa cambia per i reati con vittime vulnerabili*, in penalecontemporaneo.it, 24 Settembre 2013.

PECORA C., *Diritto all'oblio: il problema della estensione extraeuropea della deindicizzazione tra effettività della rimozione e libertà di informazione*, in medialaws.eu, 18 Settembre 2015.

PECORA C., *Diritto all'oblio: il problema della estensione extraeuropea della deindicizzazione tra effettività della rimozione e libertà di informazione*, in medialaws.eu,

18 Settembre 2015.

PECORELLA C., *Diritto penale dell'informatica*, Padova, 2006.

PECORELLA G., *Societas delinquere potest,* in *Rivista giuridica del lavoro*, 1977, p. 357 ss.

PERON S., *La diffamazione tramite i motori di ricerca*, in personaedanno.it, 3 Aprile 2011. SCANNICCHIO T., *La responsabilità del motore di ricerca per la funzione «auto-complete»*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2012, p. 1212 ss.

PETTI R., *La protezione dei dati personali e il caso Google Spain*, in dimt.it, 20 Marzo 2015.

PEZZELLA V., *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, in *Giurisprudenza di merito*, n. 9/2010, p. 2232 ss.

PICA G., *Diritto penale delle tecnologie informatiche: computer's crimes e reati telematici, internet, banche dati e privacy*, Torino, 1999.

PICA G., voce *Reati informatici e telematici*, in *Digesto* delle *Discipline Penalistiche, 2000, p. 521 ss.*

PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013.

PICOTTI L., *Commento Art. 600-ter, III comma, c. p. (Pornografia minorile)* in CADOPPI A. (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006.

PICOTTI L., *Fondamento e limiti della responsabilità penale dei Service Providers*, in *Diritto Penale e Processo*, n. 31/1999, p. 379 ss.

PICOTTI L., *I diritti fondamentali nell'uso e abuso dei social network. Aspetti penali*, in *Giurisprudenza di merito*, n. 12/2012 , p. 2522 ss.

PICOTTI L., *Internet e responsabilità penali*, in PASCUZZI G. (a cura di), *Diritto e informatica*, Milano, 2002.

PICOTTI L., *La Convenzione di Lanzarote per la tutela penale dei minori dagli abusi sessuali e la sua attuazione in Italia*, in AIAF, n. 3/2013, p. 49 ss.

PICOTTI L., *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet (l. 6 febbraio 2006, n. 38) (parte prima),* in *Studium iuris*, 2007, p. 1059 ss.

PICOTTI L., *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. 1196 ss.

PICOTTI L., *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Rivista trimestrale di diritto penale dell'economia*, n. 4/2011, p. 827

ss.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Diritto penale e processo*, n. 6/2008, p. 700 ss.

PICOTTI L., *La responsabilità penale dei service-providers in Italia*, in *Diritto penale e processo*, n. 3/1999, p. 501 ss.

PICOTTI L., *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

PICOTTI L., *Pornografia minorile: evoluzione della disciplina penale e beni giuridici tutelati*, in FIORAVANTI L. (a cura di), *La tutela penale della persona: nuove frontiere, difficili equilibr*i, Milano, 2001.

PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, in *Il Diritto dell'Informazione e dell'Informatica*, Milano, 1999, p. 283 ss.

PICOTTI L., RUGGIERI F. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Milano, 2012.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati* in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

PICOTTI L., *Studi di diritto penale dell'informatica*, Verona, 1992.

PICOTTI L., *Superamento della c.d. tecnica del "doppio testo" e tutela penale degli interessi europei*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008.

PICOTTI L., voce *Invenzioni industriali. III) Tutela penale*, in *Enciclopedia Giuridica Treccani*, 1989, p. 1.

PICOTTI L., voce *Reati informatici,* in *Enciclopedia Giuridica Treccani*, 2000, p. 30 ss.

PIERGALLINI C., *Sistema sanzionatorio e reati previsti dal codice penale,* in *Diritto Penale e Processo*, n. 11/2001, p. 1353 ss.

PIERGALLINI C., *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, p. 571 ss.

PINO G., *Assenza di un obbligo generale di sorveglianza a carico degli Internet Services Providers sui contenuti immessi da terzi in rete*, in *Danno e Responsabilità*, n. 9/2004, p. 832 ss.

PIOLETTI U., *Ingiuria, diffamazione e reti sociali*, in *Giurisprudenza di merito*, n.

12/2012, p. 2652 ss.

PIROZZOLI A., *La responsabilità dell'Internet Service Provider. Il nuovo orientatmento giurisprudenziale nell'ultimo caso Google*, in *Rivista telematica giuridica dell'Associazione italiana dei Costituzionalisti*, n. 3/2012, rivistaaic.it.

PIROZZOLI A., *La responsabilità dell'internet service provider. Il nuovo orientamento giurisprudenziale nell'ultimo caso Google*, in *Rivista AIC*, n. 3/2012, 25 Settembre 2012.

PISAPIA G. D., *La nuova disciplina della responsabilità per i reati commessi a mezzo stampa*, in *Rivista italiana di diritto e procedura penale*, 1958, p. 304 ss.

PISTORELLI L., ANDREAZZA G., *Legge 1 ottobre 2012, n. 172 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007)*, in penalecontemporaneo.it, 22 Ottobre 2012.

PISTORELLI L., *Legge 15 febbraio 2012, n. 12, recante "Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica" – Disposizioni rilevanti per il settore penale. Relazione a cura dell'Ufficio del Massimario della Corte di Cassazione*, in penalecontemporaneo.it, 28 Febbraio 2012.

PISTORELLI L., *Prima lettura del decreto-legge 14 agosto 2013, n. 93 (Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province). Relazione a cura dell'Ufficio del Massimario della Corte di Cassazione*, in penalecontemporaneo.it, 28 Agosto 2013.

PISTORELLI L., *Prime note sulla legge di conversione, con modificazioni, del d.l. n. 93 del 2013, in materia tra l'altro di «violenza di genere» e di reati che coinvolgano minori. Relazione a cura dell'Ufficio del Massimario della Corte di Cassazione*, in penalecontemporaneo.it, 18 Ottobre 2013.

POLLICINO O., *"Suggest search": le posizioni del giudice di Milano e di Parigi*, in diritto24.ilsole24ore.com, 23 Gennaio 2012.

POLLICINO O., BASSINI M., *Le parole contano", ovvero "tanto rumore per nulla". Sulla (prevista) inammissibilità della questione di legittimità costituzionale della base giuridica del Regolamento AGCOM #ddaonline*, in medialaws.eu, 4 Dicembre 2015.

POLLICINO O., *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in forumcostituzionale.it, 31 Dicembre 2013.

POLLICINO O., *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi costituzionali*, n. 1/2014, p. 45 ss.

POMANTE G., *Internet e criminalità*, Torino, 1999.

PUGIOTTO A., *Il volto costituzionale della pena (e i suoi sfregi)*, in

penalecontemporaneo.it, 10 Giugno 2014.

PULITANÒ D., *Il favoreggiammento personale tra diritto e procedura penale*, Milano, 1984.

PULITANÒ D., *L'errore di diritto nella teoria del reato*, Milano, 1976.

PULITANÒ D., *La cultura giuridica e la fabbrica delle leggi*, in penalecontemporaneo.it, 28 Ottobre 2015.

PULITANÒ D., *La responsabilità da "reato" degli enti: i criteri di imputazione*, in *Rivista italiana di diritto e procedura penale*, 2002, p. 415 ss.

PULITANÒ D., *Una sentenza storica che restaura il principio di colpevolezza*, in *Rivista italiana di diritto e procedura penale*, 1988, p. 686 ss.

PULITANÒ D., voce *Ignoranza*, in *Enciclopedia del diritto*, 1970, p. 23 ss.

PULVIRENTI A., *Sequestro e internet: un difficile binomio tra "vecchie" norme e "nuove" esigenze*, in *Processo penale e giustizia*, n. 1/2015, p. 111 ss.

RAZZANTE R., *Manuale di diritto dell'informazione e della comunicazione. Privacy, diffamazione e tutela della persona. Libertà e regole nella Rete*, Milano, 2013.

RECCHIONE S., *Il decreto legge sul contrasto alla violenza di genere: una prima lettura*, in penalecontemporaneo.it, 15 Settembre 2013.

REICHMAN J. H., DINWOODIE R. G., SAMUELSON P., *A reverse notice and takedown regime to enable public interest uses of technically protected copyrighed works*, in STROWEL A. (ed.), *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham, 2009.

RESTA F., *Diffusione telematica della pedopornografi. Pedopornografia on-line. Verso un sistema di tutela a strategia integrata?*, in *Diritto dell'internet*, n. 3/2007, p. 221 ss.

RESTA F., *La responsabilità penale del provider: tra laissez faire ed obblighi di controllo*, in *Giurisprudenza di merito*, 2004, p. 1715 ss.

RESTA F., *Libertà della rete e protezione dei dati personali: ancora sul caso Google-Vivi Down*, in *Il Diritto dell'Informazione e dell'Informatica*, 2013, p. 502 ss.

RICCIO M. G., *Diritto all'oblio e responsabilità dei motori di ricerca*, in *Diritto dell'Informazione e dell'Informatica*, 2014, p. 753 ss.

RICCIO M. G., *Google: sulle ricerche automatiche esclusa la diffamazione*, in diritto24.ilsole24ore.com, 4 Maggio 2012.

RICCIO M. G., *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e Responsabilità*, n. 2/2003, p. 1157 ss.

RICCIO M. G., *Suggest-ioni e inserzioni: a proposito di due recenti sentenze*, in medialaws.eu, 4 Gennaio 2012.

RICCIO M. G., voce *Responsabilità penale*, in *Enciclopedia giuridica Treccani*, 1993, p. 1 ss.

RINALDINI F., *art. 110 c.p.*, in DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato*, Terza Edizione, Milano, 2011.

RISICATO L., *La partecipazione mediante omissione a reato commissivo*, in *Rivista italiana di diritto e procedura penale*, 1995, p. 1267 ss.

RISTUCCIA R., TUFFARELLI L., *La natura giuridica di Internet e la responsabilità del provider*, in interlex.it, 19 Giugno 1997.

RIVERDITI M., *La responsabilità degli enti un crocevia tra repressione e specialprevenzione*, Napoli, 2009.

RODOTÀ S., *La vita e le regole. Tra diritti e non diritto*, Milano, 2006.

RODOTÀ S., *Relazione introduttiva: Libertà, opportunità, democrazia, informazione*, Convegno *Internet e privacy – Quali regole?*, Roma, 8 Maggio 1998, in privacy.it.

RODOTA' S., *Verso una Dichiarazione dei diritti di Internet*, in camera.it.

ROMANO M., *Commentario sistematico del Codice penale*, Milano, 1995.

ROMANO M., *Societas delinquere non potest (Nel ricordo di Franco Bricola)*, in *Rivista italiana di diritto e procedura penale*, 1995, p. 1031 ss.

RONCO M., *Responsabilità delle persone giuridiche*, in *Enciclopedia giuridica*, 2002, p. 1 ss.

ROSSELLO C., *Riflessioni de jure condendo in materia di responsabilità del provider*, in *Il Diritto dell'Informazione e dell'Informatica*, 2010, p. 617 ss.

ROSSETTI S., *Una sentenza di merito sembra eludere l'orientamento negativo della Cassazione in tema di responsabilità del blogger per le affermazioni diffamatorie provenienti dai frequentatori del sito*, in penalecontemporaneo.it, 11 Giugno 2013.

RUGA RIVA C., *I nuovi ecoreati, Commento alla legge 22 maggio 2015, n. 68*, Torino, 2015.

RUGGERI A., *"Dialogo" tra le Corti e tecniche decisorie, a tutela dei diritti fondamentali*, in diritticomparati.it, 19 Novembre 2013.

SALVADORI I., *L'accesso abusivo ad un sistema informatico telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti del diritto penale dell'informatica*, in PICOTTI L. (a cura di) *Tutela penale della persona e nuove tecnologie*, Padova, 2013.

SALVADORI I., *Presupposti della responsabilità penale del blogger per gli scritti offensivi pubblicati su un blog da lui gestito*, in *Giurisprudenza di merito*, n. 4/2007, p. 1069 ss.

SAMMARCO P., *Assegnazione dei nomi a dominio su Internet, interferenze con il marchio, domain grabbing e responsabilità del provider*, in *Il Diritto dell'Informazione e*

dell'Informatica, n. 1/2000, p. 67 ss.

SAMMARCO P., *Il ruolo di YouTube tra intermediario del commercio elettronico e fornitore di servizi di media audiovisivi*, in *Il Diritto dell'Informazione e dell'Informatica*, 2012, p. 965 ss.

SANSOBRINO F., *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in penalecontemporaneo.it, 30 Settembre 2014.

SARGENTI B., *Giurisdizione e competenza territoriale in materia penale*, in *Giurisprudenza di merito*, n. 12/2012, p. 2642 ss.

SARZANA C., *Note sul diritto penale dell'informatica*, in *La Giustizia Penale*, n. 1/1984, p. 21 ss.

SCANNICCHIO T., *Il provider non risponde degli accostamenti diffamatori prodotti automaticamente dal motore di ricerca*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 2/2013, p. 380 ss.

SCANNICCHIO T., *La responsabilità del provider di fronte alle corti inglesi: una vittoria di Pirro per Google?*, in *Il Diritto dell'Informazione e dell'Informatica*, 2013, p. 751 ss.

SEMINARA S., *Internet (diritto penale)*, in *Enciclopedia del diritto* – Annali vol. VII, 2014, p. 567 ss.

SEMINARA S., *La pirateria su Internet e il diritto penale*, in *Rivista trimestrale di diritto penale dell'economia*, 1997, Padova, p. 71 ss.

SEMINARA S., *La responsabilità penale degli operatori su Internet*, in *Diritto dell'Informazione e dell'Informatica*, 1998, p. 745 ss.

SEMINARA S., *Tutela penale del diritto d'autore tra normativa vigente e prospettive di riforma*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

SENOR M., *Le tensioni del diritto all'oblio*, in medialaws.eu, 21 Aprile 2015.

SENOR M., *Un altro "tango down" in tema di data retention*, in medialaws.eu, 22 Luglio 2015.

SGUBBI F., *Responsabilità penale per omesso impedimento dell'evento*, Padova, 1975.

SICA S., CODIGLIONE G., *Social network sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, n. 12/2012, p. 2714 ss.

SICA S., D'ANTONIO V., *La procedura di de-indicizzazione*, in *Il Diritto dell'Informazione e dell'Informatica*, 2014, p. 703 ss.

SICURELLA R., *"Eppur si muove!": alla ricerca di un nuovo equilibrio nella dialettica tra legislatore comunitario e legislatore nazionale per la tutela degli interessi dell'Unione europea*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo.*

Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale, Milano, 2008.

SICURELLA R., *«Prove tecniche» per una metodologia dell'esercizio delle nuove competenze concorrenti dell'Unione Europea in materia penale*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

SICURELLA R., *Prosegue l'azione dell'Unione europea nella lotta alla tratta di esseri umani*, in penalecontemporaneo.it, 25 Luglio 2011.

SIEBER U., *Information technology crime*, Köln, Berlin, Bonn, München, 1994.

SIEBER U., *Responsabilità penali per la circolazioni di dati nelle reti internazionali di computer. Le nuove sfide di internet*, trad. it. a cura di Sforzi, in *Rivista trimestrale di diritto penale dell'economia*, 1997, p. 743 ss. – p. 1193 ss.

SIEBER U., *The future of European Criminal Law: a new approach to the aims and models of the European Criminal Law system*, in GRASSO G., SICURELLA R. (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, 2008.

SIEBER U., *The international emergence of Criminal Information Law*, Köln, 1992.

SORO A., *Persona vulnerabile. La protezione dei dati nella società digitale. Discorso del Presidente. Relazione 2014*, Roma, 23 Giugno 2015.

SPAGNOLETTI V., *La responsabilità del provider per i contenuti illeciti in internet*, in *Giurisprudenza di merito*, 2004, p. 1922 ss.

STAMATOUDI I., TORREMANS P. (eds.), *EU Copyright Law: A Commentary*, Cheltenham-Northampton, 2014.

STORTONI L., *Profili penali delle società commerciali come imprenditori*, in *Rivista italiana di diritto e procedura penale*, 1971, p. 1163 ss.

STROWEL A. (ed.), *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham-Northampton, 2009.

SUSSMAN V., *Policing Cyberspace*, in *U.S. News & World Report*, 23 Gennaio 1995.

TABARELLI DE FATIS S., *Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione on-line*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013.

TIBERI G., *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in GRASSO G., PICOTTI L., SICURELLA R. (a cura di), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

TIEDEMANN K., *La responsabilità penale delle persone giuridiche nel diritto comparato*,

in *Rivista italiana di diritto e procedura penale*, 1995, p. 615 ss.

TRABUCCHI A., *Istituzioni di diritto civile*, Padova, 2004.

TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, London, 2013.

TRAVIS H., *Who controls the Internet? The second circuit on YouTube,* in TRAVIS H. (ed.), *Cyberspace Law: Censorship and Regulation of the Internet*, London, 2013.

TROPINA T., CALLANAN T., *Self- and co-regulation in cybercrime, cybersecurity and national security*, Cham-Heidelberg, 2015.

TURCHETTI S., *L'art. 57 c.p. non è applicabile al direttore del periodico online*, in penalecontemporaneo.it, 17 Novembre 2010.

TURCHETTI S., *Un secondo "alt" della Cassazione all'applicazione dell'art. 57 c.p. al direttore del periodico on line*, in penalecontemporaneo.it, 16 Dicembre 2011.

UNGARO S., MAIO E., *Ma la "sentenza Facebook" non invalida il safe harbour: ecco perché*, in agendadigitale.eu, 18 Ottobre 2015.

URBAN J., QUILTER L., *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act: Summary Report*, 2005, in law.berkeley.edu.

VACIAGO G., *La disciplina normativa sulla data ritention e il ruolo degli internet service provider*, in LUPARIA L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012.

VALLE L., *Registrazione e tutela del domain name*, in NIVARRA L. - RICCIUTO V. (a cura di), *Internet e il diritto dei privati*, Torino, 2002.

VAN EECKE P., *Online service providers and liability: A plea for a balanced approach*, in *Common Market Law Review*, n. 48/2011, p. 1455 ss.

VANBERG M., *Competition and cooperation among Internet Service Providers*, Baden, 2009.

VASSALLI G., *La protezione della sfera della personalità nell'era della tecnica*, in *Studi in onore di Emilio* Betti, vol. V, Milano, 1962, p. 675 ss.

VASSALLI G., *Note in margine alla riforma del concorso di persone nel reato*, in DOLCINI E., DOLCINI E., PALIERO C. E. (a cura di), *Studi in onore di Giorgio Marinucci*, cit., p. 1939 ss.

VASSALLI G., *Sulla illegittimità costituzionale dell'art. 57 n. 1 c.p.*, in *Giurisprudenza Costituzionale*, 1956, p. 218 ss.

VASSALLI G., *Sulla legittimità costituzionale della responsabilità penale obbiettiva per fatto proprio*, *e leggi penali e la Costituzione*, in *Giurisprudenza Costituzionale*, 1957, p. 1005 ss.

VENEZIANI P., *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

VENTURI R., *Turchia: promulgata legge-censura su Internet*, in ilreferendum.it, 21 Febbraio.

VERRI A., *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE*, in penalecontemporaneo.it, 28 Marzo 2012.

VIGANÒ F., *L'adeguamento del sistema penale italiano al "diritto europeo"*, in penalecontemporaneo.it, 14 Febbraio 2014.

VIGANÒ F., *Pubblicato sulla Gazzetta Ufficiale il nuovo decreto legge in materia di contrasto al terrorismo*, in penalecontemporaneo.it, 23 Febbraio 2015.

VIGEVANI G. E., *La «sentenza figlia» sul direttore del giornale telematico: il caso Hamaui*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 6/2011, p. 798 ss.

VINCIGUERRA S., *Appunti sull'inoffensività, la tenuità dell'offesa e la tenuità del reato in Italia nel secondo Novecento*, in DOLCINI E., PALIERO C. E. (a cura di), *Studi in onore di Giorgio Marinucci*, Tomo II, Milano, 2006.

VIOLA DE AZEVEDO CUNHA M., MARIN L., SARTOR G., *Peer-to-Peer Privacy Violations and ISP Liability: Data protection in the user-generated web*, in *International Data Privacy Law*, vol. 2, n. 2, 2012, p. 50 ss.

VIZZARDI M., *Sull'"adescamento" di minore tramite social network e il tentativo di atti sessuali con minorenne, Nota a Tribunale di Milano, Uff. Gup, 25 ottobre 2011, Giud. Domanico*, in penalecontemporaneo.it, 9 Febbraio 2012.

VOZZA D., *I confini applicativi del principio del ne bis in idem interno in materia penale: un recente contributo della Corte di Giustizia dell'Unione europea*, in penalecontemporaneo.it, 15 Aprile 2013.

WALL D. S., *Cybercrime: The transformation of crime in the information age*, Cambridge, 2007.

WALL D. S., *Mapping out cybercrimes in a cyberspatial surveillant assemblage*, in WEBSTER F., BALL K. (Eds.), *The intensification of surveillance: Crime, terrorism, and warfare in the information age*, London, 2003.

WALL D. S., *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace*, in *Police Practice & Research: An International Journal*, 8(2), p. 183 ss.

WALL D. S., *The Internet as a Conduit for Criminal Activity (Revised March 2010)*, in PATTINAVIA A. (ed.), *Information Technology and the Criminal Justice System*,

Thousand Oaks, Califronia, 1995.

WEBSTER F., BALL K. (eds.), *The intensification of surveillance: Crime, terrorism, and warfare in the information age*, London, 2003.

ZENO-ZENCOVICH V., *I «prodotti editoriali» elettronici nella l. 7 marzo 2001 n. 62 e il preteso obbligo di registrazione*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 2/2001, p. 153 ss.

ZENO-ZENCOVICH V., *Note critiche sulla nuova disciplina del commercio elettronico dettata dal d.lgs. 70/03*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 3/2003, p. 505 ss.

ZENO-ZENCOVICH V., *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 1/1998, p. 15 ss.

ZICCARDI G., *International Encyclopaedia of Laws – Cyber Law. Italy*, The Netherlands, 2012.

ZICCARDI G., *Internet provider, computer ethics e codici di auto-regolamentazione della condotta*, in LUPARIA L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012.