Collana DIPLAP
Sezione Atti
2015

La giustizia penale nella "rete"

Le nuove sfide della società dell'informazione nell'epoca di Internet

A cura di

Roberto Flor, Daniela Falcinelli, Stefano Marcolini

Edizioni
DiPLaP

I Convegno Nazionale del Laboratorio Permanente di Diritto Penale
Perugia, 19 settembre 2014

Con il patrocinio ed il finanziamento del
Dipartimento di Giurisprudenza dell'Università di Perugia

Laboratorio Permanente di Diritto Penale
Via Fontana, 28 – 20122 Milano (Italia)
C.F. 97664840150
Web: http://labdirpen.wix.com/diplap

DIPLAP Editor

ISBN: 9788894094909

Laboratorio Permanente di Diritto Penale
Via Fontana, 28 – 20122 Milano (Italia)
C.F. 97664840150
Web: http://labdirpen.wix.com/diplap

Collana DIPLAP 2015

Gli autori

Marco Bassini	Dottorando in Diritto Costituzionale Italiano ed Europeo - Università di Verona
Chiara Bigotti	Dottoranda in Diritto Processuale Penale interno, internazionale e comparato - Università degli Studi di Urbino 'Carlo Bo'
Mario Caterini	Ricercatore di Diritto Penale - Università della Calabria
Daniela Falcinelli	Ricercatrice di Diritto Penale - Università degli Studi di Perugia
Roberto Flor	Ricercatore di Diritto Penale - Università di Verona
Gianclaudio Malgieri	SSSUP, Scuola Sant'Anna di Pisa
Stefano Marcolini	Ricercatore di Diritto Processuale Penale - Università dell'Insubria
Josè Antonio Ramos Vàzquez	Dottore in Diritto Penale, *Professor Contractado* - Università di La Coruña (Spagna)
Margherita Siracusa	Dottoranda in Diritto Penale - Università di Macerata
Valeria Spinosa	Dottoressa di Ricerca in Diritto Penale, SSSUP - Scuola Sant'Anna di Pisa
Pasquale Troncone	Ricercatore di Diritto Penale - Università di Napoli Federico II
Marco Trogu	Assegnista di Ricerca in Diritto Processuale Penale - Università di Cagliari

I relatori sono stati selezionati mediante valutazione anonima tra coloro che hanno risposto alla *call for papers*.

INDICE

INTRODUZIONE

Daniela Falcinelli
Roberto Flor
Stefano Marcolini

Il I Convegno nazionale del Laboratorio Permanente di Diritto Penale, tenutosi a Perugia il 19 settembre 2014, ha proposto alla comunità scientifica un incontro di studio sul tema "La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet". Il riscontro si è espresso attraverso un vivace dibattito sui temi più attuali che coinvolgono le complesse implicazioni fra il sistema penale e le nuove tecnologie: la società dell'informazione, infatti, caratterizzata dall'esplosione di Internet e dei nuovi prodotti tecnologici, ha da tempo comportato dei cambiamenti epocali in ogni settore della vita umana, implicanti non solo molteplici opportunità di sviluppo "positivo", sul piano sociale, culturale ed economico. Su questo fertile terreno fioriscono difatti anche nuovi fenomeni, modi e tipi di comportamenti di rilievo penale, e si aprono "altri" percorsi per commettere reati "tradizionali"; d'altro canto il mondo digitale si dimostra una fondamentale frontiera per la lotta alla criminalità moderna, offrendo innovativi strumenti e mezzi per la ricerca delle prove e, in generale, per il contrasto a vasti settori di illiceità penale.

Il *cyberspace*, del resto, costituisce uno spazio virtuale in continua evoluzione, che consente la delocalizzazione delle risorse e la loro raggiungibilità, da parte dell'utente, da ogni luogo e distanza, *real-time*, anche grazie alle nuova dimensione del *cloud* e della "struttura" del *web*, nonchè per effetto della detemporalizzazione delle attività, che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente.

In questa costante trasformazione – che è trasformazione delle stesse modalità comunicative umane, quindi di accesso alle informazioni e di circolazione del sapere - le manifestazioni criminose che si realizzano "in rete", "attraverso la rete" o "tramite strumenti tecnologici" conquistano un crescente rilievo offensivo ed un allarmante impatto sociale, necessitando di una specifica (nel *quomodo* e nel *quantum*) risposta normativa a livello nazionale e sovranzionale. In qust'ottica, sul piano europeo, con l'entrata in vigore del Trattato di Lisbona la "criminalità informatica" è stata inserita nell'art. 83 TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha "competenza penale".

In questo momento storico di grandi cambiamenti - in cui il ricorso alle tecnologie telematiche ed informatiche deve confrontarsi con le esigenze di accertamento dei reati, da un lato, e con quelle di rispetto delle garanzie e dei diritti inviolabili dei cittadini, dall'altro lato – le principali questioni interrogative che il giurista deve affrontare si inseriscono in uno sfondo in cui rimangono minate le categorie classiche del diritto penale, e messi in tensione i principi di offensività, sussidiarietà e proporzione.

I relatori, che sono stati scelti dal comitato scientifico attraverso una *call for papers* anonima, hanno trattato alcune delle tematiche più attuali che emergono in questo orizzonte, evidenziando le difficoltà applicative dell'attuale – lacunoso - assetto

normativo, tenuto a confrontarsi con la pluralità di fonti eterogenee espresse dall'ordinamento europeo ed internazionale, e profilando le concrete prospettive *de jure condendo*.

LA DISCIPLINA PENALE DELLA STAMPA ALLA PROVA DI INTERNET: AVANZAMENTI E ARRESTI NELLA DIALETTICA GIURISPRUDENZIALE DA UNA PROSPETTIVA COSTITUZIONALE[1]

Marco Bassini

Sommario: 1. Introduzione. Una premessa all'apparenza inconferente; 2. La disciplina penale della stampa, a sessant'anni dalla Costituzione; 3. L'applicabilità a Internet delle norme penali di sfavore; 4. La (non) applicabilità a Internet delle norme di favore; 5. Per concludere, tra prospettive di riforma e miopie legiferatrici

1. Introduzione. Una premessa all'apparenza inconferente

Non trovo inutile, nell'introdurre questo scritto, muovere dall'analisi di un caso che ha in realtà ben poco a che vedere con la disciplina della stampa, ma che restituisce senz'altro spunti di interesse comuni all'ambito che più direttamente forma oggetto di questo intervento.

Mi riferisco a una sentenza che la Corte di cassazione ha consegnato di recente,[2] annullando una pronuncia della Corte d'appello di Firenze che aveva condannato l'imputato per il reato di molestie, di cui all'art. 660 c.p., a causa di una serie di apprezzamenti volgari e a sfondo sessuale che questi aveva pubblicato sulla pagina pubblica Facebook in uso a una collega.

La decisione del Supremo Collegio si è concentrata soprattutto su un profilo, vale a dire l'assimilabilità del social network Facebook, e segnatamente della pagina personale di un utente, alla nozione di "luogo pubblico o aperto al pubblico" cui l'art. 660 c.p. àncora (alternativamente all'uso del mezzo telefonico) la rilevanza penale degli atti di molestia o di disturbo.

La Cassazione ha così annullato la condanna emessa dalla Corte d'appello di Firenze, che aveva giudicato la condotta dell'imputato rientrante nella fattispecie incriminatrice, equiparando –in maniera assai discutibile- Facebook all'uso di un telefono.[3] Tuttavia, nell'argomentare il proprio ragionamento, la Corte ha offerto interessanti indicazioni sulla possibilità che gli atti di molestia o disturbo integrassero, astrattamente, la contravvenzione ascritta all'imputato. Secondo la Cassazione, infatti, la riconducibilità alla fattispecie *ex* art. 660 c.p. «non dipenderebbe tanto dall'assimilabilità della comunicazione telematica alla comunicazione telefonica, quanto

[1] L'articolo costituisce una rielaborazione della relazione dal titolo "L'applicabilità della disciplina penale sulla stampa a Internet. Un terreno ancora controverso" tenuta al workshop "La giustizia penale nella rete" organizzato dal Laboratorio Permanente di Diritto Penale (DiPLap), Perugia, 19 settembre 2014.

Sono molto grato al Prof. Giulio Enea Vigevani e all'Avv. Carlo Melzi d'Eril, ai quali devo gli insegnamenti, le indicazioni e i suggerimenti sempre preziosi che hanno accompagnato la preparazione e la stesura di questo lavoro.

[2] Cass., sez. I, 12 settembre 2014, n. 37596.

[3] Giova precisare che nel caso di specie la sentenza pronunciata dalla Corte di Cassazione ha annullato senza rinvio la decisione della Corte d'appello, rilevando l'avvenuta estinzione del reato per prescrizione.

dalla natura stessa di 'luogo' virtuale aperto all'accesso di chiunque utilizzi la rete, di un social network o community quale Facebook». E sul punto, la Corte dichiara che appare innegabile come tale social network rappresenti una sorta di '*agorà* virtuale'. Aggiungendo: «[u]na 'piazza immateriale che consente un numero indeterminato di 'accessi' e di visioni, *resa possibile da un'evoluzione scientifica, che certo il legislatore non era arrivato ad immaginare*. Ma che *la lettera della legge non impedisce di escludere dalla nozione di luogo* e che, a fronte della rivoluzione portata alle forme di aggregazione e alle tradizionali nozioni di comunità sociale, *la sua ratio impone anzi di considerare*».

Con una chiosa finale, la sentenza sembra comunque voler richiamare l'esigenza di una rigorosa verifica (assente nella sentenza gravata) circa l'effettiva pubblicazione di commenti sulla pagina pubblica, così evocando forse un collegamento tra l'accertamento circa la sussistenza del requisito del luogo pubblico o aperto al pubblico e le impostazioni di accesso alla pagina web.

Si tratta di una decisione che, se per un verso risponde probabilmente a un impeto di estensione della tutela penale della vittima rispetto a condotte perpetrate mediante la rete, per altro non sembra pienamente rispettosa dell'essenza del concetto di luogo pubblico o aperto al pubblico immaginata dai padri costituenti, la cui rilevanza è imperniata tutta, stando al dettato costituzionale, sull'esercizio della libertà di riunione, intesa come compresenza volontaria di più persone nello stesso luogo.[4]

Ciò che appare criticabile, in altri termini, è la disinvolture con la quale la giurisprudenza e in alcuni casi lo stesso legislatore sottopongono a torsione l'autenticità del portato costituzionale per favorire una lettura di certe categorie più consona alla garanzia di maggior tutela di alcuni dei diritti in gioco. Con il rischio, tuttavia, di trascurare le conseguenze che questa operazione può recare con sé.

Non si tratta, infatti, di dover pietrificare la lettura delle libertà e delle categorie costituzionali ai tempi in cui esse sono state pensate e ideate, così opponendosi radicalmente a un'opera di interpretazione che l'evoluzione tecnologica spesso impone. Occorre invece coltivare proprio l'atteggiamento opposto: vale a dire offrire una lettura evolutiva alle categorie costituzionali, cogliendo i margini di flessibilità che le stesse disposizioni poste a tutela delle libertà fondamentali offrono, senza tuttavia che tale operazione si risolva in una manipolazione del dettato costituzionale, che si ha quando lo spirito che vi è sotteso viene di fatto a essere snaturato.

Questo atteggiamento, di cui si è voluto dar conto evocando una decisione piuttosto recente, seppure relativa ad altro ambito, si ritrova assai frequente nel dibattito che a livello legislativo e giurisprudenziale caratterizza il tema dell'applicabilità della disciplina penale della stampa a Internet. Tale approccio si traduce essenzialmente lungo due direttrici: talvolta, un'eccessiva disinvoltura nell'applicazione di determinate categorie a Internet, frutto di una lettura semplicistica che pretenda una necessaria riconduzione del mezzo Internet alla stampa tradizionale; talaltra, nell'escludere l'applicazione di garanzie a tutto quanto stampa non è, almeno *strictu sensu*, così interpretando secondo un atteggiamento opposto, cioè con eccessiva rigidità, le

[4] Per alcuni commenti in dottrina, si vv. A. PACE, *La libertà di riunione nella Costituzione italiana*, Milano, 1967; G. AMATO - A. PACE - F. FINOCCHIARO, *Rapporti civili. Art. 13-20 Costituzione*, in *Commentario della Costituzione Branca-Pizzorusso*, Bologna-Roma, 1977; M. RUOTOLO, *Le libertà di riunione e di associazione*, in R. NANIA - P. RIDOLA (a cura di), *I diritti costituzionali*, Torino, II, 2006, 677 ss.; A. GARDINO CARLI, *Riunione* (libertà di), in *Dig. disc. pubbl.*, XIII, Torino, 1997, 479 ss.

categorie alle quali il Costituente e il legislatore hanno inteso riferire un regime di particolare favore.

Si assiste così a uno scontro tra regole antiche e nuovi media, in cui l'obsolescenza delle norme non implica, tuttavia, necessariamente l'esigenza di una loro riformulazione o estensione *ope legis* a fattispecie di nuova emersione. Piuttosto, è un'applicazione delle norme esistenti che sia fedele allo spirito costituzionale loro sotteso e coerente con la logica garantista di cui la disciplina della stampa è pervasa ciò che occorre per evitare un'esacerbazione dello scontro che conduca a esiti, come la proliferazione di norme settoriali, che non paiono certo appaganti.[5]

Muovendo da questo inquadramento, ci si propone di offrire in primo luogo una panoramica dei principali problemi che caratterizzano le regole dell'informazione rispetto all'avvento di Internet per verificare, in seconda istanza, come sullo sfondo di una sostanziale stasi legislativa in materia, la giurisprudenza abbia fornito alcune risposte iniziali, in alcuni casi molto convincenti, in altri meno persuasive.

Esaminatone il merito, diverrà possibile comprendere quali criticità resistano tuttora e invochino una soluzione che, ove non passi per via legislativa, dovrà giocoforza riposare su un coraggioso slancio giurisprudenziale.

2. La disciplina penale della stampa, a sessant'anni dalla Costituzione

Quando nel 1948 la Costituzione proclamò per la prima volta in forma solenne, all'art. 21, la libertà di manifestazione del pensiero, il passo in avanti che la Repubblica stava allora compiendo costituiva una conquista molto più ampia di quanto la semplice sua veste formale potesse lasciare immaginare. Queste considerazioni valgono in particolare per quel che attiene alla libertà di stampa.

Infatti, se lo Statuto albertino, vigente fino ad allora,[6] si era limitato in proposito a dettare il principio secondo cui «la stampa sarà libera ma una legge ne reprime gli abusi» (art. 28), affidando, nei fatti, al legislatore un potere e una discrezionalità assai ampi nel limitare o comunque condizionare l'ambito di effettivo esercizio di tale libertà,[7] la Costituzione repubblicana sovverte questa impostazione. Non è un caso che la norma affidata all'art. 21[8] assomigli per certi aspetti più a una disposizione codicistica che a una vera e propria previsione costituzionale. La scelta dell'Assemblea costituente, infatti, fu nel senso di assicurare un margine di tutela il più ampio possibile

[5] É appena il caso di menzionare, a questo proposito, il disegno di legge S 1119 attualmente in fase di discussione in Parlamento, che sembra muovere in direzione opposta a quella auspicata. Si vv. i commenti di M. OROFINO, *Il disegno di legge S. 1119: alla ricerca di un nuovo bilanciamento tra la libertà di espressione e il diritto all'onore e alla reputazione,* in *Astrid rassegna*, n. 17, 13 ottobre 2014; C. MELZI D'ERIL - G.E. VIGEVANI, *Nella «nuova» diffamazione un arsenale pericoloso,* in *Il Sole 24 Ore*, 31 ottobre 2014, 41; ID., *Diffamazione: il legislatore che voleva troppo*, *www.medialaws.eu*, 10 novembre 2014; A. NAPOLITANO, *La responsabilità del direttore di testata giornalistica on-line: orientamenti giurisprudenziali e prospettive di riforma*, in *DIMT*, 2014, 84 ss.

[6] Per un commento, si v. G. *Arangio-Ruiz, Il diritto di stampa*, Modena, 1905.

[7] Tra i numerosi provvedimenti introdotti dal 1848 in poi, si ricordano la legge 26 marzo 1848, n. 695 (cosiddetto "Editto Albertino"), che per prima ha regolato la materia; la legge 26 febbraio 1852; la legge 28 giugno 1858; il decreto 28 aprile 1859; la legge 6 maggio 1877; la legge 22 novembre 1888; la legge 19 luglio 1894; la legge 28 giugno 1906; la legge 9 luglio 1908; la legge 7 luglio 1910; i decreti 31 dicembre 1925; la legge 31 dicembre 1925, n. 2307; il decreto 9 agosto 1943, n. 727; i decreti nn. 13 e 14 del 14 gennaio 1944.

[8] Si v. P. COSTANZO, *Stampa (libertà di)*, in *Dig. disc. pubbl.*, XIV, Torino, 1999, 525 ss.

alla libertà di manifestazione del pensiero (compresa, evidentemente, la libertà di stampa), alla luce degli esiti nefasti che l'epoca del fascismo aveva partorito in tale ambito, complice una cornice legislativa che, come detto, assicurava nei fatti al parlamento (e, in via mediata, all'esecutivo) il potere di restringere la garanzia della libera espressione. L'atipicità di questa disposizione, dunque, non è casuale, ma deriva dalle contingenze storiche che hanno contraddistinto il periodo immediatamente antecedente l'entrata in vigore della Costituzione. Con una norma coraggiosa, l'Assemblea costituente fissa alcuni capisaldi che, a ben vedere, riguardano perlopiù la libertà di stampa, quale specifica declinazione della manifestazione del pensiero.[9] Infatti, se il primo comma della disposizione sancisce la libertà di diffondere liberamente e con ogni mezzo il proprio pensiero, quelli successivi sono integralmente dedicati alla disciplina dell'esercizio della libertà di stampa. Alla luce delle ragioni storiche sottese a questa scelta, essa è dunque da salutare con favore.

Vengono infatti accordate diverse garanzie alla libertà di stampa: in particolare, il divieto di introdurre autorizzazioni o censure; la previsione di una riserva di legge rinforzata per contenuto e di una riserva di giurisdizione per la definizione dei casi in cui è possibile procedere al sequestro degli stampati.[10]

Già (poco) prima che la Costituzione fosse approvata, in realtà, erano state adottate disposizioni di garanzia, in relazione al sequestro degli stampati.[11]

É con questo impianto, dunque, che si è dovuta confrontare nel 1948 la legge n. 47, che ha introdotto una prima disciplina organica sulla stampa (non a caso è stata ribattezzata "legge stampa"), che stabilisce tra l'altro una serie di obblighi, munendole la violazione con sanzioni anche penali, e aggravanti di pena (come per esempio per l'ipotesi di diffamazione, reato-tipo commesso col mezzo della stampa).

È bene precisare sin d'ora che la legge stampa vincola il suo ambito di applicazione oggettivo, individuandolo nelle stampe e negli stampati, definiti come «tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici in qualsiasi modo destinate alla pubblicazione».[12]

---

[9] Per un'analisi anche in chiave storica, si v. soprattutto A. PACE - M. MANETTI, *Rapporti civili. La libertà di manifestazione del proprio pensiero. Art. 21 Costituzione*, in *Commentario della Costituzione Branca-Pizzorusso*, Bologna-Roma, 2006, spec. 432 ss. Per un quadro sull'attuale assetto costituzionale, specialmente con riferimento alla libertà di stampa, si v. invece C. MALAVENDA – C. MELZI D'ERIL - G.E. VIGEVANI, *Le regole dei giornalisti. Istruzioni per un mestiere pericoloso*, Bologna, 2012.

[10] Per alcuni riferimenti di matrice costituzionalistica, si vv. le risalenti ma straordinariamente attuali riflessioni di C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958; P. BARILE, Libertà di manifestazione del pensiero, Milano, 1975; ID., *Libertà di manifestazione del pensiero*, in *Enc. dir.*, XXIV, 1974, 424 ss.; A. LOIODICE, *Contributo allo studio sulla libertà di informazione*, Napoli, 1969. Si vv. anche A. PACE, *Stampa giornalismo radiotelevisione*, Padova 1983; P. COSTANZO, *Informazione nel diritto costituzionale*, in *Dig. disc. pubbl.*, VIII, Torino, 1993; C. CHIOLA, *Manifestazione del pensiero (libertà di)*, in *Enc. giur.* XIX, Roma, 1990; A. DI GIOVINE, *I confini della libertà di manifestazione del pensiero*, Milano, 1988; M. MANETTI, *La libertà di manifestazione del pensiero*, in R. NANIA - P. RIDOLa, *op. cit.* Sull'interpretazione della libertà di manifestazione del pensiero nella giurisprudenza costituzionale, si vv. M. LUCIANI, *La libertà di informazione nella giurisprudenza costituzionale italiana*, in *Pol. Dir.*, 1989, 605 ss.; A. PIZZORUSSO - R. ROMBOLI - A. RUGGERI - A. SAITTA - G. SILVESTRI, *Libertà di manifestazione del pensiero e giurisprudenza costituzionale*, Milano, 2005. Si v. anche V. ZENO ZENCOVICH, *La libertà di espressione. Media, mercato, potere nella società dell'informazione*, Bologna, 2004.

[11] Si v. il regio decreto legge 31 maggio 1946, n. 561.

[12] Così l'art. 1.

Questa disposizione sembrerebbe deporre un chiaro ostacolo all'applicazione, rispetto a tutto quanto non rientri nella nozione di stampa o stampato, delle disposizioni contenute nella legge stampa; o, almeno, ciò dovrebbe valere senz'altro con riguardo alle disposizioni di natura incriminatrice che essa racchiude.

Si tratta di un punto cruciale ai fini della comprensione della problematica dell'applicazione a Internet e, in generale, ai nuovi media delle norme in materia di stampa.[13]

Non sono mancati, infatti, alcuni interventi del legislatore che hanno indotto parte dei commentatori a ritenere che l'ambito di applicazione delle norme sulla stampa –beninteso, non solo quelle affidate alla l. 47/1948 ma, per esempio, anche quelle codicistiche- fosse stato esteso più in generale anche all'informazione *online.*

Senza entrare per ora nel merito di questi provvedimenti, si può dire che le diverse posizioni espresse da dottrina e giurisprudenza si sono così polarizzate verso due possibili soluzioni: da un lato, l'opzione di non considerare realizzata alcuna equiparazione tra stampa e telematica, e così ritenere applicabile la normativa vigente ai soli media tradizionali,[14] o –secondo una variante- comunque a quegli strumenti di informazione che pur tecnicamente differenti dalla stampa tradizionale, ne presentino alcuni elementi tipici al punto di essere a questi assimilabili;[15] dall'altro lato, invece, l'alternativa di giudicare perfezionata *ope legis* una vera e propria equiparazione, con tutte le correlate conseguenze sul piano dell'estensione delle norme penali a Internet, sia che si tratti di norme di favore che nel caso di norme di sfavore.[16]

Si tratta di una disputa che, nei termini in cui è stata normalmente presentata, non coglie pienamente il segno e non è suadente. Per quali motivi?

Il primo degli interventi registrati in materia risale al 2001, allorché con la legge n. 62 del 7 marzo, la cosiddetta "terza legge sull'editoria", fa la sua comparsa, all'art. 1, una definizione nuova, quella di "prodotto editoriale". Per prodotto editoriale 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».[17]

Le ragioni che hanno condotto ad ascrivere –erroneamente- a questo provvedimento l'estensione a Internet delle norme sulla stampa *online* divengono chiare guardando al successivo comma 3: laddove si prevede che al prodotto editoriale si applichi, per un verso, l'art. 2 della legge stampa, relativo alle indicazioni obbligatorie; e, per altro verso, quando si tratti di prodotto editoriale «diffuso al pubblico con periodicità regolare e contraddistinto da una testata», l'art. 5 della stessa, che prescrive un obbligo di registrazione.

---

[13] Per una prospettazione del problema, si v. V. ZENO ZENCOVICH, *La pretesa estensione alla telematica del regime della stampa*, in *Dir. inf.*, 1998, 15 ss.

[14] Tra le posizioni più importanti in questa direzione si ricordano V. ZENO ZENCOVICH, *op. ult. cit.*; P. COSTANZO, *Libertà di manifestazione del pensiero e «pubblicazione» in Internet*, in *Dir. inf.*, 1998, 372 ss.; R. CLARIZIA, *I giornali telematici*, in *AIDA*, 1998, 149 ss.; G. CORRIAS LUCENTE, *Il diritto penale dei mezzi di comunicazione di massa*, Padova, 2000.

[15] Si v. in tal senso I.P. CIMINO, *Obbligo di registrare la pubblicazione* on line *quale testata giornalistica*, in *Il Dir. ind.*, 2009, 267 ss.

[16] Tesi diffusa soprattutto (sebbene non esclusivamente) in giurisprudenza e specialmente prima dell'interpretazione autentica offerta dallo stesso legislatore. Si vv. Trib. Milano, 16 maggio 2002.

[17] Così dispone l'art. 1.

Sennonché è stato lo stesso legislatore a chiarire in modo inequivoco, attraverso due norme di interpretazione autentica, il significato da attribuirsi all'art. 1 della l. 62/2001. Tanto l'art. 31 della legge 1 marzo 2002, n. 39, quanto l'art. 7 del decreto legislativo n. 70 del 9 aprile 2003, infatti, chiariscono che il richiamato obbligo di registrazione previsto dalla legge stampa si applica soltanto al prodotto editoriale, e dunque alla testata anche telematica che intenda richiedere le provvidenze stabilite dalla l. 62/2001. Soltanto in questo caso le prescrizioni che la l. 62/2001 estende al prodotto editoriale si devono ritenere vincolanti.

A queste disposizioni, tuttavia, alcuni hanno impropriamente attribuito una pretesa equiparazione delle regole sulla stampa tradizionale ai nuovi media.[18] Nulla di tutto questo si ritrova, invece, nella l. 62/2001.[19]

Il fatto che si sia confidato su questo intervento normativo, di per sé circoscritto, per teorizzare una simile equiparazione rivela tuttavia un errore di impostazione che inficia ogni speculazione interpretativa. Non è infatti attraverso un'assimilazione legislativa *de plano* che è possibile realizzare con esiti appaganti un'operazione complessa come l'applicazione ai nuovi media delle disposizioni in materia di stampa: non lo è a ragione anche del fatto che su questo terreno si intersecano norme con rilevanza penale e garanzie costituzionali da raccordare necessariamente con i principi generali dell'ordinamento. Piuttosto, è una lettura delle disposizioni vigenti coerente con la *ratio* anche costituzionale loro sottesa a poter rivelare l'idoneità di una determinata previsione a vedere allargato il proprio campo di applicazione a Internet o meno. Una pretesa, in altri termini, di collegare automaticamente e quasi algebricamente un comparto normativo così complesso e variegato al mondo di Internet si scontrerebbe con le peculiarità che gli sono proprie, annullando nella maggior parte dei casi i motivi che si celano dietro una precisa scelta legislativa.[20]

Si deve così prendere atto che, rispetto ad alcuni aspetti (e solo rispetto a questi soltanto), può essere raggiunta la stessa conclusione (applicabilità della disciplina sulla stampa a Internet) ma seguendo percorsi diversi: e cioè non già ritenendo che le norme sull'informazione si applichino *ope legis* anche a Internet, ma per effetto di un'interpretazione che, individuata la *ratio* della disciplina vigente, ne ritenga meritevole l'applicazione anche ai fenomeni che prendono corpo in rete.

Due problematiche consentono di cogliere questa differenza di approccio in azione.

La prima riguarda l'applicabilità delle garanzie costituzionali, e in particolare del divieto di procedere a sequestro preventivo (al di fuori dei casi e dei modi previsti dalla

[18] Per una panoramica delle diverse opinioni sul punto, si v. I.P. CIMINO, *Le pubblicazioni telematiche ed i prodotti editoriali,* nota a Trib. Padova, ord. 1 ottobre 2009, in *Il dir. ind.,* 2010, 1, 75 ss.; di diverso avviso invece M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione*, Milano, 2009, 222 ss.

[19] Si v. V. ZENO ZENCOVICH, *I prodotti editoriali elettronici nella legge 7 marzo 2001, n. 62 e il preteso obbligo di registrazione,* in *Dir. inf.,* 2001, 154 ss.

[20] Questo approccio sembra trasparire in una lungimirante riflessione del Prof. Costanzo, addirittura antecedente all'introduzione della l. 62/2001, che pure nega la possibilità di estendere a Internet le garanzie costituzionali previste per la libertà di stampa, ma con argomento senz'altro ineccepibile: «Il modello costituzionale 'privilegiato' della stampa periodica […] se, da un lato, impedisce che un certo armamentario repressivo sia introdotto a suo danno e, più specificamente, in ragione dei suoi contenuti informativi o notiziali, dall'altro costituisce, proprio perché 'privilegiato', un paradigma inarrivabile, con gli ordinari strumenti d'interpretazione estensiva od analogica, per gli altri mezzi diffusivi dalla stampa». Si v. P. COSTANZO, *Libertà di manifestazione del pensiero,* cit., 375.

legge) in caso di utilizzo di Internet. Pacifico, infatti, è che l'Assemblea costituente, nel delineare un nucleo forte di tutela della libertà di stampa mediante l'art. 21 comma 3, non potesse che riferirsi, nell'individuare l'oggetto di questa garanzia, alla stampa tradizionale. Sorge allora l'interrogativo, dibattuto in dottrina ma apparentemente trascurato in giurisprudenza, in ordine all'applicabilità di questa tutela rafforzata a Internet.

La seconda problematica, invece, ha a che vedere con l'applicabilità non già delle garanzie costituzionali (e quindi di norme di favore), bensì di norme incriminatrici che il vigente quadro normativo ha stabilito in relazione a particolari tipologie di reato. Il punto può essere esaurientemente trattato considerando il caso della responsabilità per omesso controllo del direttore responsabile di un giornale, che l'art. 57 c.p. stabilisce nelle ipotesi di reati commessi col mezzo dalla stampa. Anche se in questo caso il problema si è rivelato di più facile soluzione, in virtù della natura penale delle norme in questione, e quindi dei principi generali che sanciscono il divieto di applicazione *in malam partem* delle fattispecie incriminatrici.

3. L'applicabilità a Internet delle norme penali di sfavore

Un primo ambito nel quale è possibile riscontrare il ruolo dei principi generali in materia penale rispetto all'esigenza di applicare a Internet le regole dell'informazione è rappresentato dalle norme incriminatrici che il legislatore ha introdotto al fine di reprimere ovvero aggravare le condotte poste in essere nell'espletamento di un'attività informativa. Si tratta tanto di disposizioni collocate nella legge stampa quanto di norme che si ritrovano a livello codicistico.

L'analisi della casistica che ha caratterizzato le varie disposizioni rivelerà come le soluzioni proposte dalla giurisprudenza abbiano determinato, a seconda dei casi, una maggiore o minore torsione dei principi costituzionali sottesi alla disciplina rilevante.

La prima e più interessante applicazione ha riguardato la norma affidata all'art. 57 c.p., che prevede in capo al direttore responsabile di un periodico una responsabilità per omesso controllo in ipotesi di reati commessi a mezzo stampa.[21] Si tratta di una disposizione assai controversa, che non ha mancato di provocare ampio e partecipato dibattito in campo dottrinale, configurando, ad avviso di molti e a dispetto della terminologia impiegata dal legislatore del codice, una vera e propria ipotesi di responsabilità oggettiva che entrerebbe in tensione con il principio di colpevolezza costituzionalmente tutelato dall'art. 27. Non è questa la sede opportuna per approfondire il punto; basti nondimeno osservare che si versa in campo delicato, e che la maggior parte della dottrina auspicherebbe l'abrogazione di una tale disposizione incriminatrice.

Venendo al cuore del problema, occorre considerare se una norma come quella di cui all'art. 57 c.p. possa trovare applicazione nel settore dell'informazione *online*, vale a dire nei confronti del direttore responsabile di una testata telematica.

Un primo, potenziale, indice nel senso della non applicabilità della fattispecie incriminatrice in questione si potrebbe, seppure indirettamente, ricavare dal fatto che,

[21] Così prevede l'art. 57 c.p.: «Salva la responsabilità dell'autore della pubblicazione e fuori dei casi di concorso, il direttore o il vice-direttore responsabile, il quale omette di esercitare sul contenuto del periodico da lui diretto il controllo necessario ad impedire che col mezzo della pubblicazione siano commessi reati, è punito, a titolo di colpa, se un reato è commesso, con la pena stabilita per tale reato, diminuita in misura non eccedente un terzo».

interpretando il combinato disposto tra la legge stampa, e segnatamente l'art. 2 e 3, e l'art. 1, comma 3. della l. 62/2001 (quest'ultimo come chiarito, nella sua portata, dall'art. 7 del d. lgs. 70/2003), la registrazione della testata *online* e l'indicazione del direttore responsabile sono obbligatorie solo in quanto ricorrano determinate condizioni (ossia quando la testata intenda ottenere le forme di finanziamento pubblico previste dalla stessa l. 62/2001). [22]

Il rilievo ha sicuramente un pregio, sebbene parziale: vero è che si potrebbe comunque argomentare nel senso dell'applicabilità dell'art. 57 c.p. ove il direttore responsabile sia effettivamente nominato, ma aderendo a questo indirizzo ci si scontrerebbe con l'illlogica allocazione di una responsabilità (penale!) fondata essenzialmente (ed esclusivamente) sulla circostanza che la testata intenda avvalersi o meno di provvidenze. Se la *ratio* sottesa all'art. 57 c.p., volendo semplificare, fosse quella di individuare "un colpevole a tutti i costi", prevedendo una responsabilità del direttore responsabile per omesso controllo, allora o tale responsabilità opera sempre e comunque, oppure non opera affatto, essendo del tutto irrazionale ancorarne l'esistenza alla scelta, fondata su considerazioni di ordine esclusivamente economico, di registrare o meno la testata.

Dato atto di queste criticità, bisogna confrontarsi con la tematica dell'azionabilità della norma *ex* art. 57 c.p. nei casi in cui il direttore responsabile sia stato effettivamente nominato. Assumendo che un reato sia commesso attraverso una pubblicazione telematica (per esempio, per effetto di un articolo dal contenuto diffamatorio *online*), al direttore responsabile della testata *online* può essere imputato il reato di omesso controllo?

La giurisprudenza di legittimità ha dato risposta negativa a questo interrogativo, con argomenti che appaiono del tutto convincenti, a far data dal 2010, data cui risale la prima storica sentenza in materia.[23]

Si deve infatti alla Cassazione il merito di aver fatto chiarezza sul punto,[24] in primo luogo evidenziando l'alterità della nozione di stampato (cui l'art. 57 si riferisce se non

---

[22] I.P. CIMINO, *op. ult. cit.*, 82, sembra opporsi a un'indiscriminata estensione della disciplina sulla stampa a Internet, rilevando come, se l'applicazione delle garanzie costituzionali contro il sequestro preventivo al web fosse disancorata dall'effettiva registrazione di una testata, si incorrerebbe nel paradosso per cui, mentre nel caso delle testate cartacee la tutela rafforzata opera solo in caso di registrazione, così non sarebbe per le testate *online*, laddove anche in assenza di registrazione sarebbe applicabile l'art. 21, comma 3, Cost.

Per quanto condivisibile la necessità di individuare un limite alla capacità espansiva del concetto di stampa, così come adoperato dalla Costituzione, questa affermazione non può non sfuggire alla censura per cui il Costituente, come si dirà meglio oltre, ha inteso tutelare in misura rafforzata la stampa non in quanto tale, ma in quanto *medium* della libera manifestazione del pensiero. Se così è, dunque, le garanzie che la Costituzione appresta dovrebbero intendersi riferite più genericamente agli strumenti che sono funzionali all'esercizio di questa libertà (e, con riguardo specifico alle testate, indipendentemente dalla loro registrazione, dalla quale dipende unicamente l'accesso alle provvidenze per l'editoria).

[23] Cass., sez. V, 1 ottobre 2010, n. 35511, in *Dir. inf.*, 2010, 895 ss., con nota di C. MELZI D'ERIL, Roma locuta: *la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line, *ivi*, 899 ss. Si vv. anche i commenti di A. PAPA, *La disciplina della libertà di stampa alla luce delle nuove tecnologie, ivi*, 2011, 477 ss. e A. BEVERE - V. ZENO ZENCOVICH, *La rete e il diritto sanzionatorio: una visione d'insieme, ivi,* 2011, 375 ss.; N. LUCCHI, *Internet, manifestazione del pensiero e responsabilità editoriale,* in *www.forumcostituzionale.it*, 7 aprile 2011.

[24] Su questo tema, prima della pronuncia della Cassazione, si era registrata più di un'incertezza. Ne è testimone la sentenza Trib. Firenze, 13 febbraio 2009, in *Dir. inf.*, 2009, 911 ss., commentata da C. MELZI D'ERIL - G.E. VIGEVANI, *La responsabilità del direttore del periodico telematico, tra facili equiparazioni*

letteralmente –parlando di "periodico"- almeno implicitamente) dal prodotto diffuso via Internet. Tale eterogeneità, che giustifica una differente considerazione del *medium*, diviene evidente poiché ad avviso del Supremo Collegio difettano, nel caso di Internet, gli elementi costitutivi della nozione di stampato. Vale a dire, ai sensi dell'art. 1 della legge stampa, la riproduzione tipografica e la destinazione alla pubblicazione presso il pubblico.

La Cassazione si è inoltre soffermata su altri due punti.

In primis, ha richiamato la disciplina degli Internet service provider, racchiusa nel d. lgs. 70/2003, che esonera il prestatore di servizi da un obbligo generale di sorveglianza e ne circoscrive la responsabilità alle ipotesi di mancata rimozione di contenuti illeciti appositamente segnalati. Ma, sottolinea la Cassazione, in tal caso non si tratta certo di una responsabilità per omesso controllo, come quella prevista dall'art. 57 c.p., bensì di una responsabilità per concorso nel fatto illecito. Così il ruolo del direttore della testata *online* viene in sostanza equiparato, nel regime di responsabilità, a quello dei moderatori di blog e forum.

Inoltre, la Cassazione non si è astenuta dal rimarcare l'inesigibilità tecnico-giuridica, nel caso di una testata telematica, di un controllo analogo a quello che l'art. 57 c.p. pretende dal direttore responsabile di un periodico. Ad avviso della Corte, infatti, l'interattività, vale a dire «la possibilità di interferire sui testi che si leggono e si utilizzano» che caratterizza la testata *online* renderebbe verosimilmente vano ogni controllo da parte del direttore responsabile[25].

Soltanto in chiusura i giudici di legittimità hanno dato spazio, seppur residuale, agli argomenti che più direttamente rispondono all'obiezione (fondata) del ricorrente sull'inapplicabilità dell'analogia *in malam parte.* Ha rilevato, infatti, la Corte che nonostante i vari progetti (già allora numerosi, ma inappaganti) di riforma della materia, l'estensione della disciplina sulla stampa a Internet è estranea ai propositi della l.

---

e specificità di Internet, *ivi*, 2010, 91 ss. Nella fattispecie, il Tribunale aveva ritenuto addebitare il reato di diffamazione a mezzo stampa al direttore responsabile di una testata telematica ai sensi dell'art. 57 c.p., argomentando sulla base dell'equiparazione tra stampati e giornali *online*. Questa sentenza, al pari di altre pronunce che hanno sposato la pretesa assimilazione di stampa e web, mostra in modo evidente le criticità connesse a un approccio che, sostanzialmente, fa dipendere dalla mera interpretazione letterale della l. 62/2001 l'applicazione delle fattispecie incriminatrici previste per la stampa a Internet.

[25] Non è inutile richiamare quanto ha osservato in proposito P. COSTANZO, *La «stampa» telematica nell'ordinamento italiano*, in *www.costituzionalismo.it*, 2011/2. Il Prof. Costanzo, in particolare, ha espresso alcune riserve rispetto all'opzione di ricomprendere il direttore della testata telematica, così come degli autori di un blog, nell'ambito del regime di irresponsabilità che opera per i prestatori di servizi Internet. Osserva l'Autore: «le modalità di pubblicazione proprie di internet condurrebbero a far presumere che tutti questi soggetti non siano e/o non possano essere al corrente dei contenuti in tal modo diffusi […] Derivandone, però, nell'ipotesi contraria, una responsabilità a titolo comunque differente da quella del direttore di un periodico a stampa, fondata, cioè, sul concorso doloso nel reato e non sull'art. 57 c.p.». Tuttavia, rileva il Prof. Costanzo, «non dovrebbero residuare dubbi sul fatto che, per qualsiasi pubblicazione in internet, debba, innanzi tutto, rispondere colui che ne risulta (se risulta) l'autore materiale (*ex* art. 595, comma 3, c.p.), ma anche chi risulti *dominus* del relativo spazio *web*, vuoi a titolo di concorso nella commissione del fatto illecito, o, come tipicamente avviene nel caso di un sito da lui stesso moderato, a titolo di omissione per non aver impedito il fatto pur essendone a conoscenza. *In altri termini, alla perfetta padronanza del sito non può non corrispondere una responsabilità parimenti totale*». Dello stesso Autore, si segnalano poi sul tema anche *Il blog tra vocazione libertaria della Rete e limiti costituzionali della manifestazione del pensiero,* in *Inf. e dir.,* 2008, 57 ss. e *La stampa telematica (tuttora) fra ambiguità legislative e dissensi giurisprudenziali,* in *Giur. cost.,* 2010, 5239 ss.

62/2001, sicché nessuna ipotesi di responsabilità per omesso controllo del direttore della testata *online* era ed è tuttora prevista dall'ordinamento.

Salutata con favore [26] la posizione della giurisprudenza di legittimità ormai consolidata sul punto,[27] si deve ora concentrare l'attenzione su un problema diverso, la cui soluzione, pur condivisibile, è stata raggiunta con maggior fatica dai giudici della Cassazione, eliminando il rischio di torsioni sempre frequenti specie nella giurisprudenza di merito.

Una dimostrazione di come i tribunali italiani, in alcune circostanze, si siano tristemente distinti nella mancanza di un'adeguata sensibilità nell'affrontare le problematiche giuridiche derivanti dal nuovo scenario tecnologico è data dal caso "Ruta".[28]

È servita infatti nuovamente una pronuncia dei giudici di legittimità affinché fosse sconfessato un indirizzo interpretativo che aveva fatto breccia sia nel Tribunale di Modica[29] sia nella Corte d'appello di Catania[30] e che definire inverosimile è atto di cortesia.

Il tema, stavolta, è quello dell'applicabilità della fattispecie incriminatrice di cui all'art. 15 della legge stampa nei confronti dell'autore di un blog. Il quale esercitava sì un'attività informativa, ma come privato (*freelance*) che di fatto pubblicava sul proprio sito Internet un giornale di informazione. Un semplice blogger, insomma. Il motivo dell'imputazione era da ricondursi al mancato adempimento dell'obbligo di registrazione prescritto dall'art. 5 della legge stampa.

Al centro della vicenda, dunque, si poneva ancora una volta il tema dell'assimilabilità di un sito Internet, strutturato nella forma di un blog, allo stampato. La risposta a tale interrogativo avrebbe permesso di dirimere l'ulteriore quesito: vale a dire se il blog fosse obbligato alla registrazione e se il suo autore fosse penalmente perseguibile per il caso di mancato adempimento.

La soluzione prospettata della Corte di cassazione, fortunatamente, si è rivelata ancora una volta ragionevole e contraria a ogni possibile deriva nel senso di un'iper-responsabilizzazione, così rimediando alle pronunce di merito, che avevano all'opposto accolto posizioni destinate a scatenare conseguenze assai difficilmente controllabili.

Il ragionamento dei giudici di legittimità, molto lineare, ha preso le mosse anche in questo caso dalla considerazione delle peculiarità proprie di Internet e dello stampato, per concludere –così come la Corte aveva fatto già nel 2010, nel caso che si è poc'anzi descritto- nel senso dell'incompatibilità del giornale telematico con i requisiti che la legge stampa prevede alla base della nozione di stampato.

---

[26] Sul punto si v. anche G. GARDINI, *Le regole dell'informazione: Dal cartaceo al bit,* Torino, 2014, 285.

[27] Oltre alla già menzionata sentenza "Brambilla", si deve ricordare anche Cass., sez. V, 29 novembre 2011, n. 44126, in *Dir. inf.,* 2011, 795 ss., con nota di G.E. VIGEVANI, *La «sentenza figlia» sul direttore del giornale telematico, ivi,* 798 ss. e G. CORRIAS LUCENTE, *Al Direttore Responsabile di un periodico on line non si applica il reato previsto dall'art. 57 del codice penale,* in *Dir. inf.,* 2012, 82 ss.

[28] Cass., sez. III, 10 maggio 2012, n. 23230, in *Dir. inf.,* 2012, 1118, con nota di P. DI FABIO, *Blog, giornalisti on line e «obblighi facoltativi» di registrazione delle testate telematiche: tra confusione del legislatore e pericoli per la libera espressione del pensiero su Internet, ivi,* 1120 ss. Si v. anche il commento di G. CORRIAS LUCENTE, *I titolari di blog o di testate telematiche non rispondono del reato di stampa clandestina se non rispettano gli obblighi di registrazione,* in *www.medialaws.eu*, 9 ottobre 2012.

[29] Trib. Modica, 8 maggio 2008, in *Dir. inf.,* 2008, 815 ss.

[30] App. Catania, 2 maggio 2011.

La Cassazione ribadisce poi che nessuna estensione della nozione di stampato si è perfezionata con la l. 62/2001, che anzi rafforza l'assunto per cui la registrazione del giornale è obbligatoria solo per ragioni amministrative.

La conclusione della Corte è così nel senso che nessuna norma incriminatrice, nemmeno l'art. 16 della legge stampa, può applicarsi al giornale *online* in relazione al reato di stampa clandestina: e ciò perché nessun obbligo di registrazione grava in capo al proprietario di un sito Internet.

A fronte di una giurisprudenza di legittimità che è sembrata sgomberare il campo da una pericolosa deriva verso l'applicazione indiscriminata e disinvolta di fattispecie incriminatrici pensate dal legislatore per la stampa tradizionale, bisogna nondimeno registrare alcuni arresti da parte delle corti di merito, che sono parse aderire a fasi alterne ai principi enunciati dalla Cassazione.

Ne è riprova uno dei casi più recenti, una decisione del GUP del Tribunale di Varese che ha condannato l'autrice di un blog per il reato di diffamazione in relazione a commenti pubblicati sul sito da terzi.[31] In particolare, il giudice ha ritenuto integrata la fattispecie di diffamazione aggravata ai sensi del comma 3 dell'art. 595 c.p. (in relazione al mezzo di pubblicità utilizzato), pur escludendo l'applicabilità dell'art. 13 legge stampa (prevista per le ipotesi di diffamazione a mezzo stampa).

Questa pronuncia sembra muoversi in controtendenza sia rispetto a quanto affermato dalla Cassazione sul tema della responsabilità del direttore della testata *online* (anche se, come si dirà, il giudice ha aggirato il punto) sia in relazione alla configurabilità nella fattispecie di un prodotto equiparabile allo stampato.

La costruzione argomentativa del Tribunale di Varese contraddice frontalmente la tesi della eterogeneità fra blog e stampato mentre elude indirettamente le conquiste giurisprudenziali sulla figura del direttore responsabile.

Smentendo, infatti, l'ampia casistica formatasi al riguardo, il giudice non sembra intravedere nell'argomento che si richiama alla nozione di stampato contenuta nella l. 47/1948 nulla più di una semplice interpretazione letterale. A dispetto di questo dato testuale, infatti, la nozione di stampa sottesa alle intenzioni del legislatore andrebbe ben al di là della semplice riproduzione tipografica, estendendosi anche a una nuova forma di editoria, quella di Internet, del tutto identica. Così, secondo il GUP, non si tratterebbe di rileggere l'art. 1 della legge stampa, ma semplicemente di una «sopravvenienza coerente […] con un concetto di stampa idoneo *ab origine* a ricomprendere la sopravvenienza dei quotidiani o periodici [...] su Internet».

Secondo il Tribunale, è pertanto compito dell'interprete ricondurre alla nozione di stampa un sito Internet sulla base delle caratteristiche «intrinseche e fenomeniche». Il ragionamento del giudice sta per cadere in contraddizione quando giunge, riparatore, un salto logico: anche se il blog in questione non presenta le caratteristiche di informazione ascrivibili alla stampa, esso rappresenta «la base per la costruzione di un gruppo settoriale di interesse, composto da scrittori esordienti, o aspiranti tali, mediante la discussione di temi comuni».

Così, il giudice giunge a ritenere applicabile nella fattispecie la responsabilità dell'autrice del blog per il reato di diffamazione, aggravato non già *ex* art. 13 legge

[31] Trib. Varese, 8 aprile 2013, in *Dir. inf.*, 2013, 531 ss. con nota di G. CORRIAS LUCENTE, *ivi*, 536 ss. Si v. anche il commento di S. ROSSETTI, *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 *www.penalecontemporaneo.it*, 11 giugno 2013.

stampa (giacché lo stesso Tribunale riconosce che, almeno formalmente, stampa non è), bensì *ex* art. 595, comma 3, e cioè in ragione del mezzo di pubblicità utilizzato. Si tratta quindi di una responsabilità che al proprietario del sito Internet viene imputata direttamente, seppure in relazione a contenuti pubblicati da terzi.

In questo modo il Tribunale di Varese elude anche l'ulteriore argomento fondato sull'irresponsabilità del direttore di un giornale *online.* Quella attribuita all'autrice del blog, secondo il giudice, non è una responsabilità che deriva dall'art. 57 c.p., ma piuttosto da una posizione di garanzia di cui il proprietario del sito Internet si ritiene titolare, essendogli ascritto *de facto* un obbligo giuridico di impedire l'evento. Ad avviso del Tribunale, infatti, «la disponibilità dell'amministrazione del sito Internet rende l'imputata responsabile di tutti i contenuti di esso accessibili dalla Rete, sia quelli inseriti da lei stessa, sia quelli inseriti da utenti: è indifferente sotto questo profilo sia l'esistenza di una forma di filtro […] sia l'inesistenza di filtri». Così ragionando, il giudice ha evitato di scontrarsi con la giurisprudenza di legittimità formatasi in relazione all'art. 57 c.p., i cui argomenti, come non si è mancato di evidenziare *supra*, non riposavano esclusivamente sul conforto letterale della nozione di "stampato" *ex* art. 1 legge stampa, ma si allargavano all'incompatibilità di un controllo come quello esigibile dal direttore della testata cartacea rispetto a un sito Internet. Inoltre, il Tribunale di Varese consegna una conclusione che appare *prima facie* in frontale contrasto con i principi racchiusi nel d. lgs. 70/2003 sulla responsabilità del prestatore di servizi, almeno nella misura in cui a essere interessati siano contenuti non già dalla stessa autrice pubblicati ma inseriti da terzi.

Si è così assistito a una deviazione alquanto pericolosa, che sarebbe auspicabile vedere presto sovvertita se la pronunzia –consegnata all'esito di un giudizio abbreviato- sarà appellata.

Il caso non è isolato stando alla cronaca giudiziaria, che riporta di alcune condanne nei confronti di autori di blog nei quali i tribunali avrebbero fatto specificamente applicazione dell'aggravante di cui all'art. 13 della l. 47/1948, relativa alle ipotesi di diffamazione commessa a mezzo stampa. [32]A questo proposito la rilevanza dei casi non è legata tanto alla configurazione di una responsabilità per diffamazione in capo al blogger (pacifica, ove questi sia l'autore del messaggio offensivo per la reputazione altrui), quanto piuttosto al venire in gioco della aggravante prevista dalla legge stampa, la cui applicazione presuppone l'equiparazione tra il sito Internet e lo stampato.

Anche in questo caso, vi è l'auspicio che queste deviazioni dall'indirizzo marcato dalla Corte di cassazione mediante le pronunce che si sono illustrate possano trovare rimedio nei successivi gradi di giudizio, alla luce di una più meditata ponderazione delle peculiarità che contraddistinguono Internet e ne fanno qualcosa di eterogeneo rispetto al concetto di stampato cui si riferisce la legge stampa.

Non sono però mancate anche applicazioni virtuose, come quella di cui si è reso recentemente artefice il Tribunale di Lecco, seppure nel contesto di una causa civile.[33]

Una pronuncia che ha interessato segnatamente la posizione dell'autore di un blog, cui gli attori in giudizio chiedevano il risarcimento dei danni causati dalla pubblicazione

[32] Così almeno riporta l'Avv. Fulvio Sarzana commentando una pronuncia (non pubblicata) del Tribunale di Roma, giudice Terranova, che avrebbe applicato nei confronti del proprietario di un blog la circostanza aggravante del reato di diffamazione *ex* art. 13 legge stampa. Si v. F. SARZANA, *Internet e diffamazione: assolti i giornalisti, condannato il blogger,* in *Il Fatto Quotidiano,* 17 febbraio 2014.

[33] Trib. Lecco, sez. II civile, 3 ottobre 2014.

di commenti diffamatori da parte di terzi, evocando –a fondamento della responsabilità del convenuto- la norma affidata all'art. 57 c.p., che prevede –come si è visto- la fattispecie di omesso controllo in capo al direttore responsabile di un periodico in caso di reati commessi con il mezzo della stampa.

Si è trattato di una pronuncia tutt'altro che scontata, dal momento che a essere dedotti in giudizio non erano i profili di responsabilità penale dell'autore del blog, bensì quelli di natura civile. Risulta nondimeno apprezzabile l'approdo cui è pervenuto il giudice, che facendo tesoro degli insegnamenti della Cassazione penale ha escluso la possibilità di collocare l'art. 57 c.p. anche a fondamento di una responsabilità civile del proprietario di un blog.

Non è inutile peraltro evidenziare come lo stesso Tribunale di Lecco, oltre a richiamare i precedenti rilevanti della giurisprudenza di legittimità, si sia premurato di precisare (argomentando così in modo radicalmente opposto rispetto al GUP del Tribunale di Varese) come le norme in materia di stampa e quelle sul direttore responsabile sarebbero del tutto inaccostabili al fenomeno dei blog, così offrendo una chiave di lettura non meramente adesiva rispetto ai principi enunciati dalla Cassazione penale.

Dovendo tracciare un bilancio sull'applicazione a Internet delle fattispecie incriminatrici, e più in generale delle norme di sfavore stabilite in materia di stampa, si deve constatare l'apprezzabile opera chiarificatrice della giurisprudenza di legittimità. La quale non si è appagata di un generico richiamo (argomento senz'altro più sbrigativo e immediato) ai principi dell'ordinamento penale, e in particolare al divieto di analogia *in malam partem*; ma che piuttosto ha seguito una strada che, a fronte di una considerazione pressoché sacrale della l. 62/2001 diffusa in certi commenti[34], ha chiaramente valorizzato l'alterità della stampa tradizionale rispetto ai nuovi mezzi di informazione, rendendo così vana ogni discussione sulla possibilità di ricomprenderle nell'ambito di applicazione di fattispecie incriminatrici "antiche".

Un approccio, quest'ultimo, coerente con l'esigenza che si è affermata in premessa di un percorso che non addivenga a qualificare le norme sulla stampa come rilevanti o meno solo in ossequio a una pretesa equiparazione *de plano*, invero insussistente, che avrebbe potuto trovare riscontro nella l. 62/2001; ma che, all'opposto, muova dalla *ratio* delle norme che il legislatore ha stabilito per derivarne un'applicazione rispettosa non solo, evidentemente, dei principi dell'ordinamento penale, ma anche della dimensione costituzionale che è inestricabilmente connessa ai nuovi mezzi dell'informazione.

4. La (non) applicabilità a Internet delle norme di favore

Un'esigenza analoga si presenta anche in relazione a un problema opposto a quello finora esaminato, vale a dire la possibilità di applicare a Internet le norme di favore che il legislatore ha previsto per la stampa tradizionale.

Sarebbe ancora una volta semplicistico rispondere a questo interrogativo facendo affidamento sul mero argomento letterale della presunta estensione a Internet della nozione di stampato. Anzi, tale approccio risulterebbe doppiamente inappagante: non

[34] Argomento che si è dovuto confrontare anche con l'obiezione secondo cui non di analogia ma di mera estensione si tratterebbe, come tale non confliggente con il divieto di applicazione di norme sfavorevoli, perché Internet sarebbe semplicemente annoverato nell'ambito oggettivo cui le previsioni della legge stampa si riferiscono.

solo perché appiattirebbe l'analisi a un'interpretazione testuale, ma perché in questa sede –discutendo di norme di favore- non osterebbero nemmeno i principi generali del diritto penale a una lettura che estenda il campo d'azione delle garanzie.

Il terreno d'indagine, in particolare, è quello delle garanzie costituzionali in materia di stampa, previste all'art. 21 Cost. [35]

In quest'ambito, va detto sin da subito, è mancato finora nella giurisprudenza di legittimità uno slancio coraggioso che avrebbe consentito di allargare a Internet il campo di applicazione delle garanzie costituzionali. Il timore, probabilmente, è che così argomentando si sarebbe creata una zona franca nella quale, esclusa la possibilità di adoperare gli strumenti sanzionatori previsti per la stampa (ma, verrebbe da obiettare, affatto quella di altri e più conferenti strumenti), se ne sarebbero nondimeno ritenute applicabili le guarentigie, con possibile detrimento per i diritti delle persone interessate.[36]

Il tema rivela in tutta la sua pienezza l'importanza di una interpretazione che non sia esclusivamente calata sul dato letterale, ma che percorra l'evoluzione tecnologica alla luce delle intenzioni del legislatore in una prospettiva costituzionalmente orientata.

Il dibattito si concentra, su questo versante, specificamente sull'art. 21, comma 3, Cost., norma che stabilisce –alla stregua di una previsione codicistica- una tutela rafforzata in favore della stampa, munendo il sequestro preventivo dello stampato della duplice garanzia della riserva di legge e di giurisdizione.

Il sequestro preventivo, infatti, è ammesso soltanto nei casi per i quali la legge stampa lo autorizzi o nel caso di violazione delle norme prescritte dalla legge stampa per l'indicazione dei responsabili. Inoltre, è consentito soltanto per atto motivato dell'autorità giudiziaria.

La domanda che sorge spontanea è se questo compendio di garanzie possa trovare applicazione anche quando si tratti di un sito Internet.

Per rispondere correttamente a questo interrogativo sarebbe del tutto inappropriato evocare la mancata estensione a Internet della disciplina prevista dalla legge stampa, peraltro ormai pacifica. Anzi, sia che si opini in un senso sia che si sposi l'orientamento contrario, il richiamo a questo tema rischia di riuscire fuorviante.

Va premesso che si versa in un terreno in cui a un'operazione analogica non ostano certamente, come detto, i principi dell'ordinamento penale. Bene ha fatto, a questo riguardo, un Autore a ricordare che non vi è alcuna soluzione "obbligata", al contrario di quanto è accaduto rispetto all'applicazione delle disposizioni incriminatrici.[37] Ciò chiarito, il punto merita forse un'analisi più inclinata sul versante costituzionale che su quello strettamente penalistico: occorre comprendere, in altri termini, se l'ambito della tutela rafforzata possa dilatarsi fino a comprendere Internet e i nuovi media.

Solo in tempi recentissimi si è assistito a un primo passo che potrebbe condurre, in futuro, a quello slancio coraggioso che si è invocato in apertura di paragrafo. Infatti, la prima sezione della Corte di cassazione ha deferito alle sezioni unite, con ordinanza del

[35] Si v. ancora G. GARDINI, *op. cit.*, p. 286.

[36] In tal senso, fra tutti si v. S. SEMINARA, *Internet (diritto penale)*, in *Enc. Dir. Annali*, VII, Milano, 2014.

[37] Mi riferisco a C. MELZI D'ERIL, *Il sequestro di siti on-line: una proposta di applicazione analogica dell'art. 21 Cost. "a dispetto" della giurisprudenza,* in *Dir. inf.*, 2014, 153 ss., spec. 162.

30 ottobre scorso,[38] la questione relativa all'applicabilità del sequestro preventivo a un sito Internet. Finora, infatti, la giurisprudenza, di merito e di legittimità, aveva alternativamente ignorato il problema, semplicemente evitando di porselo, o ritenuto inapplicabili le garanzie racchiuse nell'art. 21, comma 3, in favore di Internet.

Sul punto, il rinvio sollevato dalla prima sezione investe due profili: da un lato, la possibilità da un punto di vista tecnico di procedere al sequestro preventivo di un sito Internet, stante la lacunosa formulazione dell'art. 321 c.p.p. e il particolare meccanismo (un ordine di oscuramento rivolto a un terzo soggetto) su cui si fonda la sua concreta imposizione;[39] dall'altro lato il problema che più rileva ai fini di questa indagine, vale a dire la possibilità di dilatare la tutela rafforzata della libertà di stampa fino a comprendervi Internet.

Bisogna dare atto che la giurisprudenza aveva finora espresso un orientamento pressoché granitico, con occasionali aperture (soprattutto da parte dei giudici di merito[40]) fondate però solo su affermazioni incidentali, senza mai prendere posizione apertamente a favore dell'applicazione a Internet del divieto di sequestro preventivo. Stupisce, allora, ma è certamente da salutare con favore, l'iniziativa della prima sezione, i cui esiti si potranno evidentemente apprezzare soltanto nei prossimi mesi.

Se non si tratta (ancora, auspicabilmente) di un punto di non ritorno, va però sottolineato come ci si trovi di fronte a un momento di rottura rispetto alla consolidata elaborazione giurisprudenziale, che sembra poterne mettere in discussione la portata fino a ora granitica.

E, infatti, i margini per un'interpretazione contraria a quella che limita alla stampa tradizionale la tutela rafforzata dell'art. 21 Cost. sono risultati da subito piuttosto ridotti.

La Corte di cassazione ha infatti inanellato una serie di pronunce che hanno costantemente negato l'accesso a detta tutela per i siti Internet. Diverse sono state le

[38] Si v. Cass., sez. I, ord. 30 ottobre 2014, n. 45053. Si v. anche il commento di F. MAZARA GRIMANI, *La Prima Sezione della Cassazione rinvia alle Sezioni Unite la decisione sulla possibilità di sequestrare pagine web di testate giornalistiche in caso di articoli diffamatori*, in *www.medialaws.eu*, 5 novembre 2014.

[39] Su questi aspetti si v. ancora C. MELZI D'ERIL, *op. ult. cit.*, 156 ss.

[40] Proprio dalla giurisprudenza di merito è utile trarre alcune decisioni che hanno restituito parziali aperture, cui i giudici di legittimità sono però parsi tendenzialmente indifferenti. Fra tutte, si segnala anzitutto Trib. Padova, ord. caut. 1 ottobre 2009, in *Il dir. ind.*, 2010, 73 ss., a commento della quale I.P. CIMINO, *op. cit.* Si tratta di una pronuncia resa nell'ambito di un procedimento cautelare (civile) nel quale era stato emesso in via d'urgenza un decreto che disponeva la rimozione di alcuni contenuti da due testate telematiche (peraltro registrate). Il Tribunale di Padova, argomentando nel senso dell'avvenuta equiparazione tra stampa e telematica per effetto della l. 62/2001 (argomento che, secondo l'avviso di chi scrive, non è in realtà conferente alla soluzione del problema), ha ritenuto che il divieto di sequestro previsto all'art. 21 Cost. si estendesse anche ai siti Internet considerati "stampa" e, giudicando che il provvedimento d'urgenza concesso si risolvesse in un sequestro in via cautelare, ne ha disposta la revoca. Una seconda apertura, seppure foriera di una *ratio* non del tutto condivisibile, si è accompagnata a una pronuncia del Trib. Milano, sez. Riesame, 25 giugno 2011, n. 157, che ha invece espresso un indirizzo per così dire "mediano" ma non condivisibile, secondo il quale l'applicabilità delle garanzie contro il sequestro preventivo sarebbe condizionata dall'adempimento al (preteso) obbligo di registrazione del periodico. Si tratta di una posizione che, come già è stato posto in evidenza, non può godere di approvazione, essendo la registrazione mera facoltà della testata il cui mancato compimento non è munito di alcuna sanzione. Su quest'ultima pronuncia, si v. il commento di J. ANTONELLI DUDAN – C. MELZI D'ERIL, *In assenza dei presupposti previsti dalla norma inapplicabili le garanzie sulla non sequestrabilità*, in *Guida dir.*, 2010, n. 44, 24 ss. Sul tema, più diffusamente ancora G. GARDINI, *op. cit.*, 288 s.

sollecitazioni che la Cassazione ha ricevuto in questo senso.[41] Vale la pena ricordare, per esempio, che solo nel 2011 si sono registrate due sentenze in cui il Supremo Collegio non ha dato peso all'argomento, apparentemente indifferente alla possibilità di impiego dello strumento cautelare anche su Internet,[42] e a tratti forse inconsapevole addirittura del portato dell'art. 21.[43] Ancor prima, nel 2009, la Suprema Corte aveva però radicalmente escluso la rilevanza, tra gli altri, di forum e blog ospitati da un sito Internet: i quali costituiscono sì espressione della libera manifestazione del pensiero ma ad avviso dei giudici di legittimità non rientrerebbero nel più ristretto concetto di "stampa", cui solo l'art. 21 Cost. si riferisce, peraltro secondo un'accezione tecnica, tale da escludere una generica rilevanza di tutti i mezzi di informazione.[44]

Il tema è tornato d'attualità nella giurisprudenza della Cassazione più recentemente. Oltre alla già ricordata ordinanza che ha rimesso la questione alle sezioni unite, si devono menzionare due pronunce, entrambe del marzo scorso,[45] che non hanno però mutato l'orientamento già delineatosi nelle precedenti prese di posizione. Così la Corte è tornata a ribadire, riferendosi direttamente al proprio precedente del 2009, la diversità tra stampa e Internet, che sarebbe confermata da quelle stesse pronunce che hanno escluso l'applicabilità a Internet delle fattispecie incriminatrici previste per la stampa.

Questo genere di aporie è il frutto di un approccio ancora troppo rigidamente legato all'alternativa fra equiparabilità e non equiparabilità del sito Internet allo stampato. Ecco perché questa prospettiva di indagine, almeno nella misura in cui si versa nel terreno di norme di favore, può risultare inappagante.

Così facendo, congelando e pietrificando l'interpretazione delle norme (si badi: non penali, ma costituzionali!) all'epoca in cui esse sono state introdotte, si finisce per rovesciare quelle che verosimilmente erano le intenzioni dello stesso legislatore costituente. Una simile difesa avrebbe forse ragione di porsi nell'ambito delle disposizioni di sfavore, laddove la pretesa di applicare regole antiche a un *medium* nuovo potrebbe risolversi in un contrasto con il divieto di applicazione analogica. Ma ciò non dovrebbe accadere nel campo delle norme di garanzia, dove anzi l'avanzare delle tecnologie rende necessaria un'interpretazione in senso evolutivo del significato

[41] Cass., sez. III, 24 ottobre 2007, n. 39354. Sul punto si v. anche M. FUMO, *La diffamazione mediatica*, Torino, 2012, 66 ss. Si tratta di una presa di posizione interessante perché la Corte ha esplicitamente ammesso l'equiparabilità dei messaggi veicolati da un sito Internet agli stampati, legittimando però la misura del sequestro data la natura oscena delle pubblicazioni interessate, che in quanto tali sono espressamente escluse dalla tutela costituzionale dall'art. 21, comma 6, Cost.

[42] Cass., sez. V, 10 gennaio 2011, n. 7155, in *Guida al diritto*, 2011, n. 13, 62 ss., con nota di C. MELZI D'ERIL, *La Cassazione reintroduce una misura cautelare esclusa con il passaggio dal fascismo alla libertà*, *ivi*, 64 ss.; si v. anche ID., *La complessa individuazione dei limiti alla manifestazione del pensiero in Internet*, in *Dir. inf.*, 2011, 571 ss., spec. 578.

[43] Cass., sez. V, 14 dicembre 2011, n. 46504. Si v. in proposito il commento di C. MELZI D'ERIL - G.E. VIGEVANI, *Sul sequestro di pagine web: Vladimiro ed Estragone attendono ancora*, in *www.medialaws.eu*, 28 dicembre 2011. Nessun riferimento all'art. 21, comma 3, *tamquam non esset*, incredibilmente, anche in Cass., sez. V, 4 giugno 2012, n. 21489.

[44] Cass. pen., sez. V, 10 marzo 2009, n. 10535, in *Dir. inf.*, 2009, 508 ss., con nota di L. BACCHINI, *Il sequestro di un forum on-line: l'applicazione della legge sulla stampa tutelerebbe la libertà di manifestazione del pensiero in Internet?*, *ivi*, 512 ss.

[45] Cass., sez. V, 5 marzo 2014, n. 10594; Cass., sez. V, 12 marzo 2014, n. 11895. Si vv. i commenti di G. CORRIAS LUCENTE, *La Cassazione interviene ancora sull'equiparazione fra stampa e giornali telematici*, in *www.medialaws.eu*, 20 maggio 2014; C. MELZI D'ERIL, *La Cassazione esclude l'estensione ai siti Internet delle garanzie costituzionali previste per il sequestro di stampati*, www.penalecontemporaneo.it, 5 marzo 2014 e ID., *Il sequestro di siti-online*, cit., 153 ss.

delle medesime norme costituzionali, a pena di disperdere il senso della tutela che il Costituente intese garantire.

Chi scrive sente quindi di aderire all'opinione per cui l'art. 21, specie al comma 3, è una norma che disciplina un mezzo per regolare in realtà una libertà,[46] perché quello specifico mezzo era verosimilmente l'unico, all'epoca, attraverso il quale potesse concretarsi l'esercizio della libera manifestazione del pensiero. Allora questa norma, che oggi appare connotata da una veste codicistica, distinguendosi in ciò dall'ecosistema costituzionale in cui si inserisce, non traduce una selezione da parte del Costituente di una fra le diverse possibili forme di esercizio della libera manifestazione del pensiero. Al contrario, il Costituente si è occupato della stampa non perché mezzo privilegiato, ma perché unico *medium* ai tempi della libera espressione.[47] Ciò che oggi appare una norma codicistica, al punto da indurre taluni a opinare nel senso dell'eccezionalità della disposizione (tesi senz'altro legittima, ma inusuale per una norma di rango costituzionale), non era altro che lo strumento mediante il quale l'Assemblea costituente volle tutelare in modo rafforzato la libertà di manifestazione del pensiero.

Chi maggiormente ha dedicato attenzione a questo tema,[48] cogliendo lo spunto offerto da una pronuncia di merito,[49] ha indicato una possibile via di soluzione nel considerare le garanzie *ex* art. 21, comma 3 applicabili soltanto a determinate condizioni. E cioè quando sia identificato o identificabile il soggetto che è autore di un messaggio pubblicato via Internet o che, comunque, pur non essendone autore, ne risponda. La norma affidata all'art. 21, infatti, allude -a ben vedere- al diritto che ciascuno vanta a manifestare il "proprio" pensiero.

Si tratta di una proposta che ritengo senza dubbio interessante, ma che collegando al tema dell'anonimato l'applicazione delle tutele previste per la stampa, finisce per modulare l'accesso alla tutela rafforzata dell'art. 21 Cost. sulla base di condizioni che poco hanno a che vedere, forse, con il contenuto essenziale della libertà tutelata. Vero è che la stessa normativa racchiusa nella legge stampa considera obbligatorie precise indicazioni relative agli stampati, così come è vero che non si tratta certamente di mere incombenze di natura amministrativa, risultando funzionali, tra l'altro, all'individuazione di un soggetto responsabile.

Non sono tuttavia convinto che l'accesso alle garanzie previste dall'art. 21, comma 3, possa essere condizionato solo da fattori come l'adempimento di questi obblighi, e

---

[46] Si v. C. MELZI D'ERIL, *Il sequestro di siti on-line*, cit., 165.

[47] Presta indirettamente sostegno a questa visione il provocatorio ma geniale pamphlet di V. ZENO ZENCOVICH, *Alcune ragioni per sopprimere la libertà di stampa*, Roma-Bari, 1995, 9: «La libertà di stampa non nasce certo per tutelare stampatori e tipografi; nasce perché, a partire dal 1500, la stampa è *il* mezzo per esprimere e comunicare le proprie idee. Assicurando il libero esercizio dello strumento si volevano garantire le attività politiche, culturali, religiose, morali o scientifiche che per suo tramite si svolgevano. Certo non si vorrà sostenere la inviolabilità dei biglietti da visita o delle partecipazioni di nozze sol perché composti da una linotype e riprodotti da una stampatrice. Allora, cominciamo con il dire che quando, come ora, la stampa è una tecnica che serve a riempire dei pezzi di carta bianca o colorata producendo indifferentemente bibbie o calendari pornografici, discorsi di un capo di Stato o poster di un cantante, il bilancio di una società o i piccoli annunci delle massaggiatrici, non ha molto senso – e anzi si presta a gravi equivoci- accomunare tutto sotto lo stesso termine. Si devono fare delle distinzioni e certo non basta qualificarsi 'pubblicazione periodica' per sfuggire ad ogni controllo».

[48] C. MELZI D'ERIL, *Il sequestro di siti web: una possibile soluzione, prendendo spunto da un recente decreto del Gip di Milano*, in *www.penalecontemporaneo.it*, 20 settembre 2012.

[49] Si v. Trib. Milano, GIP, 25 maggio 2012.

ciò anche in funzione della rilevanza costituzionale che in alcuni casi le manifestazioni del pensiero non riferibili individualmente, o comunque anonime, possono rivestire.

La circostanza che le sezioni unite siano state chiamate a pronunciarsi, soprattutto sullo sfondo di un orientamento tutt'altro che contrastato, appare come un'occasione irripetibile per ottenere una risposta pressoché definitiva.

Non resta che attendere, auspicando –da un punto di vista squisitamente costituzionale- più che una conferma un *revirement* che avrebbe molto il sapore di una conquista in termini di garanzie. Con buona pace, peraltro, dell'usato e abusato argomento dell'equiparabilità tra stampa e Internet.

5. Per concludere, tra prospettive di riforma e miopie legiferatrici

Il percorso che si è tracciato nei paragrafi che precedono descrive le reazioni partorite dalla giurisprudenza a una situazione di sostanziale inerzia che il legislatore ha opposto all'evoluzione tecnologica che, nel frattempo, ha dato vita a nuove modalità di diffusione del pensiero. Ampliando, di fatto, l'ambito di tutela oggi riconducibile all'art. 21 Cost. Non c'è certo bisogno di una norma (sia essa una norma di rango legislativo, sia essa una norma costituzionale) a spiegarlo.

Anche quando il legislatore è intervenuto, come nel 2001 con la l. 62, il suo intervento si è distinto per confusione e assoluta mancanza di chiarezza. Buona parte delle reazioni che si sono osservate hanno preso le mosse proprio dall'analisi di questi svolgimenti, che però, data la natura effimera, sul piano legislativo hanno mantenuto di fatto ferma a circa sessant'anni fa la legislazione tuttora vigente in materia di stampa. Le difficoltà interpretative non sono poche ma, alla luce dei tentativi di regolazione che sono stati in discussione, vi è da esprimere paradossalmente l'auspicio che il legislatore si confermi fedele al proprio atteggiamento di inerzia.

L'auspicio di un non-intervento non riposa sull'adesione a un indirizzo incline a non considerare necessarie nuove norme, *rectius* a considerare sufficienti quelle tuttora esistenti. Tutt'altro, esso riposa sulla consapevolezza dell'inadeguatezza delle riforme che il Parlamento potrebbe approvare in materia, che trova conferma nei disegni di legge che hanno formato oggetto di discussione negli ultimi mesi e soprattutto nelle ultime settimane.

Mi riferisco, per concludere con alcuni spunti di attualità, in particolare al DDL S 119, sul cui contenuto i commenti, già emarginati in nota, di Marco Orofino, da un lato, e di Giulio Enea Vigevani e Carlo Melzi d'Eril dall'altro offrono uno spaccato dettagliato. Si tratta di un provvedimento sconcertante, che –purtroppo non isolato- ignora radicalmente le conquiste giurisprudenziali che anni di elaborazione hanno permesso di raggiungere.

In primo luogo, in palese contraddizione con la giurisprudenza di legittimità ormai consolidata, il DDL mira a estendere la responsabilità *ex* art. 57 c.p. al direttore responsabile della testata *online* registrata. In questo modo vengono trascurate le motivazioni di natura "tecnica" che la Cassazione, in occasione delle sue pronunce sul punto, aveva individuato come ostative a un'estensione *de plano* della responsabilità per omesso controllo. Viene così polverizzato il contributo non solo della giurisprudenza ma anche della dottrina che ha patrocinato questa soluzione.

Non solo: alla testata telematica registrata vengono estese anche le norme contenute nella legge stampa, in modo da creare una simmetria quanto più forte tra il web e la stampa tradizionale.

Peccato però che questo meccanismo sia ancorato alla scelta di registrare la testata *online*: sicché, come acutamente rilevato,[50] basta evitare la registrazione per non incorrere nell'applicazione dello stesso regime previsto dalla legge stampa.

Sotto altro profilo, si assiste a un tentativo di codificare un diritto all'oblio in versione estrema rispetto alle notizie pubblicate da siti Internet che risultino, per esempio, diffamatorie. Si introduce la possibilità di ottenere, per l'interessato, non già l'aggiornamento del contenuto delle pagine web, ma addirittura la rimozione delle stesse, il tutto senza la necessità di attendere la pronuncia di una sentenza definitiva.[51]

Anche su questo versante, evidentemente, il legislatore trascura le evoluzioni che si potrebbero registrare sul piano giurisprudenziale. E istituisce, in ogni caso, una misura che appare davvero sproporzionata rispetto al necessario bilanciamento tra tutela della reputazione e diritto all'informazione. Non solo: così facendo, probabilmente, il legislatore considera scontata l'inapplicabilità dell'art. 21, comma 3, Cost. a Internet, anticipando un'interpretazione che potrebbe anche risultare differente da parte della giurisprudenza di legittimità.

Se queste sono le premesse di un intervento riformatore, si comprendono bene allora le ragioni della sfiducia verso il legislatore e ogni iniziativa da questi promossa.

Meglio affidarsi, allora, alla più equilibrata attività interpretativa della giurisprudenza di legittimità, che è parsa iniziare a restituire i suoi frutti, correggendo le derive ancora non del tutto debellate nella giurisprudenza di merito. Confidando in ulteriori slanci coraggiosi che a un tentativo di governo confuso e incoerente della materia si rendano preferibili per l'attenzione ai principi che informano il diritto penale e alla dimensione costituzionale dei valori in gioco.

[50] Così C. MELZI D'ERIL - G.E. VIGEVANI, *Diffamazione: il legislatore che voleva troppo*, cit.

[51] In questo senso, il DDL sembra contrastare con quanto affermato, in merito all'obbligo di contestualizzazione delle notizie *online* in sede civile da Cass. civ., 5 aprile 2012, n. 5525.

INTERNET E I DELITTI DI OPINIONE: L'ELEMENTO SOGGETTIVO DEL REATO COME STRUMENTO DI SALVEZZA DELLA LIBERTÀ DI MANIFESTAZIONE DEL PENSIERO

Margherita Siracusa

Non approvo quello che dici,
ma difenderò fino alla morte il tuo diritto di dirlo.
(Voltaire)

Sommario: 1.Premessa all'ardua impresa:campo di battaglia, strumenti di lotta e obiettivi perseguiti 2.Internet: un nuovo luogo e un nuovo strumento di manifestazione del pensiero 3.L'elemento soggettivo nei reati di istigazione: come salvare la manifestazione del pensiero anche su internet

1. Premessa all'ardua impresa: campo di battaglia, strumenti di lotta e obiettivi perseguiti

Vi è il presagio che l'analisi del presente argomento costituirà un'ardua impresa.

E' certamente tale l'impresa che ha per oggetto lo studio del primario diritto della libertà di manifestazione del pensiero: fondamento ed impulso del progresso materiale e spirituale di ogni società (in ogni tempo) e presupposto di ogni altro diritto ritenuto fondamentale. Non può che costituire "ardua impresa", altresì, il dover necessariamente analizzare i limiti imposti a questo diritto; limiti che non minano l'assolutezza dello stesso ma ne garantiscano l'integrità. Assolutezza non vuol dire assenza di regolamentazione[1]; la regolamentazione è necessaria per impedire che un consociato, esercitando un proprio diritto, danneggi la sfera di libertà di un altro consociato, minacciando il cammino evolutivo della società. Nella presente "impresa", dunque, saranno analizzati i complessi rapporti tra il diritto di manifestare il pensiero e i diritti della persona che rilevano nei delitti di opinione.

Preme subito specificare, però, la necessità di abbandonare la locuzione "delitti di opinione", foriera di troppi equivoci. No, l'opinione non può mai assurgere ad elemento costitutivo di un delitto. Lo impedisce non solo il riconoscimento fatto dalla Costituzione all'art. 21 della libertà di manifestare il proprio pensiero ma, prima ancora, lo stesso principio di materialità (*cogitationis poenam nemo patitur*) *ex* art. 25 Cost. ed anche il principio di offensività, immanente nell'ordinamento giuridico.

I delitti che saranno oggetto di analisi saranno quelli c.d. di espressione[2]. Attraverso questa locuzione si vuole porre l'accento sull'importanza del carattere "esterno" che

[11] "*la garanzia di un diritto non esclude il regolamento dell'esercizio dello stesso*", così D. PULITANÒ, *Libertà di manifestazione del pensiero, delitti contro la personalità dello Stato e contro l'ordine pubblico*, in G. VASSALLI, in *Diritto penale e Giurisprudenza*. Cost., Napoli, 2006, 240.

[2] Locuzione utilizzata per indicare la necessità che, sia nel comportamento istigatorio sia in quello apologetico occorre un *minimum* di condotta esterna, idonea a creare il pericolo concreto di realizzazione

deve necessariamente assumere il pensiero, per essere offensivo dei beni giuridici tutelati. Segnatamente, i delitti di espressione oggetto di analisi saranno quelli di istigazione, realizzati però in un particolare contesto (e attraverso un particolare strumento) comunicativo. L'ardua impresa si svolgerà, infatti, su un "campo di battaglia" che negli ultimi decenni ha rappresentato una rivoluzione sia nel modo di comunicare il proprio pensiero sia nel modo di interagire con gli altri consociati.

Internet è senza dubbio un mass media unico nel suo genere. John Perry Barlow nel 1996 aprì così la sua dichiarazione di indipendenza del Cyberspazio "*Internet, il più grande spazio pubblico che l'umanità abbia mai conosciuto, la rete che avvolge l'intero pianeta, non ha sovrano*"[3].

Tutti i consociati possono attingere liberamente da internet ogni tipo di notizia e, al contempo, sono liberi di immettere ogni informazione che li riguarda e che riguarda la porzione di società in cui vivono. Internet è come una grande agorà. Un'agorà senza confini e senza tempo[4] in cui tutti hanno il desiderio di prendervi parte[5].

Le informazioni immesse, con il passa parola, assumono i contorni dei dati di massa e influenzano le interazioni tra i soggetti partecipanti (ma paradossalmente anche tra quelli che non vi prendono direttamente parte) minacciando l'integrità dei diritti fondamentali della persona. Non stupisce, allora, come internet sia l'agorà perfetta per compiere ogni genere di illecito, soprattutto quelli che dalla rapidità di diffusione della notizia ovvero dalla particolare relazione che si crea tra soggetto attivo e soggetto passivo del reato traggono linfa vitale.

Si fa riferimento alle attuali problematiche, giuridiche e criminologiche, connesse ai reati di istigazione: al suicidio- art. 580 c.p.- (si pensi agli effetti devastanti che il cyberbullismo ha provocato su alcuni adolescenti) alle pratiche pedofile -art. 414 *bis* c.p.- (impressionanti perché inestimabili le cifre di diffusione di immagini pornografiche e pedopornografiche immesse ogni giorno nella rete) alla violenza art. 3 L. n. 654/1975[6] (innumerevoli i siti telematici incitanti all'odio e alla violenza razziale), al sovvertimento degli ordini politici costituiti (si pensi al terrorismo), all'uso delle sostanze stupefacenti- art. 82 D.P.R. 309/1990.

La disamina di tutte le problematiche afferenti questi reati esula dal presente lavoro. Si tenterà, però, di trovare un punto di equilibrio tra la tutela della libertà di manifestare il proprio pensiero (anche quello più sgradevole o malvagio, giacché qui si discute di responsabilità giuridica e non di responsabilità morale) e i diritti connessi alla integrità fisica e alla libertà morale e sessuale della persona, soprattutto laddove i titolari di questi diritti siano i fanciulli.

---

del reato. Così G. BOGNETTI, *Apologia di delitto punibile ai sensi della Costituzione e interpretazione della norma dell'art. 414 c.p. u.c.*, in *Riv.it.dir.proc.pen*., 1971,55.

[3] Si v. S. RODOTÀ, *Il mondo della rete. Quali diritti e quali vincoli*, Bari, 2014.

[4] Molto attuale la problematica connessa al c.d. diritto all'oblio. Esso è stato ritenuto prevalente dalla Corte di Giustizia sul diritto di informazione giornalistica, al fine di garantire il ritorno allo stato di anonimato. Si v. sentenza della Corte di Giustizia C-131/12 del 13 maggio 2014, rep. *in* www.altalex.it. Per una introduzione si v. T. E. FROSINI, *Diritto all'oblio ed internet*, rep. *in* www.federalismi.it

[5] Nell'ultimo decennio vi è stata una "*tumultuosa diffusione*" dei social network che ha inciso profondamente sulla individualità e sulle relazioni interpersonali tra i consociati. Per una introduzione si v. L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. Mer*., 12, 2012, 252 ss.

[6] E succ. modif.: L. n. 205 del 25 giugno 1993 e L. n. 85 del 24 febbraio 2006.

Il legislatore ha tentato la sua "ardua impresa" attraverso la definizione delle citate fattispecie di istigazione. E' chiaro l'obiettivo di anticipazione della tutela di beni giuridici di inestimabile importanza: tutte le citate fattispecie, infatti, sono di pericolo astratto e ciò che si persegue è, nella maggior parte dei casi, l'atto di istigazione in sé. Qui si inserisce "l'ardua impresa" dell'interprete: ricercare delle soluzioni che creino un dialogo e non una contrapposizione tra valori costituzionalmente garantiti.

La ricerca di questo punto di equilibrio può rinvenirsi nell'elemento soggettivo. O meglio, accogliendo i principi fondamentali della teoria finalistica dell'azione di origine Welzeliana, nel dolo c.d. istigatorio, che risiede non solo nella colpevolezza ma anche nel fatto tipico. Questo presupposto appare importante per scongiurare delle conseguenze che altrimenti potrebbero verificarsi sul piano dell'accertamento probatorio: esse potrebbero consistere nell'approdare ad un giudizio di responsabilità penale attraverso l'accertamento di un *dolus in re ipsa* ovvero di una prova dell'elemento soggettivo che si perde nella prova del rapporto di causalità.

E sullo sfondo permane il "campo di battaglia" di internet, che è un'agorà privo di confini normativi e giudiziari, in cui i confini territoriali degli Stati non hanno più senso[7].

2. Internet: un nuovo luogo e un nuovo strumento di manifestazione del pensiero

La libertà di manifestazione del pensiero non ha una valenza dogmatica, definibile a priori: è una libertà variabile nel tempo e nello spazio, le cui caratteristiche dipendono dal momento storico e dalle condizioni politiche, culturali, religiose della comunità di riferimento. E' una libertà che varia perché variano gli interessi e le esigenze che attraverso di essa si esprimono; essa varia, perché variano gli strumenti attraverso cui è possibile esprimerla.

Innegabile, allora, la lungimiranza del legislatore costituente che all'art. 21 Cost[8]. ha sancito: "*Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, con lo scritto ed ogni altro mezzo di diffusione*". Quest'ultima locuzione garantisce la modernità della previsione costituzionale, potendosi adattare all'evoluzione delle forme di comunicazione. Si potrà diffondere il proprio pensiero attraverso la stampa, attraverso un comizio in luogo pubblico, attraverso la radio o la più moderna televisione; o ancora, attraverso un quadro, una canzone, una rappresentazione teatrale. Tutti questi sono mezzi di diffusione delle idee. E non è complesso comprendervi anche il particolare strumento di internet. Altresì, questa locuzione risalta l'intento del legislatore costituente di assicurare l'esercizio della libertà di espressione non tanto nei confronti di un particolare destinatario (diritto ugualmente garantito ma all'art. 15 Cost.) quanto nei confronti di destinatari indeterminati, di un

[7] Ormai notorie le problematiche inerenti la individuazione dei responsabili del reato e, conseguenzialmente, della giurisdizione sussistente. Chi immette informazioni sul web si trova in un luogo fisico, come il terminale da cui le immette e il modem che sfrutta per la connessione, tuttavia il server utilizzato per le attività di *down* e *up loading* può trovarsi anche a migliaia di chilometri di distanza.

[8] Art. 10 Convenzione europea dei diritti dell'uomo, art. 19 Dichiarazione Universale dei diritti dell'uomo e art. 11 della Carta di Nizza. Previsioni più complete rispetto alla Costituzione Federale degli Stati Uniti D'America del 1787 (art.1) e la Dichiarazione dei diritti dell'uomo francese del 1789 (art.11) che riconoscevano la sola accezione attiva e non anche quella passiva della libertà di manifestazione del pensiero.

pubblico indefinito. E' evidente, infine, come la libertà di cui all'art. 21 Cost. sia il presupposto di ogni altro tipo di libertà garantita dalla Costituzione (artt. 8,15,33 Cost. ecc.).

Species del *genus* della libertà di manifestazione del pensiero è la libertà informatica, comprensiva della libertà telematica. Ad ogni individuo sono garantite entrambe[9]: la libertà di elaborare elettronicamente i dati, di immetterli nella rete informatica e, dunque, di farli circolare liberamente nonché la libertà di acquisirne di nuovi e di diversi. Internet rappresenta una nuova frontiera della comunicazione anche perché, a differenza della stampa o della televisione, i soggetti attivi (cioè chi ha il potere di accesso alla rete)[10] coincidono con quelli passivi (gli utenti che ne usufruiscono)[11]. Ed è una libertà che deve essere garantita ad ogni età: la Convenzione Onu sui diritti dell'infanzia ha espressamente stabilito che è un diritto inviolabile del minore avere accesso alle informazioni, in particolare a quelle che mirano a promuovere il suo benessere sociale e morale nonché la sua salute fisica e mentale[12].

L'avvento di internet, che è un sistema dotato di una propria logica e di una propria semantica, ha contribuito a modificare il contenuto stesso della libertà di manifestare il pensiero sia nella sua accezione attiva sia in quella passiva.

L'informazione è più ricca: ogni individuo può accedere, attraverso l'ausilio dei motori di ricerca, ad intere biblioteche, librerie, banche dati, edicole virtuali senza ostacoli né finanziari né territoriali. Tuttavia, ciò comporta il noto fenomeno per cui più alto è il grado di diffusione di una informazione, più alto è il grado di veridicità che alla stessa è attribuito.

L'informazione ha un effetto di propagazione più celere e non risente dei confini territoriali o delle differenze linguistiche. Tuttavia, tale effetto fa perdere il controllo, il dominio sulla notizia: l'utente che immette delle informazioni su internet non sa da quali server passeranno e quanti avranno accesso alle stesse.

L'informazione può essere trasmessa simultaneamente ad un numero indefinito di soggetti. Attraverso chats, community, forum si può interagire, contemporaneamente, con un numero indeterminato di altri utenti. Di contro: tutte le informazioni, di dati in parte sensibili, sono visibili a tutti. E' come affiggere dei manifesti, in una grande piazza, sulla propria vita e non poter controllare chi può guardarli e per quanto tempo.

L'informazione sulla rete si fonda sulla forza delle parole. In specie, in assenza di una interazione fisica, fondata sulla forza suggestiva dello sguardo o dei gesti, le interazioni si fondano esclusivamente (o quasi) sul contenuto delle parole. Le relazioni

---

[9] L'informatica è quel settore della tecnologia (ramo del sapere) che studia l'informazione e il suo trattamento automatico attraverso l'elaborazione elettronica dei dati; per telematica, invece, si intende un sistema di apparati interconnessi in grado di comunicare a distanza, scambiandosi dati attraverso la tecnologia informatica.

[10] Esistono delle società che gestiscono il sistema delle rete internet (access provider), cui è necessario versare un "canone" per poter ottenere l'accesso alla rete. Si discute sulla inviolabilità della libertà telematica, ossia del diritto all'accesso gratuito alla rete. Si v. Direttiva n. 2000/31 del Parlamento e del Consiglio d'Europa , 8-06-2000 pubblicata in *Dir.Inf*., 2000, 683ss.

[11] Interessante la locuzione spesso utilizzata di "*Cyberdemocracy*". Si v. ad es. W. FISHER, *Freedom of Expression on the internet*, 2001, rep. in www.cyber.law.harvard.edu.

[12] Sempre attuali e preziose le riflessioni di J.S. MILL, *Saggiò sulla libertà*, Milano, Trad. Est., Ed.1999,19 ss. per cui impedire l'espressione di una opinione sarebbe un crimine commesso contro la razza umana, sia contro i posteri che contro i vivi, sia contro coloro che dissentono sia contro coloro che condividono.

che sorgono sulla rete (tramite chat, community, forum ecc) risultano per i soggetti coinvolti particolarmente profonde, coinvolgenti; forse, questo è un effetto dell'assenza dei condizionamenti offerti dalle apparenze.

La diffusione di internet, infine, incentiva la voglia di esprimere se stessi. Assecondando le inclinazioni narcisistiche umane, grazie alle esaminate peculiarità, internet incentiva ad esternare la propria personalità, comprensiva del personale modo di pensare (gli esempi eclatanti sono i social networks in cui, attraverso la creazione di un proprio profilo, corredato di immagini personali, si mette "in vetrina" la propria persona). Altresì, la voglia di esprimere se stessi è certamente incentivata dalla apparente, od in certi casi reale[13], anonimità garantita dall'uso di nickname o, frequentemente, di identità completamente inventate e per ciò solo inesistenti.

Si, internet è un'agorà, dove chiunque può salire sul palco dell'attenzione, anche celando la propria identità con una maschera, con la possibilità di urlare ad un numero indeterminato di persone, con effetti immediati e persistenti nel tempo, la propria personalità, il proprio modo di pensare e non in ultimo, le proprie degenerazioni, i propri disagi, le proprie patologie.

3. L'elemento soggettivo nei reati di istigazione: come salvare la manifestazione del pensiero anche su internet

Internet come agorà di interscambio e di interconnessione è il luogo ideale per la manifestazione del pensiero ma anche delle patologie individuali e sociali. Si suole distinguere tra reati informatici propri, in cui la *res* informatica è oggetto materiale del reato e reati informatici impropri, che sono reati comuni realizzati attraverso il computer, sub specie attraverso internet, che si atteggia a *instrumentum delicti*[14].

E' dall'osservazione della realtà che è derivata la curiosità circa le dinamiche sottese ai reati di istigazione commessi sul e mediante web. Si sono verificati casi in cui si è proceduto o contro ignoti o contro noti per istigazione al suicidio *ex* art. 580 c.p. Adolescenti che si sono tolti la vita perché vittime di pesanti e reiterati insulti, del c.d. cyberbullsimo[15], soprattutto perpetrati attraverso i social networks. Ovvero casi di siti in cui, attraverso la discussione in "privato"[16] o in forum "pubblici", o attraverso la fruizione di manuali appositi, si forniscono i modi "migliori" per compiere il suicidio. Casi di scambio e diffusione di materiale pedopornografico ed in specie di siti in cui si professa la bontà delle relazioni affettive/sessuali tra adulti e minori, che impongono alcuni interrogativi circa la frastagliata disciplina penalistica in materia, comprensiva del nuovo reato di istigazione alle pratiche pedofile *ex* art. 414 *bis* c.p. Casi di istigazione ad atti di terrorismo, anche e soprattutto a livello sovranazionale, che a volte

[13] Il riferimento è alla *darknet* o *deep net*: rete alternativa e parallela ad internet e del tutto anonima, il cui accesso è possibile solo attraverso determinati strumenti. Nata per scopi lodevoli, ossia per dare voce ai dissidenti politici ed ideologici dei Paesi dispotici, oggi rappresenta un grande bazar dell'illegalità. In essa si può acquistare di tutto: dalle armi alle sostanze stupefacenti, dagli stupri agli omicidi su commissione.

[14] Si v. D. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, 2004.

[15] Ultimo caso, il suicido di una adolescente per gli insulti ricevuti sul social network, dalla natura ambigua e per certi versi pericolosa, "Ask.fm". La notizia è rep. in www.ilmattinopadova.it.

[16] Emblematico il caso di un uomo statunitense che è stato condannato per istigazione al suicidio di due persone, una inglese ed una canadese, con cui aveva stretto, via mail, dei "patti suicidari". La notizia è rep. in www.NYTimes.com

si mescolano o si alternano ad accuse per istigazione all'odio e alla violenza[17] ispirata da motivi razziali. In essi accade spesso che al reato di istigazione si affianchino i reati di apologia, propaganda, proselitismo o reclutamento[18].

Casi, infine, di istigazione all'uso delle sostanze stupefacenti per l'esistenza di siti in cui si fa commercio o si offrono manuali istruttivi sulla coltivazione casalinga delle droghe.

Chiaramente non è questa la sede per analizzare tutte le problematiche afferenti le citate fattispecie; si cercherà, però, in pochi passaggi, di trovare un bilanciamento tra le esigenze di tutela dei beni giuridici sottesi alle fattispecie di istigazione e la libertà di manifestare il proprio pensiero.

Il bilanciamento non potrà svolgersi sul piano dell'elemento oggettivo del reato: di per sé sono fattispecie indeterminate sotto il profilo della condotta; di per sé il concetto di istigazione è vago. È più efficace, ossia più rispettoso del principio della personalità della responsabilità penale, il termine utilizzato all'art. 580 c.p. : "*determinare…altri al suicidio*", sebbene presenti anch'esso delle difficoltà connesse all'accertamento probatorio. Di fatto, il termine "istigare" indica l'attività di inferire da situazioni o condizioni i principi in essa impliciti. Non a caso le ipotesi di istigazione al suicidio vengono impropriamente definiti a "concorso necessario", per la necessaria collaborazione dovuta dall'istigato. Istigato, che innegabilmente, il più delle volte, ha già assunto una determinazione circa la soluzione suicidaria[19]. Altrimenti, non avrebbe alcun senso ricercare su internet dei manuali o chi ti possa spiegare come realizzare il letale gesto.

Si concorda, comunque, con quella dottrina che ritiene che il requisito della "pubblicità" conferirebbe maggiore determinatezza alla fattispecie: rispetto ad una induzione privata, un pensiero diretto ad un pubblico indeterminato produce un effetto suggestivo potenzialmente indefinito, a cui le interazioni collettive conferiscono un notevole contributo[20]. E questo discorso vale ancora di più se certi "proclami" sono fatti su community e social networks: ribadendo la loro natura di agorà in cui tutti vogliono partecipare e la cui partecipazione deve essere notata e sottolineata (si pensi all'esercito di "mi piace"; "follower" ecc).

Eppure sul requisito della pubblicità occorre fare un distinguo (che nella fattispecie di cui all'art. 414 *bis* c.p. sottende una critica, giacché rende vano il perseguimento dell'istigazione alle pratiche pedofile): un discorso è "aprire" un sito o fare un discorso pubblico, facendo un monologo persuasivo del proprio pensiero (sulla bontà dei suicidi, delle pratiche pedofile, delle differenze razziali ecc.) al fine di esprimere la propria opinione ovvero di avere qualche minuto di notorietà o di semplice, compassionevole considerazione (ai fini dell'imputazione non rileva); un discorso diverso è fare un monologo del proprio pensiero al fine di determinare altri nella commissione di illeciti.

---

[17] Si v. L. SCAFFARDI, *Oltre i confini della libertà di espressione:istigazione all'odio razziale*, Milano, 2009, 168 ss.

[18] Associazione per delinquere che utilizzava un blog per inneggiare all'odio razziale ed istigare ad atti dimostrativi. Cass, 31 luglio 2013, 33179 rep. in www.foroitaliano.it

[19] Sul punto: L. ALESIANI, *I reati di opinione: una rilettura in chiave costituzionale*, Milano, 2006, 349 ss e F. SCLAFANI, G. OTTAVIANO, G. BALBI, *Istigazione e aiuto al suicidio. Profili giuridici, criminologi, psicopatologici*, Napoli, 1997.

[20] Così A. SERENI, *Istigazione al reato e auto responsabilità*, Padova, 2000, 161 ss.

Nei reati di mera condotta, in assenza di un evento naturalistico, è necessario tenere in considerazione l'evento giuridico, in specie l'indirizzamento della volontà verso tale fine. Come insegna la teoria finalistica dell'azione di Welzel ogni individuo è capace di prevedere la direzione causale della propria azione; quando si realizza una condotta, si persegue un dato obiettivo o scopo. Il dolo, allora, ha una duplice collocazione: nella tipicità del fatto, perché senza il dolo la descrizione legale del reato non si può realizzare nella forma richiesta e nella colpevolezza, perché senza esso non si può distinguere dalla colpa. Il dolo è volontaria e cosciente realizzazione di un fatto ed è, dunque, ciò che consente di distinguere un fatto penalmente rilevante da uno che non lo è (ed un fatto doloso da uno colposo). Sul piano probatorio occorre dimostrare il rapporto di causalità tra intenzione e attuazione della condotta, non essendo sufficiente la dimostrazione del rapporto di causalità tra condotta ed evento[21]. Dalle modalità della condotta e dalla conoscenza delle circostanze di fatto, nonché dalla direzione univoca nei confronti di un soggetti determinati[22] e dal particolare strumento utilizzato occorre dimostrare che l'istigante mira alla determinazione dei reati, consapevole che l'evento giuridico deriverà dalla sua condotta[23]. Viceversa il rischio è di ledere non solo il principio della personalità della responsabilità penale, ma anche la libertà di manifestazione del pensiero (anche di quello malvagio, aberrante e riprovevole).

Il rischio è di modificare i reati di espressione in reati di opinione.

Chi apre un sito o un forum esprimendo pensieri, anche riprovevoli, non ha il dominio sugli accessi che avvengono sul proprio sito; è come se non avesse percezione della vastità e della suggestionabilità del pubblico che "lo legge" (potendo dubitare anche della di lui percezione del soggetto istigato).

Piuttosto è possibile parlare di apologia di reato, nei limiti in cui la stessa è prevista dalla fattispecie (non lo è ad esempio nel caso di istigazione all'odio razziale) ed è ritenuta ammissibile (perché, a volte, palesemente in contrasto con l'art. 21 Cost.). Ovvero di altre più gravi fattispecie che sono applicabili anche per le espresse clausole di riserva contemplate dalle norme sull'istigazione.

Viceversa, il rischio più concreto sarebbe quello non solo di scorciatoie probatorie ma anche di ammettere forme di istigazione con dolo eventuale o forme di "istigazione colposa". Ad esempio non aiuta l'ultimo comma dell'art. 414 *bis* c.p., in cui è stabilita l'impossibilità del soggetto di invocare a sua discolpa finalità di ordine artistico, culturale ecc.[24]; quasi come se si ammettesse una forma di responsabilità oggettiva per la forza istigatoria, deplorevole, dell'opera artistica realizzata[25].

Infine, preme sottolineare che questo ragionamento non avrebbe alcun senso se non si partisse dal presupposto che i beni giuridici tutelati e messi in rapporto con la libertà di cui all'art. 21 Cost siano beni, comunque, afferenti la persona. La sua integrità fisica

[21] Sempre fondamentale la lettura di F. BRICOLA, *Dolus in re ipsa*, Milano, 1960. Si v. anche G. P. DE MURO, *Il dolo: l'accertamento*, Milano, 2010, 65 ss.

[22] Non è di difficile accertamento il caso di un soggetto che aveva aperto più siti internet, connessi tra loro, in cui vendeva sostanze stupefacenti, metteva a disposizione manuali per la coltivazione e dettagliatamente ne discuteva sul suo forum. Si v. Trib. Rovereto, 17 maggio 2012, n. 109, per un commento si v. www.penalecontemporaneo.it

[23] Si v. Cass. 15 giugno 2010, n. 22782, rv 247519 o Cass. 1 febbraio 2007, n. 3924, rv. 235623.

[24] In generale si v. F. RIMOLI, *Sulla libertà dell'arte nell'ordinamento italiano*, Padova, 1992,17 ss.

[25] Si v. sul punto M. STRAMAGLIA, *Ratifica ed esecuzione della Convenzione di Lanzarote:istigazione a pratiche di pedofilia e pedopornografia (art. 414 bis c.p.) e adescamento di minorenni (art. 609 undecies c.p.)*, in *Giur. Mer*., 5, 2013, 95 ss.

(suicidio) la libertà sessuale del fanciullo (pedofilia) la salute anche pubblica (droga) la dignità umana e sociale (violenza e odio razziale) il suo diritto alla percezione di uno stato di sicurezza (terrorismo). Partendo dall'incomprensibilità della collocazione sistematica dell'art. 414 *bis* c.p., no, non si presiede la tutela di una ideologia[26], di una morale, anche sessuale, di un ordine pubblico[27] precostituito di cui si fa portatore uno Stato.

Lo Stato è privo di pensiero, non può essere tutelato su questo.

[26] Ha colpito la condanna in Spagna di una giovane 21enne, incensurata, per atti di terrorismo a mezzo Twitter, per aver scritto, ad esempio, che si sarebbe tatuata il nome di chi avrebbe ucciso il presidente spagnolo o che desiderava che l'ETA le fornisse le armi che essa ha deposto. Si ha notizia di ciò sul sito www.ebookextra.it.

[27] Si v. la tematica del c.d. negazionismo, per cui si pone anche il problema se il bene giuridico tutelato sia l'ordine pubblico o la dignità umana. Si v. E. FRONZA, *Il Negazionismo come reato*, Milano, 2012.

IL FURTO DI "IDENTITÀ DIGITALE": UNA TUTELA "PATRIMONIALE" DELLA PERSONALITÀ

Gianclaudio Malgieri

1. Introduzione: un diritto all'identità digitale

La moltiplicazione dell'identità personale in molteplici proiezioni digitali, la pervasività dei *social media* come mezzi privilegiati di interazione umana e come strumento di sviluppo della personalità, ha fatto parlare taluni di un diritto all'identità digitale[1].

In effetti la smaterializzazione dell'individuo e la giuridificazione dell'identità[2] scolpiscono con sempre maggiore forza i nuovi confini dell'identità della persona, fino a portare su un piano di sostanziale equivalenza l'identità personale e l'identità digitale. Se in sociologia si è parlato al riguardo di post-umano[3], la dottrina giuridica già da quasi un decennio fotografa le trasformazioni del corpo umano[4] in un corpo elettronico.[5]

La metafora della maschera artistica (non a caso significato della "*prosopon*" greca da cui il termine "persona"[6]) è forse quella che meglio riassume il concetto di identità digitale, soprattutto nell'ottica del furto d'identità.[7]

L'immagine della identità-maschera è ben precedente allo sviluppo delle tecnologie informatiche, tuttavia attraverso lo schermo tale metafora si rafforza: l'individuo contribuisce in prima persona a scrivere il suo profilo (o i suoi tanti diversi profili,

[1] Cfr. S. RODOTÀ, *Quattro paradigmi per l'identità,* in *Il diritto di avere diritti,* Bari, 2012, 298-310; G. RESTA, *dentità personale e identità digitale,* in *Dir.Informatica,* fasc.3, 2007, 511 ss.

[2] G. MARINI, *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità,* in Riv. dir. civ., 2006, 359 ss.

[3] N.K. HAILES, *How we became Posthuman, virtual bodies in Cybernetics, Literature and Informatics*, London, 1999.

[4] S. RODOTÀ, *Trasformazioni del corpo*, in Politica del diritto, 2006/1, 3.

[5] A. KROKER, M. WINSTEIN, *Data Trash*, trad.it. G. e A. Cara, Milano, 1996, XI.

[6] Cfr. al riguardo G. RESTA, *Identità personale e identità digitale*, cit., 514; J. ARESTY, *Digital identity and the lawyer's role in furthering trusted online communities*, 38 U. Toledo Law Review, 139.

[7] Cfr. P. CIPOLLA, *Social Network, furto d'identità e reati contro il patrimonio, cit., 2672B* ss. che analizza gli spunti letterari, religiosi e culturali della sostituzione di identità nella storia; Cfr. Anche S. TURKLE, *La vita sullo schermo. Nuove identità e relazioni sociali nell'epoca di Internet*, Milano, 2005, 210 ss. che vede il social network come medium per "maschere"molto discordanti dal sé, concordanti con il sé ma rivelate solo agli appartenenti alla propria cerchia, parzialmente concordante.

soprattutto sui *social network*[8]) e la maschera è così rafforzata da uno stile di scrittura, un vocabolario specifico e dei soggetti selezionati.[9]

Tale maschera artistica, tuttavia, è sia rappresentazione della persona, sia creazione dell'ingegno della persona (proprio perché è ad un tempo identità ed elemento esterno ad essa)[10]: una sorta di autoritratto che merita una doppia protezione, in quanto identità e in quanto espressione di (ingegno della) identità.[11] Questa ultima accezione merita tutela non soltanto nei confronti dei terzi, ma soprattutto nei confronti del gestore della piattaforma *online*, che potrebbe vantare propri diritti di proprietà intellettuale su realtà digitali frutto dell'espressione identitaria dell'utente,[12] pretesa da evitare quanto è da evitare l'essere (parzialmente) nella proprietà di qualcun altro, ma al tempo stesso elemento da cui trarre uno spunto: la nostra identità digitale è (anche) creazione del nostro intelletto.

Per tali considerazioni, occorre forse riferirsi ai dati personali non già come "dati identificativi" (e cioè che aiutano a identificare), bensì come "dati identitari" perché espressivi dell'identità personale, traducendo il concetto di *identity information* coniato dalla tradizione di *common law*[13].

Parallelamente si sta assistendo ad una patrimonializzazione o "proprietarizzazione" dei dati personali del consumatore, un sempre maggiore interesse commerciale all'acquisizione di quei dati, al punto da spingere la dottrina a parlare di "oro digitale"[14]. Si tratta del "costo della gratuità" dei servizi su internet[15], e non solo su Internet se pensiamo a un recente esperimento di *business model* in Danimarca, in cui in un negozio la metà dei beni sono gratuiti a patto che ci si registri con i propri dati e si indichino i propri gusti e interessi[16].

---

[8] P. CIPOLLA, *ult.op.cit.*

[9] D. WISZNIEWSKI, R. COYNE, *Mask and Identity: The Hermeneutics of Self-Construction in the Information Age., Building Virtual Communities*, 2002, 191-214; S. TURKLE; *ult.op.cit*.,

[10] Cfr. P. SAMUELSON, *Samuelson, privacy as intellectual property?*, in *Stanford Law Review*, 52, 1125 ss.

[11] Cfr. fuor di metafora l'emblematico problema della tutela del ritratto digitale in F. MONTALDO, *Il ritratto fotografico digitale tra diritto d'autore, diritti della persona e tutela della privac*y, *Resp. civ. e prev*., 2010, fasc.11, 2369B

[12] Interessante al riguardo J. ARESTY, *Digital identity and the lawyer's role, 38 U. Toledo Law Review,* nota 10 in cui si cita il caso di un conflitto tra un utente di un gioco online che ha provato a vendere la sua identità di gioco e il proprietario del gioco che ha obiettato che si trattava di sua proprietà intellettuale: è il macro-argomento degli *user-generated content*; S.P. CRAWFORD, *Who's in charge of who I am?, 9 N.Y.L. Sch. L. Rev.*, 2004/2005, 221 secondo cui la propria identità digitale consiste solo in un ingresso ad un database, dato che l'intermediario può arguire che tale identità è di sua proprietà intellettuale.

[13] Cfr. J. CLOUGH, *Principles of Cybercrime*, Cambridge, 2010, *passim.*

[14] Cfr. P. CIPOLLA, *Social network, furto d'identità e reati contro il patrimonio*, cit., par. 7

[15] Cfr. W.J. ROBINSON, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, in *Georgetown L.J.*, Vol. 98, 2010, 1195.; A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007; Cfr. L.C. UBERTAZZI, *Riservatezza informatica ed industria culturale*, in AIDA, Milano,1997, 530 ss; R.S. MURPHY, *Property Rights in Personal Information: An Economic Defense of Privacy*, in 84 Geo. L.J., 1996, 2381; P. MELL, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Elecrtonic Wilderness*, in *Berkeley Tech. L.J.*, vol. 11, 1996 , 1.

[16] C. ACCOGLI, *In Danimarca c'è un negozio dove si compra senza pagare*, pubblicato su www.repubblica.it il 3-09-2014, (consultabile su http://www.repubblica.it/tecnologia/2014/09/03/news/freemarket_in_danimarca_compri_gratis_in_cambio_di_pubblicit-94917875/).

Dunque il "patrimonio umano digitale" si fraziona in chiave d'accesso ad un patrimonio materiale (*bancomat*, carte di credito, ecc.), strumenti per un guadagno commerciale (il valore economico dei dati personali in sé), domicilio virtuale, estrinsecazione della proprietà intellettuale e strumento per i rapporti sociali (*online*): una proiezione complessa, economicamente più appetibile e più facilmente riproducibile dell'identità personale.

Pertanto, come si vedrà, né il delitto contro la persona (nella sua identità e riservatezza), né quello contro il patrimonio (che peraltro già subisce, per opera delle nuove tecnologie, la rottura dello storico dualismo violenza/frode[17]), né quello ad un bene soprarindividuale[18] (fede pubblica[19], amministrazione della giustizia[20]) riescono a fotografare fedelmente il fenomeno in esame.

È necessaria, dunque, un'opera di ripensamento degli schemi attuali della tutela penale del bene digitale (a partire da una riflessione sull'attuale concetto del bene "persona" e del bene "patrimonio"), anche grazie ad una riorganizzazione delle attuali fattispecie criminose, a partire dal furto d'identità digitale.

2. La nuova ipotesi di "frode informatica aggravata da furto d'identità digitale"

Non a caso è di recente introduzione nel nostro ordinamento penalistico il concetto di "furto d'identitià digitale". Si tratta della novella introdotta dall'art. 9 del d.l. 14 agosto 2013 n. 93 (il c.d. d.l. "femminicidio", convertito con modifiche dalla legge 15 ottobre 2013 n. 119[21]) che ha posto come nuova circostanza aggravante della frode informatica *ex* art. 640-*ter* c.p. che il fatto sia commesso "con furto o indebito utilizzo dell'identità digitale".

Lo scopo manifesto di tale nuova norma era quello di colmare un vuoto legislativo denunciato da più parti[22], anche considerando la sempre maggiore diffusione

[17] Un dualismo già fortemente riscontrabile alla base della ripartizione tra capo I e capo II del titolo XIII del Libro II del codice penale, cfr. L. PICOTTI, *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 38.

[18] *Ibidem*, 39.

[19] In caso di mera sostituzione di persona, *ex* art. 494 c.p., rientrante appunto nel Titolo VII "i delitti contro la fede pubblica".

[20] In caso di calunnia indiretta *ex* art. 368 c.p. (che rientra nel Titolo III "i delitti contro l'amministrazione della giustizia") che si verifica tutte le volte che il soggetto (sostituendosi ad altro soggetto) "simuli a carico di lui le tracce di un reato", e cioè ad esempio commetta diffamazione, ingiuria, o violazione del diritto d'autore utilizzando l'*account* di altra persona. Cfr. P. CIPOLLA, *Social network, furto d'identità e reati contro il patrimonio*, cit., par. 4

[21] Legge 15 ottobre 2013, n. 119, *Conversione in legge, con modificazioni, del decreto-legge 14 agosto 2013, n. 93, recante 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* (13G00163) *(GU n.242 del 15-10-2013).*

[22] Cfr. Comunicazione della Commissione europea "Verso una politica generale di lotta contro la cibercriminalità" (COM(2007)267); Agenda digitale europea, (COM(2010)245). La IX Commissione della Camera dei Deputati (DOC XVII, n. 26, del 22 gennaio 2013), ha sostenuto che «per combattere efficacemente il furto di identità digitale, oltre alle misure di carattere preventivo […], appare necessario dotare le istituzioni di adeguati strumenti normativi, introducendo nell'ordinamento il reato di furto di identità digitale, prevedendo adeguate sanzioni penali».

Inoltre, nella seduta del 19 settembre 2012, il direttore del servizio di Polizia postale e delle comunicazioni aveva affermato che «Il furto di identità digitale non ha oggi una specifica previsione normativa in Italia: sarebbe opportuno dare autonome configurazioni legislative da questo punto di

dell'utilizzo dei *social network* (sconosciuti al legislatore del 1993, come in parte anche a quello del 2008) e di nuove forme di *cybercrime*[23] che esulino dal classico *phishing.*

Che si tratti di una circostanza aggravante è dimostrato dal comma IV, che afferma che il delitto è punibile a querela della persona offesa "salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o *un'altra circostanza aggravante*"[24], sottintendendo dunque che le circostanze di cui al secondo e terzo comma siano delle aggravanti (ad effetto speciale).[25]

Pertanto, in base al principio *genus-species* che lega l'ipotesi generale a quelle aggravanti bisogna concludere che il "furto o l'indebito utilizzo di identità digitale" sia una specificazione di un elemento della fattispecie, ossia della condotta.[26] Occorre dunque analizzare in che termini si atteggia l'ipotesi comune e poi valutarne le ricadute in tema di protezione dell'identità digitale.

Il reato di frode informatica, introdotto all'art. 640-*ter* c.p. dalla legge n. 547/1993[27], recita così: "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032".

Pur trattandosi di una fattispecie a forma libera ("alterare in qualsiasi modo", "intervenire con qualsiasi modalità"; "dati, informazioni o programmi")[28], essa, come si vedrà, pone dei forti limiti ad una tutela piena all'identità digitale[29].

Un primo limite potrebbe ravvisarsi già nella descrizione della condotta sanzionata nella fattispecie di frode informatica. Infatti, si è ritenuto che l'indebito utilizzo di dati non possa integrare da solo il reato di frode informatica, necessitando questo di un "intervento" modificativo sulla struttura dei dati e dunque, almeno, di un trasferimento illecito di denaro da un patrimonio all'altro (dato che solo così si avrebbe un "intervento

---

vista>>. Cfr. Dossier del Servizio studi del Senato sull'A.S. n. 1079, ottobre 2013, n. 64, 102. In dottrina, cfr. A. DEL NINNO, *Il furto d'identità*, in *Trattato sui nuovi danni*, Vol. V, a cura di P. Cendon, Padova, 2011, 940; R. BARTOLI, *La frode informatica tra modellistica, diritto vigente, diritto vivente e prospettive di riforma*, in *Dir.Inf.*, fasc.3, 2011, 383 ss; C. PECORELLA, *Diritto penale dell'informatica*, II ed., Padova, 2006, 277 ss. Da ultimo in giurisprudenza cfr. le difficoltà della Cassazione nell'estendere troppo la fattispecie tradizionale di sostituzione di persona (art. 494 c.p.) per punire i furti d'identità digitale: Cass, sez. V, 29 aprile 2013, n. 18826, C., in *Cass. pen.*, 2014, 146 ss. con nota di G. STAMPANONI BASSI.

[23] Per una ricognizione generale sul fenomeno J. CLOUGH, *Principles of Cybercrime*, Cambridge, 2010.

[24] Si noti che lo stesso legislatore che ha introdotto il comma 3, ha esteso il comma 4 anche "alle circostanze di cui al terzo comma" (art. 9, comma 1, lett. b), D.L. 14 agosto 2013, n. 933, convertito, con modificazioni, dalla L. 15 ottobre 2013, n. 119).

[25] A. DI TULLIO D'ELISIIS, *Frode informatica commessa con sostituzione d'identità digitale: i profili applicativi*, in Altalex, 14.11.2013 (http://www.altalex.com/index.php? idnot=66034); L. PISTORELLI, *Relazione n. III/03/2013 del 16/10/13*, consultabile su www.dirittopenalecontemporaneo.it, 6-7.

[26] Cfr. T. PADOVANI, *Diritto Penale*, X ed., Milano, 2012, 252-253.

[27] Art. 10, l. 23 dicembre 1993, n. 547 (modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica).

[28] Cfr. A. DELLO IACOVO, *Articolo 640 ter: truffa o furto?, La frode informatica e il modello 640*, Temi Romana, 1996, 597. Per un'analisi specifica dei singoli elementi proposti dalle varie ipotesi sanzionate cfr. C. PECORELLA, *Diritto Penale dell'informatica*, cit., 61 ss.

[29] A. DI TULLIO D'ELISIIS, *cit.*

senza diritto sui dati").[30] Seguendo tale impostazione dovremmo concludere che il "furto o indebito utilizzo di identità digitale" (in quanto uso illecito di dati) possa costituire soltanto delle condotte strumentali alla realizzazione del fatto tipico. In realtà, la norma così formulata tutela l'identità digitale almeno nei casi (per nulla rari) in cui essa sia "rubata" o indebitamente utilizzata tramite un'azione di *hackeraggio,* rientrando quest'ultimo nella "alterazione del funzionamento di un sistema telematico" o comunque in un "intervento senza diritto su dati, informazioni, programmi".[31]

Tuttavia, per valorizzare pienamente il richiamo all'identità digitale compiuto dal più recente legislatore, e considerando che la vaghezza del dato linguistico non richiede una lettura univoca in senso di "modificazione", sembra preferibile sposare l'opposta lettura in dottrina, per cui anche il mero utilizzo di dati (tra cui *password* e *account* e quindi una "sostituzione d'identità digitale" [32]) costituisca una condotta rientrante nell'"intervento senza diritto sui dati", purché a ciò consegua un danno ed un profitto.[33]

3. L'ingiusto profitto con altrui danno: gli "elementi-ostacolo". Modelli a confronto

È dunque necessario analizzare proprio questi ultimi due elementi della fattispecie.

Innanzitutto bisogna chiedersi se questi siano degli elementi costitutivi del fatto tipico o delle condizioni obiettive di punibilità.

Data la formulazione sintattica della norma non sembra ci siano dubbi sulla loro natura di elementi costitutivi. Infatti, il "profitto" è l'oggetto della condotta di "procurare" nella proposizione principale del periodo del primo comma e non un mero elemento accidentale o di chiusura.[34] E ciò è confermato dal fatto che il bene giuridico tutelato dal reato di frode informatica è indubbiamente quello del patrimonio [35]: l'appropriazione illecita di denaro (l'ingiusto "profitto") non può essere mera condizione per attivare la punibilità, ma è spina dorsale della norma.

L'"altrui danno" in questa ottica è la conseguenza diretta di tale "ingiusto profitto"[36], pertanto anche tale elemento sembra costituire la fattispecie e non determinarne solamente la punibilità.[37]

---

[30] C. PECORELLA, *ult.op.cit.*, 90 e 103.

[31] C. PECORELLA, *ult.op.cit*., 82-83; cfr. Anche P. CIPOLLA, *Social network, furto d'identità e reati contro il patrimonio,* cit., par. 4 che prevede il concorso tra l'art. 640-ter c.p. e la sostituzione di persona *ex* art. 494 c.p. intendendo proprio questa ipotesi. Si sottolinea tuttavia, come si vedrà *infra*, la necessità comunque della dimostrazione del profitto per l'agente e del danno per la vittima.

[32] Si noti che "sostituzione d'identità digitale" è la rubrica dell'art. 9 del d.l. 93/2013, dunque il *nomen iuris* della fattispecie in esame.

[33] L. SCOPINARO, *Internet e reati contro il patrimonio*, Torino, 2007, 72-73.

[34] Una questione analoga si è posta in dottrina per individuare la natura del requisito del "nocumento" nel trattamento illecito di dati *ex* art. 167 cod.privacy e si è arrivati ad una soluzione opposta sia da un'analisi formale della fattispecie sia considerando il bene della riservatezza a fondamento della norma; Cfr. ad es. L. MANNA, *Commento al d.lg. 196/03, DPP*, 2004, 17; V. DESTITO, *Dati personali (tutela penale dei),* (I agg.), *Digesto delle discipline penalistiche*, Torino, 2008. Vd. *Infra.*

[35] Ciò si evince dalla collocazione al Titolo XIII del libro II, ovvero tra i delitti contro il patrimonio, al Capo II (Delitti contro il patrimonio mediante frode) per di più con un forte richiamo (nel *nomen* e nella numerazione) al reato comune di truffa *ex* art. 640 c.p. Cfr. A. DELLO IACOVO, *Articolo 640-ter: truffa o furto?*, cit., 597; G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 154-156.

[36] Per un'analisi dettagliata sulla "ingiustizia" del profitto nella frode informatica cfr. G. PICA, *ult.op.cit.,*144 ss.

Sul punto è, del resto, concorde la totalità dei pronunciamenti della giurisprudenza di legittimità.[38]

Tuttavia, per comprendere quanto la richiesta di tali ultimi requisiti riduca fortemente il portato di tutela all'identità digitale della novella, si può confrontare la norma in esame con le altre disposizioni penali che sanzionano condotte simili a quella di sostituzione d'identità digitale.

In primis, la sostituzione di persona *ex* art. 494 c.p. Tale norma non prevede la realizzazione di un danno e di un profitto, ma solo il dolo specifico di danno oppure di "vantaggio".

Il motivo della mancanza del danno tra i requisiti del fatto tipico può desumersi dalla collocazione di tale reato tra quelli contro la "fede pubblica", un bene che è leso già nel momento in cui uno o più soggetti (in quanto esponenti della titolarità diffusa della fede pubblica) sono tratti in inganno, senza necessità di dimostrare ulteriormente l'offensività del fatto, se non nella volontà criminosa dell'agente (per cui il dolo specifico).[39]

Passando poi all'art. 167 cod.privacy, che sanziona il "trattamento illecito di dati", si nota che anch'esso richiede il medesimo dolo specifico di danno o di vantaggio, ma in più richiede l'inverarsi di un "nocumento".

Quest'ultimo, interpretato come una condizione obiettiva di punibilità intrinseca e non come elemento costitutivo della fattispecie[40], si ritiene sia stato introdotto per

---

[37] L. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 93, secondo cui la previsione di un evento di profitto e danno aventi consistenza economica sono centrali allo scopo di identificare nel "fatto digitale" l'offesa al patrimonio individuale e di distinguere tale offesa da altre possibili offese a beni giuridici diversi realizzate parimenti con impiego di dati; C. PECORELLA, *Diritto Penale dell'informatica*, cit., 118, secondo cui l'ingiusto profitto con altrui danno costituisce la conseguenza diretta ed immediata dell'esito alterato del processo di elaborazione; anche G. PICA, *Diritto penale delle tecnologie informatiche*, cit., 144 che parla di tali elementi in termini di "momento consumativo" e di "evento giuridico del reato", analogamente A. MASI, *Frodi informatiche e attività bancaria*, in *Riv.pen.dell'Economia*, 1995, n. 4, 428.

[38] Cass., sez. II, 11 novembre 2009, Gabbriellini, rv. 245696.; Cass., sez. VI, 4 ottobre 1999, De Vecchis, rv. 214942; conf. Sez. V, 24 novembre 2003, Rv. 227459; da ultimo Cass., Sez. II, 24 maggio 2012, n.23798, in *Diritto & Giustizia*, fasc.0, 2012, 487, con nota di A. FERRETTI.

[39] Sul ruolo del dolo specifico come elemento di tipizzazione del fatto di reato, cfr. L. PICOTTI, *Il dolo specifico. Un'indagine sugli elementi finalistici delle fattispecie penali*, Milano, 1993, 501 ss. Riguardo al caso in commento cfr. A. ROCCO, *Relazione del Guardasigilli, Lavori preparatori*, V, p. II, Roma, 1929, 270, per cui l'intento manifesto dell'introduzione del reato di sostituzione di persona giace proprio nell'obiettivo di evitare che la tutela della pubblica fede fosse lasciata soltanto alla truffa e ai reati contro il patrimonio, e dunque è una fattispecie costruita proprio sull'irrilevanza dei requisiti del danno e del profitto; C. FLICK, *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, Dir. informatica, fasc.4-5, 2008, par. 2; R. CAPPITELLI, *La sostituzione di persona nel diritto penale italiano*, nota a Cass., sez. V, 26 febbraio 2004, n. 8670, in Cass. Pen., 2005, 1269, 2993 ss.; A. PAGLIARO, *Falsità personale*, *voce* Enciclopedia del diritto, XVI, Giuffrè, 646 ss.

[40] Cass., sez. III, 9 luglio 2004, n. 30134, *GDir*, 2004, n. 35, 67; Cass., sez. III, 17 febbraio 2011, rv. 249991, da ultimo Cass., sez. II, 24 maggio 2012, n. 23798, in *Diritto & Giustizia*, fasc.0, 2012, 487, con nota di A. FERRETTI. In dottrina Cfr. L. MANNA, *Commento al d.lgs. 196/03*, *DPP*, 2004, 17; V. DESTITO, *Dati personali (tutela penale dei)*, (I agg.), *Digesto Online*, 2008, che hanno interpretato il nocumento come una condizione obiettiva di punibilità poiché non si spiegherebbe la presenza del dolo specifico di profitto "o" di danno se poi il danno stesso fosse parte costitutiva della fattispecie, del resto se così non fosse il nocumento dovrebbe rientrare nel rappresentazione soggettiva, quandanche sia necessario anche il solo dolo specifico di "profitto" (e non anche di danno, data la presenza di una

ragioni di tecnica legislativa[41], con la volontà di rispondere ai dubbi di legittimità costituzionale sollevati da un'incriminazione troppo lata, circoscrivendo la fattispecie ai casi in cui il bene subisca un'effettiva e tangibile lesione, dimostrata dal verificarsi del nocumento.[42] Si è anche detto, in altre parole, che il riferimento al nocumento evoca ed istituzionalizza il principio di offensività.[43]

Non deve trascurarsi, inoltre, che questa è l'unica norma penale che esplicitamente tutela il bene giuridico dell'"identità personale" [44]; pertanto, i requisiti per la verificazione del fatto tipico sono particolarmente collegati a tale oggetto di protezione e andrebbero presi a modello per una eventuale futura norma che si occupi di tutelare l'identità digitale.[45]

Infine, l'art. 615-*ter* c.p. che sanziona l'accesso abusivo ad un sistema informatico o telematico non richiede altro che che la mera introduzione in un sistema elettronico protetto. Essendo posto tra i reati a tutela del domicilio non stupisce che l'offesa sia insita nella mera intrusione in tale "domicilio informatico", purché tale luogo virtuale sia realmente riservato (e dunque abbia delle misure di sicurezza adeguate).[46]

La frode informatica, invece, è l'unica delle norme fin qui analizzate che tutela (grazie alla nuova aggravante di sostituzione d'identità) l'identità personale digitale da una prospettiva patrimonialistica e non può prescindere dunque dalla dimostrazione in concreto dello spostamento economico dalla vittima al reo.[47]

Si tratta tuttavia di valutare in che termini il "danno" e l'"ingiusto profitto" siano effettivamente ostativi ad una tutela "pura" all'identità digitale (e cioè non surrogata ad istanze economiche) e se ci siano perciò spazi per una interpretazione non meramente patrimonialistica di tali due elementi.

4. Il profitto e il danno : margini per una tutela "non patrimoniale"?

La fattispecie di frode informatica, così come formulata, sembra lasciare spazio ad interpretazioni ampie dei concetti di danno e profitto; tuttavia, ciò non deve lasciare il campo ad arbitrarie interpretazioni manipolatrici, ma occorre anzi uno sforzo maggiore per portare a determinatezza e coerenza gli elementi costitutivi in commento.

---

disgiuntiva). Di opinione contraria D. IELO, V. SAPONARA, in AA.VV., *Codice della privacy*, II, Milano, 2004, 710 e 2148.

[41] V. DESTITO, *Dati personali (tutela penale dei), cit.*, che parla di una esigenza di "effettiva necessità del trattamento sanzionatorio".

[42] Così Cass., sez. III, 9 luglio 2004, n. 30134, *GDir*, 2004, n. 35, 67.

[43] Cass., Sez., II, 24 maggio 2012, n.23798, cit.

[44] Assieme alla " riservatezza", e al "diritto alla protezione dei dati personali". Cfr. Art. 2, comma 1, cod.privacy.

[45] *A contrario*, si può affermare che, posto il modello dell'art. 167 cod.privacy, i requisiti richiesti dalla "frode informatica commessi con sostituzione d'identità digitale" sono del tutto inopportuni per una tutela efficace dell'identità personale.

[46] R. BORRUSO, *La tutela del documento e dei dati*, in AA.VV., *Profili penali dell'informatica*, Milano, 1994, 28 ss. secondo cui il reato di accesso si perfeziona anche se "l'intromettitore non ha preso conoscenza di alcuna informazione, né ha altrimenti turbato il funzionamento del *computer*, così come commette violazione di domicilio chi voglia trovarvi una persona che ivi abita anche se poi non la trova". Per una disamina più approfondita sul bene giuridico tutelato dalla norma, vd. *infra*.

[47] Vd. *supra.*

Innanzitutto, bisogna sottolineare che il nostro art. 640-*ter* c.p. è l'unico nel panorama internazionale ad utilizzare tali termini ampli in una norma che ha il fine tutelare il patrimonio della vittima.[48]

In effetti il codice penale tedesco al §263*a* si esprime in questi termini: "chiunque con l'intenzione di procurare (...) un ingiusto *vantaggio patrimoniale, danneggia il patrimonio* altrui". Oltre alla peculiarità di introdurre il vantaggio come mero elemento del dolo specifico, non si può fare a meno di notare l'esplicito riferimento al patrimonio nella norma.[49]

Del tutto analoga è la disposizione all'art.386A del codice penale greco.[50] Molto simile è anche il § 148a del codice penale austriaco che parla di "ingiusto *arricchimento*" e "danno al *patrimonio* altrui",[51] così come quella portoghese che differisce solo nella espressione "illecito arricchimento".[52] Mentre il codice penale spagnolo all'art. 248 (*estafa mediante procedimentos informaticos*) si riferisce ad uno "scopo di lucro"[53] e il codice penale svizzero parla esplicitamente di un "trasferimento di attivi" (art. 147).[54]

Si noti, per altro verso, che il codice penale francese non pone la frode informatica tra i reati contro il patrimonio[55], ma contro i "beni" (e nello specifico tra i "danni ai sistemi di trattamento automatizzato di dati")[56]. Tale norma, di fatto, è analoga al nostro "accesso abusivo ad un sistema informatico" (art. 615-*ter* c.p.).[57]

Se da un lato, dunque, sembra ghiotta l'occasione per sfruttare l'indeterminatezza delle espressioni usate nel codice penale italiano a vantaggio di un significato anche non meramente patrimonialistico, dall'altra occorre specificare che le espressioni menzionate nei codici penali stranieri non sono frequenti nel nostro Titolo XIII della parte speciale del codice italiano, laddove invece si utilizza sempre l'espressione "profitto" e "danno" con valore patrimoniale. Nello specifico, la parola "profitto" ricorre nella quasi totalità dei delitti contro il patrimonio[58] e non è infrequente la parola

---

[48] Cfr. *excursus* in materia di frode informatica in C. PECORELLA, *Diritto Penale dell'Informatica*, cit., 64 ss. Solo la norma svedese (sec.1, cap.9, codice penale) parla di "profitto per il reo e danno per un'altra persona", utilizzando termini analoghi a quelli della norma italiana.

[49] K. TIEDMANN, *Strafgesetzbuch*. *Leipziger Kommentar*, XI ed., Berlin, 1998, sub § 263a.

[50] E. VASSILAKI, *Computer Crimes and Other Crimes against Information Technology in Greece*, in Rev.Int.dr.pén. (vol.64),1993, 367 ss.

[51] Cfr. G.F. SEILER, *Kritische Anmerkungen zum StrÄG 1987 den Besonderen Teil des StGB, in KBkm 1989m 751 ss.*

[52] Cfr. J. FIGUEREDO DIAS, *Introduzione al codice penale portoghese* (trad.it. a cura di G. Torre), Padova, 1997.

[53] T.S. VIVES ANTON, J.L. GONZALES CUSSAC, in AA.VV., *Comentarios al Còdigo Penal de 1995*, vol II, Valencia, 1996, *sub*. art. 248.

[54] N. SCHMID, *Computer-sowie Check und Kreditkarten-Kriminalität*, Zurigo, 1994, 215 ss.

[55] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, oggi Article 323-1 code pénal, "*Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende*".

[56] Livre III, Titre II, Chapitre III, "*Des atteintes aux systèmes de traitement automatisé de données".*

[57] L. SAENKO, *Le nouveau délit d'usurpation d'identité numérique : RLDI* juin 2011, n° 72, 63 ss.

[58] Artt. 624 (furto); 629 (estorsione, "ingiusto profitto con altrui danno"); 630 (sequestro di persona a scopo di estorsione), 632 (deviazione di acque e modificazione dello stato dei luoghi); 633 (invasione di terreni o edifici); 640 (truffa); 640-*quinquies*; 646 (appropriazione indebita); 648 (ricettazione) c.p.. Tutti

"danno"[59], quando il danno patrimoniale non sia già un requisito implicito nella fattispecie.[60]

La giurisprudenza è unanime nel considerare il "danno" in soli termini patrimoniali, mentre è più elastica sul significato di profitto[61].

Tale interpretazione ha fatto leva sulla forte analogia sussistente tra la truffa e la frode informatica e la conseguente applicazione alla seconda fattispecie dei requisiti formali da sempre richiesti per la prima (la truffa comune). Non è mancato neppure chi estendesse alla frode informatica il portato giurisprudenziale in tema di estorsione (l'altro reato tradizionale che presenta la stessa formulazione dell'art. 640-*ter* riguardo all'"ingiusto profitto con altrui danno").[62]

Il danno dunque deve comportare esplicitamente una *deminutio patrimoni* per la vittima.[63]

Escluso casi isolati[64], anche la dottrina sottolinea che il danno deve essere sempre apprezzabile economicamente, non potendovi rientrare utilità di tipo strettamente personali o morali, al punto che si è affermato che anche il trasferimento di un bene dotato solo di valore personale o affettivo per la vittima non può integrare il danno richiesto per la sussistenza del reato.[65]

Per quanto riguarda l'"ingiusto profitto", invece, la situazione è molto diversa. In effetti, nonostante il legislatore del 1930 mirasse (per la truffa) ad un'idea di profitto totalmente patrimonialistica,[66] la giurisprudenza da sempre interpreta il profitto in un senso più ampio, comprensivo di "qualsiasi utilità, anche di natura non patrimoniale", spingendosi fino a "vantaggi soltanto psicologici o morali".[67]

---

reati in cui lo spostamento patrimoniale è evidente. Cfr. del resto A. ROCCO, *Relazione del Guardasigilli al Codice Penale, Lavori preparatori*, cit., 270 per cui il profitto è espressamente economico.

[59] Artt. 629 (estorsione) e 640 c.p. (truffa).

[60] Ad esempio nel furto si parla di "spossessamento" (art. 624 ss.), nella rapina di "impossessamento" (art. 628) e nella usurpazione di "appropriazione" (art. 631): sono tutte descrizioni empiriche di un pregiudizio patrimoniale ai danni della vittima.

[61] Cfr. G. PICA, *Diritto penale delle tecnologie informatiche*, cit., 148 ss.

[62] Cass., sez. III, 2 maggio 2012, n. 23798, in *Guida dir*., 2012, 38, 81; Cass. pen. sez. II, 11.11.09, Gabbriellini, rv. 245696.; Cass., sez. VI, 4.10.99, De Vecchis, Rv. 214942; conf. Cass., sez. V, 24.11.03, Rv. 227459.

[63] Cfr. Cass., sez.II, 3 aprile 1986, in Cass. Pen., 1987, 2137; Cass., sez. V, 20 settembre 1989, in *Giust.pen.*, 1990, II, 438 per cui "il danno deve avere contenuto patrimoniale, deve concretizzarsi cioè in un *detrimento del patrimonio*". Analogamente Cass., sez. II, 05-03-2008, n. 10085, rv. 239508.

[64] A. DI TULLIO D'ELISIIS, *cit*., che afferma che il "danno" può essere anche non patrimoniale.

[65] G. PICA, *Diritto penale delle tecnologie informatiche*, cit., 154.

[66] Ad es. nel caso dell'art. 494 c.p. Si noti al riguardo A. ROCCO, *Relazione del Guardasigilli al Codice Penale*, cit., 270, per cui "*i caratteri differenziali (...) sono evidenti: nella truffa occorre il fine di procurare a sé o ad altri un ingiusto profitto con altrui danno; nella sostituzione di persona è sufficiente il fine di procurare, a sé o ad altri, un vantaggio, o di procurare ad altri un danno. L'ingiusto profitto con altrui danno, nella truffa, delitto contro il patrimonio, ha un contenuto patrimoniale, o, almeno, incide sul patrimonio altrui; nella sostituzione di persona, invece, «vantaggio» indica una qualsiasi utilità, anche non economica. Inoltre, nella truffa, all'ingiusto profitto del colpevole è correlativo il danno altrui, nella sostituzione di persona questa correlazione può mancare*".

[67] Su tale interpretazione nell'ambito della truffa *ex* art. 640 c.p., cfr. Cass. 17 gennaio 1957, in *Giust.pen.*, 1957, II, 458 per cui "non è necessario che il profitto perseguito dall'agente abbia carattere economico, neppure in forma mediata, ben potendo esso consistere nel soddisfacimento di un bisogno di qualsiasi genere, anche soltanto psicolgico o morale". Similmente Cass. 6 marzo 1974, in *Cass.pen.mass.ann.*, 1975, 1135; Cass., 3 aprile 1986, in *Cass.pen.mass.ann*, 1987, 2137. Invece in tema di estorsione, Cass., sez. II, 14 aprile 1983, n. 3110, in *Riv.pen*., 1983, 910; in precedenza: Cass., sez.II,

In effetti, il delitto contro il patrimonio si estrinseca in un detrimento del patrimonio della vittima, ma non per forza in una *traditio,* cioè in un'operazione di perfetto trasferimento da un patrimonio all'altro.[68]

Del resto, anche in altri ambiti (come il reato di traffico illecito di rifiuti di cui al d.lgs. n. 22 del 1997, art. 53-bis) la giurisprudenza di legittimità ha constatato che l'espressione ingiusto profitto "non deve assumere necessariamente carattere patrimoniale, potendo questo essere costituito anche da vantaggi di altra natura".[69]

5. Spiragli per un nuovo concetto di patrimonio?

Tali spunti sembrano un interessante spiraglio per slegare la frode informatica commessa con furto d'identità digitale dai suoi stretti binari patrimonialistici.

Tuttavia quand'anche il profitto potesse riguardare anche solo vantaggi giuridici, morali, sociali, il "danno" resta unanimemente circoscritto ad un pregiudizio al patrimonio.

Pertanto, l'unica strada percorribile per estendere l'applicazione del reato di frode informatica commesso con furto d'identità digitale oltre le strette maglie economiche può derivare da un totale ripensamento del concetto di "patrimonio". Si tratterebbe cioè di estendere tale nozione ad un concetto di "patrimonio personalissimo", inteso come contrappeso in termini di riservatezza e libertà negoziale del guadagno concreto che gli operatori del *web* ricevono a fronte di un "bene" immateriale ma economicamente rilevante: i dati personali.[70]

Del resto, illustre dottrina giuseconomica statunitense già un decennio fa[71] ha abbozzato una monetizzazione del valore medio dei dati personali di un consumatore-tipo. Su questi beni di valore, ogni persona detiene un monopolio passivo (in quanto unico soggetto che originariamente possiede e può disporre di quei dati) e attivo (in quanto unico soggetto che può creare e modificare quei dati nel tempo). Il monopolio su beni immateriali è un concetto mutuato dal diritto della proprietà intellettuale, del resto le forme in cui i "*data collector*" (leciti o illeciti) vendono i dati personali dei consumatori è tramite "base di dati"[72], su cui il fornitore può vantare un diritto di proprietà intellettuale.

E' chiaro che un eventuale lesione di tale monopolio va a costituire un danno economico.

In realtà, è un danno solo eventuale e per la sua dimostrazione bisognerebbe appoggiarsi ai ragionamenti svolti dalla giurisprudenza civilistica in tema di danno all'immagine: il danno consisterebbe nel mancato guadagno che si sarebbe avuto da una possibile vendita dei propri dati personali a operatori del web (pubblicitari, *ecc*.)

---

21 aprile 1965, in *Giust.pen*., 1966, II, 351; Cass. Sez.II, 20 giugno 1967, in *Arch.pen.*, 1968, II, 104; Cass., sez.I, 3 novembre 1967, in *Cass.pen.mass.*, 1968, 743.

[68] Come conferma la Cassazione penale a SS.UU., 29.9.11, Rossi, rv. 251499.

[69] Cass., sez. III, 16.10.05, Fradella, rv. 232351; ripreso anche da Cass., sez. III, 24/05/2012, n. 23798, *Guida dir*.2012, 38, 81.

[70] A. RICCI, *Il valore economico della reputazione nel mondo digitale. Prime considerazioni*, cit., 1297, che sottolinea "il ruolo di bene essenziale nei processi di produzione economica che la reputazione digitale è destinata ad assumere nella società dell'informazione"; P. CIPOLLA, *Social network, furto d'identità e reati contro il patrimonio*, cit., par. 7: i profili dei social network, "oro digitale".

[71] R.S. MURPHY, *Property Rights in Personal Information,* cit., 2381.

[72] P. MELL, *Seeking Shade in a Land of Perpetual Sunlight,* cit., *passim.*

interessati. Si tratta, ad esempio, del Caso Kodak, molto rilevante ai nostri fini perché (seppur in ambito prettamente civilistico) proietta sul piano economico del danno patrimoniale la tutela dell'identità personale.[73]

Del resto, pur uscendo dall'ottica del "monopolio", da più parti in dottrina si è insistito, nell'applicazione della fattispecie di truffa, sulla necessità di ripensare il patrimonio in termini non più meramente "economico-materiali", ma "giuridici".[74]

Inoltre, si è anche specificata la peculiarità delle fattispecie di "truffa" e "frode informatica" nel panorama dei delitti contro il patrimonio: esse, infatti, non tutelano soltanto il patrimonio *tout court*, ma anche (proprio perché reati di inganno) "la libertà negoziale", garantendo che ciascun soggetto possa liberamente e consapevolmente determinarsi nel compiere ogni atto di disposizione del proprio patrimonio.[75]

In effetti, nei casi di furto di dati del consumatore, l'asimmetria informativa e strutturale si amplifica. Si avranno degli imprenditori sempre più forti, con un completo bagaglio informativo non solo sul prodotto, ma anche sul consumatore e dei consumatori sempre più deboli, spogliati anche dell'unico velo di ignoto sui propri gusti personali, le proprie inclinazioni, la propria storia e dunque sempre più influenzabili.

Da ultimo, si noti come l'ordinamento francese nel punire la "frode informatica", la colloca sì tra i delitti contro il patrimonio (*Livre III, Des crimes e delictes contre les biens*), ma laddove il "bene" leso è l'integrità della struttura informatica (*Titre II, Chapitre III, des atteintes aux systèmes de traitement automatisé de données*) , intesa anche come dati elaborati dalla macchina e dunque la lesione al bene, *lato sensu*, potrebbe giacere già solo nell'alterazione di un *account*, in quanto "bene"[76] nella titolarità delle vittima.[77]

Del resto, una riconsiderazione del valore del "patrimonio" fu fatta propria anche dal "Progetto Pagliaro" (Libro I, Titolo XI) che sottolineava la necessità di una rilettura in termini "personalistici" del concetto di patrimonio.[78]

Altra strada ipotizzabile sarebbe semplicemente quella di considerare che per quanto riguarda la novella in commento non si debba interpretare il "danno" alla stregua dell'ipotesi di truffa, ma piuttosto in un senso anche non strettamente patrimoniale.

Tuttavia, tali coraggiose interpretazioni *sic stantibus rebus* mal si confanno al principio di stretta legalità proprio del diritto penale.

E in attesa di una riformulazione autonoma della norma[79] non resta che: da un lato valorizzare il più possibile la portata innovativa della novella in commento senza

---

[73] Cfr. Cass. civ., sez. III, 16.05.2008, n. 12433, per cui l'illecita pubblicazione dell'immagine altrui obbliga l'autore al risarcimento dei danni patrimoniali e non patrimoniali: qualora non sia possibile dimostrare specifiche voci di danno patrimoniale, va comunque risarcito il cd. prezzo del consenso, cioè il compenso che la vittima avrebbe presumibilmente richiesto per dare il suo consenso alla pubblicazione.

[74] G. PICA, *Diritto penale delle tecnologie informatiche*, 149 che analizza specificamente, in tale contesto, il significato della "ingiustizia" del profitto.

[75] Cfr. E. PALOMBI, G. PICA, *Diritto penale dell'economia e dell'impresa*, Vol.1, Torino, 1996, , 687 ss.; G. PICA, *ult.op.cit.*, 151.

[76] *Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, oggi *Article 323-1 code pénal*.

[77] Peraltro l'alterazione di dati è vista come aggravante speciale della norma di frode informatica, che però, così come è strutturata coincide sostanzialmente con la nostra fattispecie di accesso abusivo ad un sistema informatico, art. 615-ter.

[78] Cfr. G. FORTI, *L'ordinamento lessicale dei beni giuridici personali nella parte speciale del codice penale. Un'analisi quantitativo-strutturale sui codici di 20 paesi secondo la prospettiva delle "capacità"*, in L. PICOTTI (cur). *Tutela penale della persona e nuove tecnologie*, cit., 459.

manipolarla, dall'altro cercare gli attuali strumenti alternativi a tutela dell'identità digitale.

6. Ipotesi di "abuso dell'identità digitale" astrattamente tutelabili dalla novella

Tra le ipotesi che rientrano pacificamente nella frode informatica aggravata dal furto d'identità, il caso meno problematico riguarda il trasferimento di denaro dalla disponibilità della vittima a quella del reo[80], ad esempio utilizzando il "portafogli elettronico" della vittima su un portale di acquisti *online*, oppure abusando dell'account di *home banking* della vittima.[81]

Nella definizione di "danno" può certamente rientrare anche il "lucro cessante" e cioè il mancato guadagno cui la vittima va incontro in seguito alla frode informatica commessa con furto d'identità digitale. È indubbio che il concetto di "danno patrimoniale" vada mutuato dal campo civilistico, ed è proprio il codice civile (art. 1223) a parlare di danno indistintamente in termini di "perdita subita" o "mancato guadagno".[82]

Casi che rientrerebbero in tale ipotesi sarebbero, ad esempio, la sostituzione d'identità digitale commessa ai danni di un ente commerciale[83], al punto che questi subisca un danno alla propria immagine agli occhi del consumatore[84], o anche nei confronti di un lavoratore (dipendente o professionista) che ne subisca una ricaduta lavorativa negativa oppure, infine, nei confronti di un personaggio "pubblico"[85], la cui lesione all'immagine possa arrecargli un danno in termini di popolarità (e dunque di mancato guadagno nel caso si tratti di un cantante, attore, *blogger* o anche di un

---

[79] Cfr. i medesimi auspici in A. DI TULLIO D'ELISIIS,*Frode informatica commessa con sostituzione d'identità digitale: i profili applicativi,* cit.

[80] Sulla qualificazione di tale trasferimento illecito di denaro, cfr. R. BARTOLI, *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma*, cit., par. 2.

[81] Cfr. C. PECORELLA, *Le frodi informatiche*, in *Diritto penale dell'informatica*, cit., 103; tale condotta è stata oggetto di studio approfondito da parte della dottrina tedesca (cfr. K. TIEDMANN, *op.cit.*, *sub § 263a*) e svizzera (cfr. N. SCHMID, *op.cit.*, 238). Nonostante in dottrina c'è chi ritiene questo sia una "forma tecnologicamente evoluta di furto", cfr. P. CIPOLLA, *Social network, furto d'identità,* cit.*, par. 6.*

[82] Per la configurabilità del "lucro cessante" tra i danni patrimoniali causati dal reato di truffa cfr. Cass., sez. II, 11 settembre 2013, n. 37170, analogamente Cass., Sez. II, 23 ottobre 2009, n. 40790; Cass., sez. II, 05 marzo 2008, n. 10085, Cass., sez VI, 20 gennaio 1992, n. 470, rv. 188993.

[83] Cfr. i profili di diritto all'identità per gli enti collettivi, A. FUSARO, *Nome e identità personale degli enti collettivi. Dal "diritto" all'identità* uti singuli *al "diritto" all'identità* uti universi, NGCC 2002, Parte seconda, 51 ss.

[84] In merito alla configurabilità di un "lucro cessante" in seguito al reato di diffamazione. Cfr. Cass., sez. V, 02 febbraio 2010, n. 4424

[85] Cfr. il recente caso di cronaca in cui il profilo personale sul social network "*Twitter*" del blogger, imprenditore ed esponente politico Gianroberto Casaleggio ha subito un attacco informatico con una sostituzione d'identità digitale e la conseguente pubblicazione a nome della vittima di una serie di messaggi irriverenti o contro di sé. Cfr. R. MENICHINI, "*Chiudiamo il buco dell'ozono": il finto Casaleggio spopola sul web*, in *La Repubblica*, 27 febbraio 2014, http://www.repubblica.it/politica/2013/04/11/news/chiudiamo_il_buco_dell_ozono_il_finto_casaleggio_spopola_sul_web-56387456/

politico).[86] Non si nasconde, tuttavia, il grande problema in termini probatori nella dimostrazione di tale tipo di danno.

Un altro caso molto rilevante, inoltre, è il caso di accesso abusivo all'account di *home banking* della vittima o ad altri registri patrimoniali o di dati sensibili *online* da parte di un istituto di credito o assicurativo per riuscire a raccogliere informazioni sulla situazione patrimoniale (o altre informazioni economicamente rilevanti, come stato di salute, speranza di vita, ecc.), solvibilità e affidabilità economica del cliente o aspirante cliente.[87] Il danno economico si rinviene nella eventuale non erogazione del mutuo o nelle sue condizioni sfavorevoli o ancora negli alti premi assicurativi in sede di sottoscrizione della polizza (o addirittura nella non assicurabilità/bancabilità del cliente) e più in generale nella fortissima asimmetria informativa tra le parti.

Si consideri, inoltre, il caso (alquanto raro) in cui il soggetto subisca un furto d'identità con conseguente commissione di un reato da parte del reo che si finge la vittima. Qualora a ciò consegua una incriminazione a danno della vittima è indubbio che si possano configurare i profili di un danno patrimoniale (per sostenere le spese legali, ad esempio).[88]

Si noti, tuttavia, che per tutte le ipotesi sopra esposte il nesso cronologico tra la condotta e il danno appare alquanto tenue e ciò rende la problematica alquanto complessa, considerando che per la frode il profitto con altrui danno è momento consumativo del reato, in quanto elemento strutturale.[89]

Infine, è interessante soffermarsi sui risvolti di tutela della proprietà intellettuale su Internet. In effetti ci si può chiedere se integra la fattispecie di "frode informatica aggravata dal furto o indebito utilizzo d'identità digitale" l'ipotesi di una usurpazione delle opere d'ingegno realizzate dal soggetto su Internet, attraverso una propria pagina personale su un *social network* (c.d. *user-generated content*) oppure tramite un proprio sito web.

In effetti, il tema è particolarmente rilevante ai nostri fini poiché la proprietà intellettuale vive di un forte dualismo di tutela nel nostro ordinamento: da una parte tutela patrimoniale, dall'altra tutela dei diritti della personalità.[90] È un caso del tutto analogo a quello di frode informatica commessa con abuso d'identità digitale, per di più se si considera che anche in quel contesto incriminatorio la tutela della personalità è inserita solo incidentalmente come aggravante di un delitto patrimoniale, proprio come per il nostro nuovo furto d'identità.[91]

---

[86] Cfr. A. RICCI, *Il valore economico della reputazione nel mondo digitale. Prime considerazioni*, in Contratto e Impr., 2010, 1297.

[87] A. MURRAY, *Information Technology Law: The Law and Society*, Oxford, 2010, 464-465.

[88] Si tratta dell'ipotesi di calunnia indiretta, per cui cfr. P. CIPOLLA, *Social Network, furto d'identità e reati contro il patrimonio,* cit., nota 22 e par. 4*;* ID., *L'evoluzione giurisprudenziale in tema di calunnia diretta e indiretta* (nota a Trib. Camerino 13 ottobre 1994), in *Giur.merito*, 1995, 562 ss

[89] Vd. *Retro*, § 3; cfr. L. SCOPINARO, *Internet e reati contro il patrimonio,* cit., 93; G. PICA, *Diritto penale delle tecnologie informatiche,* cit., 144.

[90] R. FLOR, *Concezione dualistica dei diritti d'autore e tutela penale: quali prospettive per la rivalutazione della componente personalistica,* in L. PICOTTI (cur.), *Tutela penale della persona e nuove tecnologie*, cit., 77 ss.

[91] *Ibidem,* 90. Art. 171, comma 3. legge 22 aprile 1941 n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).

Per integrare tale ipotesi nella novella in commento, bisogna ora verificare i requisiti dell'"intervento senza diritto sui dati", del danno patrimoniale con un profitto per l'agente e di un effettivo abuso dell'identità digitale della vittima.

Che si tratti di un abuso dell'identità personale della vittima sembra facilmente dimostrabile, dal momento che si è ammesso che l'opera di ingegno *incarna delle parti di sé, il proprio pensiero, le proprie idee, i propri sentimenti*[92] si tratta in altre parole di una *manifestazione della personalità dell'individuo*[93] tale da far sorgere un interesse meritevole di tutela, al pari degli altri interessi della personalità.[94]

Affinché tale abuso possa riguardare anche l'"identità *digitale*" occorre che l'usurpazione avvenga a danno di una di quelle "forme creative che la persona sceglie come mezzo di proiezione di sé nella realtà virtuale.[95] Ed anzi forse la violazione del diritto d'autore come abuso dell'identità è più forte nel campo digitale[96], data l'opinione secondo cui i mezzi di manifestazione dell'io nel mondo di Internet sono già di per sé opere d'ingegno e in quanto tali, elementi interni/esterni al soggetto capaci di estrinsecare un interesse alla protezione non solo del *rappresentato*, ma anche della *rappresentazione* stessa.[97]

Per configurare l'"intervento senza diritto sui dati" occorre pur sempre che l'attività avvenga tramite un'alterazione dei normali procedimenti digitali, ovvero tramite un'azione di *hacheraggio*, accesso manipolativo ad un *account*, alterazione delle opere creative tramite, ad esempio, una modifica del nome dell'autore o la sostituzione del proprio nome al suo.[98]

Infine, per dimostrare la sussistenza di un danno patrimoniale occorre ricordare che un'usurpazione della proprietà intellettuale altrui riguarda anche (e soprattutto) diritti economici, laddove seppur nell'attuale normativa il requisito del danno patrimoniale non è richiesto, esso emerge implicitamente nella "riduzione di potenziali guadagni futuri" tramite le proprie opere d'ingegno.[99]

Tuttavia, laddove l'organizzazione "creativa" del proprio profilo su un *social network*, oppure i contenuti innovativi immessi nel proprio spazio web non siano finalizzati ad un'attività di guadagno futuro, sembra molto difficile dimostrare il danno

---

[92] Cfr. H. HANSMANN, M. SANTILLI, *Authors and Artists' Moral Rights: A Comparative Legal and Economic Analysis, 26 J.Legal Studies,* 1997, 95.

[93] B. VÖLZMANN STICKELBROCK, *Reichweite von Urheberrechten,* Berlin, 2009, 17 ss.

[94] cfr. R. FLOR, *ult.op.cit*., 101.

[95] Cfr. S. RODOTÀ, *Quattro paradigmi per l'identità*, in *Il diritto di avere diritti,* Bari, 2012, 298-310; cfr. anche G. RESTA, *Identità personale e identità digitale,* Dir.Informatica, fasc.3, 2007, 511 ss.; per un'attenta analisi sul valore giuridico dell'identità personale, da cui poter mutuare una definizione di identità digitale cfr. G. PINO, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003, 55 ss.

[96] R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata e in prospettiva europea ed internazionale*, Padova, 2010, 2 ss.

[97] Cfr. P. SAMUELSON, *Privacy as intellectual property?*, in *Stanford Law Review*, 52, 1125.

[98] Cfr. *Green Paper on Copyright and Related Rights in the Information Society* [COM(95) 382 final], 27 luglio 1995; *Libro Verde sulla distribuzione online di opere audiovisive nell'Unione europea - Verso un mercato unico del digitale: opportunità e sfide*, [COM(2011) 427 definitivo], 13 luglio 2011; R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata e in prospettiva europea ed internazionale,* cit.

[99] R. FLOR, *Concezione dualistica dei diritti d'autore e tutela penale: quali prospettive per la rivalutazione della componente personalistica,* cit., 82; P. MARCHETTI, L.C. UBERTAZZI, *Commentario breve alle leggi su proprietà intellettuale e concorrenza,* V ed., Padova, 2012, *sub* artt. 171-171-ter l.a.

patrimoniale subìto (solo in termini di *perdita di chance* di una pubblicazione originale fonte di lucro).

Dunque, la strada sicura per la dimostrazione di un pregiudizio al patrimonio può risiedere soltanto nella già esposta necessità di un ripensamento del concetto di "patrimonio". Da un lato insistendo sul termine "proprietà" (intellettuale) si potrebbe configurare l'opera creativa come una componente (immateriale) del patrimonio del soggetto[100]. Dall'altro, sembra ancora più forte la già esposta lettura francese della frode informatica, in termini di lesione patrimoniale ad un "bene informatico" (inteso come insieme di dati in un sistema automatizzato).[101]

Tuttavia, come più volte ricordato, un'interpretazione del genere si scontra con i principi di legalità del sistema penale e dunque, salvo la dimostrazione di un effettivo mancato guadagno per la vittima, non sembra che possa parlarsi di frode informatica aggravata (ai sensi dell'art. 640-*ter*, 3° comma c.p.) in ogni ipotesi di usurpazione delle espressioni creative dell'identità digitale della vittima.

Questione simile è quella dello sfruttamento dell'identità digitale altrui per ottenerne vantaggi (perlopiù commerciali). È il caso dell'abuso dell'*account* digitale della vittima per ottenere (anche tramite conversazioni *online*) informazioni riservate, omaggi, benefici sociali. È indubbio che tali utilità siano comunque un mancato guadagno per la vittima qualora abbiano un valore economico. Qualora invece non si tratti di un valore economico è difficile configurare un danno, salvo estendere (pericolosamente) l'*acquis* in tema di sfruttamento non autorizzato dell'immagine altrui in ambito giurisprudenziale civilistico. In questa materia, infatti, la giurisprudenza della Cassazione Civile ha riconosciuto che nonostante non ci sia un effettivo detrimento del patrimonio della vittima, ciò non toglie che possano configurarsi dei "danni patrimoniali" in termini di "perdita dei vantaggi economici che avrebbe potuto conseguire se - essendogli stato chiesto il consenso alla pubblicazione - avesse potuto negoziarne la concessione e chiedere per essa un compenso".[102]

7. Soluzioni alternative de iure condito di tutela dell'identità digitale

Consci dunque dei limiti (e dei rischi) di una interpretazione estensiva della novella in commento, occorre ora scrutare gli eventuali elementi alternativi nel nostro ordinamento penalistico a tutela dell'identità digitale. In altre parole, bisogna rilevare se di vero "vuoto normativo" si tratta o se altrimenti l'identità personale in rete è ben tutelabile (nella sua complessità valoriale sopra descritta) dalle fattispecie incriminatrici tradizionali del nostro ordinamento.

[100] C. GEIGER, *Copyright's fundamental rights dimension at EU level*, in E. DERCLAYE (ed.), *Research Handbook on the Future of EU Copyright*, Edward Elgar, 2009, 27 ss.

[101] Vd. *Retro.* Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, oggi Article 323-1 code pénal, "*Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende*".

[102] Cass. civ., sez. III, sentenza 16 maggio 2008 n° 12433, in *Danno e Resp.*, 12/2008.

7.1. La sostituzione di persona

Di sicuro la norma più usata a protezione dell'identità personale digitale fino ad oggi è stata la sostituzione di persona *ex* art. 494 c.p.[103]
Tuttavia, non poche sono le perplessità riguardo all'adeguatezza di tale norma (concepita nel codice Rocco a tutela della "fede pubblica"[104]) a sanzionare tutti i casi di lesione del diritto all'identità digitale che non siano accompagnati da un profitto economico dell'agente, come ha esplicitato la Suprema Corte nel suo disagio ad estendere una norma concepita per tutt'altro contesto.[105] Del resto, se bastasse una semplice traslazione applicativa della fattispecie tradizionale nel mondo informatico, non si capirebbe come mai il legislatore penale francese abbia sentito la necessità di un'estensione esplicita del reato di usurpazione d'identità "*se è commesso su una rete* online *di comunicazione al pubblico"*[106].
Inoltre, il reato di sostituzione di persona, presentandosi come fattispecie residuale e con una pena irrisoria (fino ad un anno di reclusione), non pare cogliere la gravità di una lesione all'identità digitale nel mondo in cui i *social network* e il web 2.0 in generale hanno assunto un ruolo sempre più pervasivo.[107] Non pare cogliere, d'altro canto, neppure la facilità con cui è possibile rubare o duplicare l'identità altrui tramite le tecnologie informatiche: la "nebulizzazione" delle infrastrutture nel mondo di internet, permette di sostituirsi ad un'altra persona semplicemente inserendo un nome utente ed una *password*, senza alcuno ulteriore sforzo simulatorio. In altri termini, l'aumento esponenziale di un pericolo non è corrisposto ad oggi da una reazione adeguata dell'ordinamento.
Inoltre, non si può nascondere il grave problema strutturale di tale norma nel proteggere l'identità personale (e digitale) dal momento che, a differenza della norma francese suesposta, nel suo difendere la "fede pubblica" tutela chi cade in errore, non chi è espropriato dell'identità: la condotta centrale è "indurre taluno in errore" e non già "usurpare l'identità", al punto che la "vittima" è l'ingannato piuttosto che la vittima

[103] Cass., sez. V, 28 novembre 2012, n. 18826, cit., cfr. in merito E. MENGONI, *Chattare con un nickname riconducibile ad altri (e comunicare il loro numero telefonico) integra il reato di sostituzione di persona* , in Cassazione Penale, fasc.1, 2014, 148; Trib. Bari, sez. Molfetta, 18 febbraio-20 maggio 2003, Giudice Del Castello, in *Dir. e Giust*., n. 23, 14 giugno 2003; Cass., sez. III, 15 febbraio 2005, n. 5728, in *Dir.inf.*, 2005, 499, con nota di A. DI RONZO); Cass., sez. V, 14 dicembre 2007, n. 46674 in *www.altalex.it*; cfr. anche C.FLICK, *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, Dir. informatica, fasc.4-5, 2008, 526.

[104] Cfr. *ex multis* R. CAPPITELLI, *La sostituzione di persona nel diritto penale italiano*, in Cass.pen. 2005, 1269, 2993 ss.

[105] Cass., sez. V, 29 aprile 2013, n. 18826, cit., per cui "i profondi e, per certi versi, rivoluzionari cambiamenti che l'evoluzione tecnologica ha prodotto attraverso l'affermarsi delle nuove tecnologie informatiche, che, grazie alla nota rete telematica internet, consentono una diffusione di informazioni e possibilità di comunicazione diretta tra gli utenti pressoché illimitate, hanno dispiegato i loro effetti (...) anche in materia penale, ponendo molteplici problemi, tra i quali di non poco momento appaiono quelli sottesi ad un'*attività di interpretazione estensiva che, in assenza di organici interventi legislativi, consenta di adeguare l'ambito di operatività delle tradizionali fattispecie di reato, come quella di cui all'art. 494 c.p., alle nuove forme di aggressione per via telematica dei beni giuridici oggetto di protezione, senza violare i principi della tassatività della fattispecie legale e del divieto di interpretazione analogica delle norme penali*".

[106] Article 226-4-1, comma 2, code pénal: "*lorsqu'elle est commise sur un réseau de communication au public en ligne*"".

[107] P. CIPOLLA, *Social Network, furto d'identità e reati contro il patrimonio,* cit*., passim.*

dell'usurpazione d'identità[108], nonostante la Cassazione abbia riveduto fortemente tale idea.[109]

*7.2. La riservatezza informatica: l'art. 167 cod. privacy e l'art. 615-*ter *c.p.*

Per altro verso, il trattamento illecito di dati ai sensi dell'art. 167 della disciplina sul trattamento dei dati personali, se pare coprire la maggior parte delle lesioni all'identità digitale, non risulta applicabile ai casi di creazione di un profilo a nome altrui, laddove si utilizzino esclusivamente dati presenti in pubblici registri (come nome, cognome, *ex* art. 24 codice privacy).[110]
Infine, l'accesso abusivo ad un sistema informatico *ex* art. 615-*ter* c.p.[111], per quanto tuteli un bene della personam, inserito com'è nei delitti contro l'inviolabilità del domicilio, non sembra cogliere la complessità del diritto all'identità digitale, anticipando soltanto la tutela al momento dell'accesso non autorizzato.
Per vero, tale assunto non è pacifico, dal momento che autorevole dottrina ritiene che tale reato sia stato pensato per la tutela dell'integrità dei dati e dei programmi informatici, che risulta messa in pericolo dalle intrusioni abusive ad un sistema informatico.[112] E ciò permette di introdurre nel raggio applicativo della norma i sistemi informatici privi di qualsiasi tipo di contenuto privato o personalistico.[113] Tuttavia, per superare i problemi di concorso di norme tra il delitto di accesso abusivo ad un sistema informatico così interpretato e i reati in materia di danneggiamento informatico si è preferito identificare il bene giuridico nella riservatezza dei dati e dei programmi in un sistema informatico.[114]
Tuttavia, la fattispecie non fa alcun cenno al contenuto dei sistemi informatici ed è per questo che avveduta dottrina, per riassumere e far progredire il dibattito, ha proposto come bene giuridico tipico tutelato dalla norma la "riservatezza informatica".[115]
Un bene che ingloba tanto la riservatezza domiciliare quanto quella personale, interseca la tutela del segreto e dei dati personali, ma si esplica nella protezione dell'esclusività

---

[108] R. FLOR, *Phishing, Identity Theft e Identity Abuse. Le prospettive applicative nel diritto penale vigente*, *in Riv. it. dir. e proc. pen*., fasc.2-3, 2007, 899 ss., par. 4.1.

[109] Cass., sez. V, 29 aprile 2013, n. 18826, cit. che ha affermato che la norma ha "natura plurioffensiva, in quanto preordinata non solo alla tutela di interessi pubblici, ma anche di quelli del soggetto privato nella cui sfera giuridica l'atto sia destinato ad incidere concretamente, con la conseguenza che quest'ultimo riveste la qualità di persona offesa dal reato". Cfr. anche, *ex multis*, Cass., sez. V, 2 marzo 2009, n. 21574, rv. 243884; Cass., sez. V, 09 dicembre 2008, n. 7187, rv. 243154; Cass., SSUU, 25 ottobre 2007, n. 237855, Pasquini.

[110] Come ha dichiarato Cass., sez. III, 15 febbraio 2005, n. 5728, cit.

[111] Introdotto dall'Articolo 4, L. 23 dicembre 1993, n. 547.

[112] M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica del diritto*, fasc. 4, 1994, 12 ss.

[113] C. PECORELLA, *Il diritto penale dell'informatica*, cit., 316; F. PAZIENZA, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, RIDPP, 1995, 750 ss.; L. PICOTTI, *Sistematica dei reati informatici*, cit., 80; F. MANTOVANI, *Diritto penale, Delitti contro il patrimonio*, Padova, 2013, 522.

[114] C. PECORELLA, *ult.op.cit*., cit. 321-322.

[115] L. PICOTTI, *Sistematica dei reati informatici*, cit., 78; ID., *Studi di diritto penale* dell'informatica, Verona, 1992,108; D. PETRINI, *La responsabilità penale per i reati via Internet*, Napoli, 2004, 43 ss; F. MANTOVANI, *Diritto penale, Delitti contro il patrimonio*, Padova, 2013, 502; in giurisprudenza, Cass.pen., sez. V, 20 marzo 2007, 11687.

dell'accesso ad uno *spatium operandi et deliberandi* virtuale, anche se vuoto o con dati di pubblico dominio.[116]
Tale bene giuridico, sembra particolarmente interessante ai fini di una protezione matura dell'identità digitale. In effetti tale spazio virtuale è il luogo "naturale" in cui l'identità digitale si esplica ed anzi coincide con l'intima concretizzazione di quella stessa identità (si sta parlando dell'*account* o profilo personale su un sito web).
Tuttavia, tale fattispecie sanziona soltanto la violazione di "forme di proiezione dell'identità personale in rete" già esistenti, ma non riesce a proteggere l'identità personale da un suo abuso creativo in rete. In altri termini, l'art. 615-*ter* c.p. non punisce le ipotesi di creazione *ex novo* di un *account* internet a nome altrui, ma solo le intrusioni e gli utilizzi di un *account* già esistente.

7.3. Calunnia indiretta

Infine, per i casi in cui la sostituzione d'identità digitale sia strumentale alla commissione di un reato, ci si chiede se ciò possa integrare il reato di calunnia indiretta o implicita *ex* art. 368 c.p., in quanto si "simulano a carico di" un altro soggetto "le tracce di un reato", ovvero si creano indizi idonei a far convogliare una azione penale infondata su persona di cui si conosce l'innocenza.[117]
Ovviamente, pur restando sempre nell'ambito delle "falsità personali" (stavolta a danno dell'amministrazione della giustizia) la soluzione non è così immediata, dal momento che non c'è ancora una giurisprudenza favorevole all'applicazione del 368 c.p. nei casi di sostituzione di persone, tuttavia si è ritenuto in dottrina una pacifica applicabilità di tale fattispecie alle ipotesi in commento.[118]

7.4. Diffamazione

Da ultimo, è interessante prestare attenzione al rapporto tra sostituzione d'identità digitale e diffamazione. La giurisprudenza ha ritenuto applicabile il reato di diffamazione *ex* art. 595 c.p. qualora alla sostituzione d'identità segua una lesione della reputazione della vittima. [119] In effetti, trattandosi di un reato evento in senso

---

[116] I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, cit., 149-153.

[117] P. CIPOLLA, *Social Network, furto d'identità e reati contro il patrimonio*, cit., nt. 22.

[118] *Ibidem*, par. 4*;* P. CIPOLLA, *L'evoluzione giurisprudenziale in tema di calunnia diretta e indiretta* (nota a Trib. Camerino 13 ottobre 1994), in *Giur.merito*, 1995, 562 ss. in cui si evidenzia come la calunnia reale o indiretta è ravvisabile anche in presenza di "condotte difformi rispetto a quelle consolidate nella tradizionale casistica" . Pertanto, non è apparso difficile all'autore una incolpazione per calunnia (indiretta) a danno di soggetto che commetta reati utilizzando le generalità di persona vivente, trattandosi di condotta necessariamente idonea a indirizzare sospetti di reità a carico del soggetto di cui il reo abbia assunto l'identità.

[119] Cfr. Trib. Trani, 18 febbraio 2003, in Cass. Pen., fasc. 12, 2003, 3963, con nota di F. GIUSEPPE *Diffamazione telematica attraverso la decontestualizzazione dell'identità*; Trib. Bari, sez. Molfetta, 20 maggio 2003, in *Dir. e giust*., fasc.23, 2003, pag. 88, con nota di M. FUMO. I due casi qui citati sono identici: un soggetto aveva costituito un sito web a nome della ex fidanzata, caricando immagini pornografiche e numero di telefono della vittima e messaggi a suo nome, invitando a contattare il numero per telefonate erotiche. Si noti che nessuno dei due giudici ha valutato l'evenienza del reato di sostituzione di persona (anche per le difficoltà probatorie a ricondurre la creazione del sito al soggetto imputato, cfr. al riguardo C. ARMONA, *La diffamazione a mezzo Internet: prove di maquillage (nella*

naturalistico[120], qualsiasi mezzo usato per la "offesa" della reputazione della vittima integra il reato, per di più aggravato dalla circostanza di "un mezzo di pubblicità" (art. 595, 3° comma, c.p.).[121]
Si è notato, tuttavia, che la lesione alla reputazione non coincide perfettamente con quella all'identità digitale. In effetti, pur basandosi entrambe su diritti della personalità, l'identità attiene solo al "momento gnoseologico" del rapporto di un soggetto con gli altri, mentre la reputazione attiene al "momento critico"[122], in cui si trae un giudizio positivo o negativo. In altre parole, si è sottolineato come il momento offensivo dell'identità risieda nella falsa rappresentazione del soggetto, (un'offesa alla "verità", ad un diritto ad essere se stessi), mentre quello della reputazione riguardi il "valore" attivo della persona (una offesa alla dignità delle sue relazioni sociali).[123]
Tuttavia, è innegabile il profondo legame sussistente tra i due beni giuridici in questione. Ne è dimostrazione la più volte citata norma che tutela l'identità personale (e digitale) nel codice penale francese, poiché nella descrizione del fatto tipico menziona il dolo specifico di "minare la reputazione" della vittima.[124]

8. Concorso di reati

Ci si potrebbe allora domandare se un'adeguata risposta sanzionatoria possa provenire dal concorso di reati, ad esempio dal concorso tra la nuova frode informatica aggravata e i reati appena analizzati.

Del resto, la presa d'atto che la frode informatica aggravata si muova negli stretti margini patrimonialistici e la peculiarità dei requisiti richiesti dalla fattispecie rispetto alle altre ipotesi sopra analizzate porta ad escludere qualsiasi caso di assorbimento tra fattispecie[125].

XIII legislatura), in Riv.trim.dir.pen.econ., 2001, 636 ss.), né quello di trattamento illecito di dati *ex* codice privacy, con non poche perplessità dei commentatori. Cfr. M. FUMO, *ult.op.cit.*, 88 ss.

[120] Come chiarito definitivamente da Cass., sez. I, 26 maggio 2004, n.31563, in *Cass. pen.*, fasc. 3, 2006, 929, con nota di N. MADIA, *La Corte di Cassazione ribadisce l'appartenenza del delitto di diffamazione alla classe dei reati con evento naturalistico*, ma la conferma riguardo alla diffamazione compiuta tramite internet è già in Cass., 17 novembre 2000, in *Cass. Pen.*, 2001, 1835 e ripresa da Trib. Trani, 18 febbraio 2003, cit.

[121] Trib. Trani, 18 febbraio 2003, cit.; Trib. Bari, sez. Molfetta, 20 maggio 2003.

[122] Pret. Roma, ordinanza 6 febbraio 1990 (Maiorca - Soc. Gaumont) in G. CASSANO, *La tutela della reputazione. Lineamenti dei diritti della personalità. Giurisprudenza. Materiali*, Piacenza, 2002, 115; cfr. E. MUSCO, *Bene giuridico e tutela dell'onore*, 1974, Milano, 145 ss.

[123] F. GIUSEPPE *Diffamazione telematica attraverso la decontestualizzazione dell'identità*, cit., par. 2.

[124] Oltre che il suo onore, e la sua tranquillità. Art. 226-4-1, *code pénal*.

[125] Si tratterà infatti di tutti casi di specialità bilaterale: quanto al concorso con la sostituzione di persona, l'art. 494 c.p. prevede il dolo specifico di danno o profitto, mentre l'art. 640-*ter* c.p. prevede come elementi strutturali il conseguimento di un "ingiusto profitto con altrui danno"; quanto al concorso con l'accesso abusivo ad un sistema informatico, l'art. 640-*ter* c.p. prevede la verificazione dell'ingiusto profitto con altrui danno, mentre il 615-*ter* c.p. prevede che il sistema sia sottoposto a "misure di sicurezza", quanto al concorso col trattamento illecito di dati, nella frode informatica l'ingiusto profitto con altrui danno è elemento costitutivo, mentre nel trattamento illecito è richiesto il dolo specifico di vantaggio o danno e il "nocumento" è solo una condizione obbiettiva di punibilità. È vero però che l'art. 167 cod.privacy presenta una clausola di riserva, ovvero "quando il fatto non costituisca più grave reato".La dottrina ha ritenuto che tale clausola escluda il concorso di reati ogni qual volta la violazione della norma in oggetto costituisce esclusivamente una modalità di commissione di altro e più grave reato

Pertanto, si tratterà sempre di un concorso materiale, con la specificazione che, se le condotte si susseguono con un medesimo disegno criminoso, la pena è calcolata con il cumulo giuridico, *ex* art. 81 c.p. e dunque andrà dai 2 anni (minimo edittale dell'art. 640-*ter*, 3° comma c.p.) ai 18 anni (i 6 anni massimi *ex* art. 640-*ter*, 3° comma c.p. aumentati del triplo).

Ed è altrettanto vero che le ipotesi di concorso, nell'ambito di una fattispecie così complessa come quella della frode informatica commessa con sostituzione d'identità digitale, sono frequentissime, al punto da poter configurare quasi in ogni caso un trattamento illecito di dati (*ex* art. 167 cod.privacy) e un accesso abusivo ad un sistema informatico (*ex* art. 615-*ter* c.p.).

Tre sono dunque i punti problematici che è necessario rilevare:

1.la confusione dei beni giuridici formalmente protetti, in contrasto con l'unico bene di cui qui si è cercata protezione, ossia l'identità personale digitale;[126]

2.l'eccesso sanzionatorio (fino a 18 anni di reclusione) che tale confusione comporta per un reato apparentemente non così offensivo,[127] anche considerando che in altri ordinamenti in cui è tutelata specificamente l'identità digitale, come quello francese[128] la pena è di tre anni di reclusione;

3.l'eccessivo potere discrezionale lasciato ai giudici in questa confusione normativa, al punto da prevedere margini edittali che vanno dai 2 ai 18 anni, con la possibilità di configurare o escludere svariate ipotesi di concorso di reato.

9. Conclusioni

La recente introduzione, nel nostro ordinamento, della fattispecie di "furto d'identità digitale" può dunque essere un'occasione feconda per una riflessione radicale sul ruolo del diritto penale dell'informatica: tutelare soltanto il patrimonio degli utenti delle tecnologie informatiche o spingersi coraggiosamente verso una tutela della proiezione digitale dell'identità umana.

Una volta appurato, del resto, che le fattispecie incriminatrici tradizionali non riescono a cogliere la peculiarità del fenomeno in esame, né singolarmente considerate né in concorso con la nuova frode informatica aggravata, non resta che sperare in una soluzione a questo vuoto di tutela.

D'altro canto, il goffo tentativo di racchiudere il fenomeno della criminalità informatica nelle strette maglie dei delitti contro il patrimonio è foriero di uno scatto di

---

"cioè, ad esempio, quando costituisca il mezzo per la commissione di una truffa o di un abuso in atti d'ufficio" (cfr. V. DESTITO, *Dati personali (tutela penale dei)*, (I agg.), *Digesto Online*, 2008; M.C. BISACCI, *Tutela penale dei dati personali*, *Digesto Online*, 2005). Al contrario, la giurisprudenza ha richiesto per l'assorbimento del reato di trattamento illecito di dati nella fattispecie "più grave" che i due reati siano a tutela dello stesso bene giuridico, escludendo dunque nell'ipotesi in commento tale assorbimento (Cass., sez. II, 07 maggio 2013, n. 36365, rv. 256877; *CED;* Cass. Civ., 11 aprile 1986, in *Resp. Civ. e Prev*., 1987, 85 con nota di P. ZAGNONI BONILINI. In tal caso, dunque, si tratterebbe ancora una volta di un concorso formale e dunque di un cumulo giuridico della pena.

[126] Cfr. L. PICOTTI, *Sistematica dei reati informatici*, cit., 21 ss.

[127] Anche considerando il necessario calcolo matematico delle pene, cfr. R.v. JHERING, *Der Zweck im Recht*, 1877/1883, trad.it. M.G. LOSANO, *Lo scopo nel diritto*, Torino, 1972 per cui "la pena ha lo stesso significato del prezzo nel mondo dei traffici" e "ponendo da un lato i beni sociali e dall'altro le pene, si ottiene la scala dei valori di una società".

[128] Art. 323-1 *code pénal*.

lungimiranza già al livello interpretativo: nel mondo del c.d. "oro digitale"[129] (i dati personali) è forse giunto il momento di riconsiderare il concetto stesso di "patrimonio", oppure, più realisticamente seguendo l'esempio d'Oltralpe, considerare i "dati informatici" come "beni" e dunque parte di quel patrimonio economico così severamente protetto dal nostro ordinamento penalistico.

[129] A. FURLANI, F. LUTMAN, *Social innovation. Reti sociali: le nuove protagoniste dell'innovazione. Una guida pratica per le aziende italiane,* Milano, 2012, 111; P. CIPOLLA, *Social Network, furto d'identità e reati contro il patrimonio,* cit, § 7.

NELLA BAIA DEI PIRATI:
L'ARREMBAGGIO AL DIRITTO D'AUTORE SU INTERNET

Valeria Spinosa

1. Diritto penale e pirateria informatica: *The Pirate Bay*

Con la comparsa su Internet di peculiari tecnologie telematiche (*peer to peer, streaming, cloud computing, social network*) le modalità di comunicazione delle opere dell'ingegno si sono moltiplicate e, allo stesso tempo, sono aumentate esponenzialmente le forme di violazione dei diritti di autore connessi a tali contenuti.

In particolare, sono da sottolineare due linee direttrici nuove della violazione dei diritti di autore per mezzo degli strumenti telematici più innovativi: da una parte, la rilevanza economica gigantesca dello sfruttamento abusivo di opere protette altrui; dall'altra parte, la dimensione transnazionale, per non dire globale, di siffatto fenomeno criminoso.

I rapporti tra diritto penale e pirateria informatica sono oggetto di un dibattito assai presente nella prassi dei tribunali non solo nazionali, ma anche europei. Il caso di maggior rilevanza ha riguardato il sito *The Pirate Bay*, che ha portato a pronunciarsi sia la Corte di Strasburgo sia la Cassazione.

In questo caso è possibile apprezzare entrambe le peculiarità che contraddistinguono la pirateria virtuale odierna, vale a dire sia la notevole entità del giro di affari collegato alle violazioni del diritto d'autore, sia la portata mondiale di tale industria illegale dell'intrattenimento, ramificata in ogni angolo del pianeta.

In sostanza, nella "baia dei pirati" oggetto degli accertamenti, vale a dire sul sito *The Pirate Bay* (www.thepiratebay.se) si assisteva a un vero e proprio saccheggio telematico, a livello mondiale, di opere protette da *copyright*, grazie alla tecnologia *peer to peer*, in cui non vi è un server centrale da cui scaricare i *file*, bensì più nodi paritari costituiti dai computer degli utenti stessi, i quali compiono *download* e *upload* simultaneamente.

The Pirate Bay, sito registrato in Svezia, è stato in primo luogo condannato nella persona dei suoi rappresentanti legali da un tribunale penale svedese per illecita condivisione di opere virtuali protette e gli imputati hanno presentato ricorso alla Corte europea dei diritti umani avverso tale condanna, affermando che essa contrastava con il diritto all'informazione come previsto dall'art. 10 della Convenzione europea dei diritti dell'uomo e come interpretato secondo la giurisprudenza di Strasburgo.

La Corte sovranazionale [1], tuttavia, respinse il ricorso in oggetto, sostenendo recisamente che la repressione penale delle violazioni del diritto d'autore *online* non

[1] Corte eur. dir. uomo, sez. V, 13 marzo 2013, n. 40397/12, Neij e Sunde Kolmisoppi c. Svezia, in *Cass. pen.*, 2013, n. 10, 3371 ss., con nota di E. DI AGOSTA, *Il caso* Pirate Bay *arriva alla Cedu: spunti*

rappresentano un'ingerenza né illecita né sproporzionata dei poteri statuali nel godimento delle libertà di espressione e di comunicazione nello spazio virtuale, in quanto in questo caso prevalgono gli interessi sottesi alla tutela del *copyright* e delle opere protette.

2. L'esperienza del sistema italiano

Anche in Italia vi sono stati degli strascichi della complessa vicenda giudiziale del sito *The Pirate Bay*: il Giudice per le indagini preliminari di Bergamo, infatti, nel 2008 ha disposto il sequestro preventivo di tale sito ai sensi dell'art. 321 c.p.p. ed ha ritenuto la propria giurisdizione *ex* art. 6 c.p. sulla base del fatto che parte della condotta tipica (nel dettaglio, plurime azioni di *upload* e *dowload* di utenti privati italiani) era stata commessa sul territorio nazionale, a nulla valendo l'argomento difensivo della nazionalità svedese dell'*internet service provider*.

In aggiunta, la decisione del G.i.p. di Bergamo si segnala sul piano processual-penalistico per il suo originale contenuto ablativo; per dirlo meglio, il provvedimento si componeva, da un lato, di un "ordinario" sequestro preventivo, caratterizzato dalla natura in parte reale (i server, i computer e comunque tutto *l'hardware* impiegato per la gestione del sito *The Pirate Bay*) e in parte immateriale del suo oggetto (la pagina web stessa e tutti i link ad essa riferibili).

Dall'altro lato, al sequestro con effetto di oscuramento del sito si accompagnava l'ordine, rivolto a tutti i *provider,* che svolgono la loro attività in Italia, di inibire ai loro utenti l'accesso e la connessione al sito *The Pirate Bay*, un provvedimento giudiziale a contenuto inibitorio che trova il proprio fondamento normativo negli artt. 14 - 16 del d.lgs. 70/2003 sul commercio elettronico.

Alla Corte di Cassazione era giunta la doglianza degli imputati avverso questo sequestro *sui generis*, poiché essi sostenevano che si trattasse di una misura cautelare anomala, inesistente nel c.p.p. e quindi in aperta violazione del principio di legalità.

Come nel caso sottoposto alla Corte di Strasburgo, così nel ricorso cautelare alla Cassazione italiana *The Pirate Bay* vede respinto il proprio ricorso, con la conferma del provvedimento del G.i.p. di Bergamo, ritenuto conforme al catalogo tassativo di provvedimenti cautelari, in quanto il sequestro preventivo, mirando a sottrarre la cosa pericolosa all'imputato per impedirgli di utilizzarla ulteriormente, ha già in sé un implicito contenuto inibitorio, che l'ordine impartito ai *provider* italiani non fa che esplicitare.

Passando ai profili di diritto sostanziale, il processo giunto all'attenzione della Corte di Cassazione[2] aveva ad oggetto la responsabilità ai sensi dell'art. 171 *ter* comma 2 lett. A *bis* della legge sul diritto d'autore (l. 633/1941 e s.m., d'ora in poi l. aut.); la norma incriminatrice in esame è stata introdotta nella l. aut. da una novella del d.l. 72/2004 e rivisitata poco dopo dal d.l. n. 7/2005 per colpire le condotte di condivisione *online* di contenuti protetti, attraverso la penalizzazione dell'immissione con comunicazione al pubblico a scopo di lucro.

È evidente che perseguire i singoli utenti che avevano condiviso i file protetti sarebbe stato impossibile, trattandosi di milioni di indirizzi IP. La soluzione prescelta

---

per una riflessione sulla responsabilità degli internet service provider, *tra libertà d'espressione e reati in materia di* copyright, *ibidem*, 3375 ss.;

[2] Cass., sez. III, 29 settembre 2009, n. 49437, *Foro it.* 2010, II, c. 136, con nota di G. DI PAOLA;

sia in Svezia sia in Italia è stata quella di punire non i privati, bensì il *provider* che li aveva messi in contatto.

3. Osservazioni critiche

Emerge così la questione centrale del caso *The Pirate Bay:* lo statuto penale del *provider* in materia di violazioni del diritto d'autore su Internet.

La dottrina e la giurisprudenza hanno vagliato diversi percorsi interpretativi, quali la responsabilità del direttore di giornale[3], il reato omissivo improprio[4], il concorso *ex* art. 110 c.p.[5].

Bisogna spendere alcune parole sui tentativi di ricostruire una posizione di garanzia in capo all'*Internet service provider (ISP)* in modo da configurare una loro responsabilità *ex* art. 40, cpv. c.p. per il mancato impedimento della commissione di reati in materia di diritto d'autore da parte dei propri utenti iscritti.

Le strade percorse in tale direzione sono diverse: alcuni hanno sostenuto che l'attività del *provider* sarebbe pericolosa e da ciò discenderebbe una loro posizione di garanzia, cioè di controllo della fonte di rischio[6]; altri, pur prendendo in considerazione l'opzione interpretativa dell'art. 40, comma 2 c.p., la escludono per l'inesigibilità in concreto dell'adempimento dell'obbligo di controllo, sulla falsariga di una disposizione analoga nell'ordinamento tedesco[7]; infine, vi è chi[8] suggerisce di ricavare una posizione di garanzia speciale e *ad hoc* dall'obbligo di porre fine alle violazioni del diritto d'autore a seguito di provvedimento dell'autorità giudiziaria, come previsto dagli artt. 156 e 156 *bis* l. aut.[9].

L'ultima delle soluzioni proposte, sebbene fornisca un esplicito appiglio normativo, ci pare da respingere per due ordini di motivi: prima di tutto, il d.lgs. 70/2003 all'art. 17 sancisce l'assenza di un obbligo giuridico di impedimento dei reati in capo ai *provider*, quando esclude in ogni caso il dovere di controllo preventivo e generalizzato sui dati da essi trasmessi o registrati, a prescindere dalla qualifica di *access*, *caching* o *host provider*, in ossequio al principio della cd. *net neutrality*; sul piano strettamente

---

[3] S. SEMINARA, *La responsabilità penale degli operatori su Internet, Dir. inf.,* 1998, 759 ss., nonché cfr. *retro* l'intervento precedente del dott. Bassini contrario all'estensione analogica della disciplina penale sulla stampa all'ISP, perché si tratterebbe di un'interpretazione *in malam partem.*

[4] L. PICOTTI, *La responsabilità penale dei* service providers *in Italia, Dir. pen. proc.*, 1999, 501 ss.;

[5] C. PARODI – A. CALICE, *Responsabilità penali e Internet - Le ipotesi di responsabilità penale nell'uso dell'informatica e della telematica*, Milano, 2001, 128 ss.; L. PERDONÒ, *Le responsabilità penali collegate all'uso di Internet fra comparazione e prospettive di riforma*, *Dir. inf.*, 2007, 323; E. DI AGOSTA, *Il caso* Pirate Bay *arriva alla Cedu: spunti per una riflessione sulla responsabilità degli* internet service provider, *tra libertà d'espressione e reati in materia di* copyright, *Cass. pen.*, 2013, n. 10, 3375;

[6] F. SGUBBI, *Parere pro veritate*, *Dir. inf.*, 2009, 746 ss.;

[7] Si tratta della legge federale sui servizi telematici (*Gesetz über die Nutzung von Telediensten, Teledienstegesetz* - TDG) del 27 luglio 1997, che ha introdotto nell'ordinamento tedesco alcune norme che riguardano specificamente la responsabilità dei provider e degli operatori in internet, contenute precisamente nel § 5 della legge in discorso. Sul tema rimandiamo a F. RESTA, *La responsabilità penale del provider: tra* «laissez faire» *ed obblighi di controllo, Giur. merito*, 2004, 1715 ss.;

[8] R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010, 458;

[9] Peraltro, aderendo alla posizione sopra esposta, la posizione di garanzia del provider sarebbe limitata all'impedimento dei soli reati previsti dagli artt. 171 – 171 *novies* l. aut., senza possibilità di estendere per tale via la responsabilità dell'ISP per reato omissivo improprio ad altri reati informatici propri o impropri.

penalistico, poi, gli artt. 156 e 156 *bis* l. aut. fissano un obbligo di attivazione che sorge a carico dell'ISP dopo la commissione di un reato, mentre è noto che le posizioni di garanzia e il correlativo obbligo di impedimento dell'evento devono preesistere al reato, altrimenti saremmo di fronte a meri obblighi di attivarsi[10].

Per queste ragioni, la tesi del concorso di persone nel reato *ex* art. 110 c.p. ci pare la migliore, a condizione di non dilatare i confini del contributo concorsuale atipico del *provider*; due sono soprattutto i rischi che paventiamo nella prassi giurisprudenziale: la lettura estensiva del criterio condizionalistico per quanto riguarda l'elemento obiettivo e l'impiego disinvolto del dolo eventuale sul piano soggettivo.

A nostro modesto avviso su questo versante persino la decisione della Cassazione nel caso *The Pirate Bay* mostra qualche ambiguità, nella misura in cui vi si afferma che l'indicizzazione delle opere condivise in *peer to peer* segnasse la soglia di rilevanza penale della condotta del *provider,* non considerando però la circostanza che il database fosse destinato a tutti i *file*, protetti e no, proprio per la natura "neutrale" delle attività del *provider* su Internet[11].

Ciononostante, la presenza di un indice delle opere condivise *online* è stata ritenuta dalla Corte di legittimità un'agevolazione causalmente efficiente rispetto alla commissione del delitto di cui all'art. 171 *ter*, comma 2, lett. A *bis* l. aut. da parte dei singoli autori delle condotte di *upload* e *download* simultaneo.

L'aspetto decisivo nella vicenda *sub judice* tuttavia, a nostro avviso, non è consistito tanto nell'indicizzazione delle opere per agevolarne la ricerca da parte dei "pirati della rete", quanto nel conseguimento di un ingente profitto da parte del sito *The Pirate Bay* dalle inserzioni pubblicitarie, che connotava una fiorente industria fondata sullo scambio abusivo di contenuti protetti.

In altre parole, la prova del dolo specifico di lucro, richiesto dal delitto di immissione con comunicazione al pubblico di contenuti protetti da diritto d'autore, è stata raggiunta tramite un accertamento *ex post,* ovvero valutando l'entità degli introiti pubblicitari conseguiti effettivamente dal *provider,* invece che da una prospettiva *ex ante,* finalistica, come se il guadagno illecito fosse l'evento dannoso di una fattispecie causalmente orientata, mentre la norma integra pacificamente un reato di pericolo[12].

La sentenza n. 49437/2009 compie pertanto un'evidente torsione patrimoniale della fattispecie incriminatrice della condivisione abusiva di *file* su Internet: i giudici di legittimità la trasformano difatti in un reato di danno agli interessi economici sottesi allo sfruttamento commerciale delle opere coperte da diritto d'autore, probabilmente avendo preso atto dell'insufficiente selettività del dolo specifico di lucro per determinare quali comportamenti siano realmente offensivi del bene giuridico tutelato e quali no[13].

La diffusione via Internet di opere protette, in effetti, ha raggiunto le dimensioni del fenomeno di massa, tale da porsi in concorrenza sleale con il commercio legale di *software,* film, musica, etc.; non si può però dimenticare che le opzioni di politica criminale debbono comunque fare i conti con un delicato bilanciamento di interessi.

---

[10] F. MANTOVANI, *Diritto penale. Parte generale,* VII[a] ed., 2011,160-162;

[11] G. VACIAGO, *Sistemi* peer to peer: *rilevanza penale delle condotte in violazione dei diritti d'autore e diritti connessi, Dir. internet,* 2008, n. 3, 277 ss.;

[12] Cass., 22 novembre 2006, Rizzi, in *Foro it.,* 2007, II, 73; Cass., 4 luglio 2006, Bracchi; Proc. Rep. Roma 15 dicembre 2006, in *Foro it.,* Rep. 2008, voce *Diritti d'autore*, n. 205; G.i.p. Roma, ord. 9 ottobre 2007, in *Foro it.*, Rep. 2008, voce *Diritti d'autore*, n. 205; n. 206;

[13] C. PEDRAZZI, *Aspetti penali del diritto d'autore in Italia, Riv. it. dir. proc. pen.,* 1969, 687 ss.;

Da una parte vi è la libertà di espressione dell'utente di Internet, cui si accompagna il diritto alla *privacy* sui dati di navigazione; dall'altra parte vi sono gli interessi degli autori delle opere di ingegno, di natura sia personalistica sia patrimonialistica.

Nell'epoca di Internet la legge 633/1941 (e s. m.) fissa il punto di equilibrio fra beni contrapposti dando la preminenza al diritto d'autore nella sua dimensione economico-patrimoniale, incriminandosi cioè la diffusione e la comunicazione delle opere protette qualora queste condotte assumano i connotati di un'attività imprenditoriale abusiva, come si evince dalle clausole sullo scopo commerciale e sul fine di lucro negli artt. 171 *bis* e 171 *ter* l. aut..

Questo perché di fronte alla pirateria informatica, in special modo quella relativa a *file* musicali e audiovisivi, nonché a programmi per elaboratore elettronico, il baricentro della tutela penalistica è posto nell'interesse commerciale dei produttori e dei distributori di tali prodotti dell'ingegno, piuttosto che nell'interesse personale dell'autore stesso dell'opera protetta[14].

Ne consegue, *a contrario,* che le condotte a uso personale restano estranee all'ambito di applicazione delle fattispecie penali, riservandosi a queste ultime, tutt'al più, delle sanzioni amministrative.

Il diritto d'autore nel mondo virtuale, perciò, è preso in considerazione dal diritto penale soltanto nella sua dimensione patrimoniale, secondo una tendenza paragonabile alla concezione economizzante del nuovo bene dell'"identità digitale"[15].

Il caso *The Pirate Bay* è dunque emblematico delle attuali strategie di contrasto alle violazioni del diritto d'autore *online*: a fronte della irrilevanza penale della cd. pirateria altruistica o domestica, è severamente punito il commercio illegale delle opere protette, anche da parte del *provider*.

4. Il diritto d'autore nel mondo virtuale

Dato siffatto quadro d'insieme, è possibile comprendere il fondamento di requisiti essenziali quali lo scopo di lucro (cioè di vero e proprio guadagno economicamente apprezzabile) e l'uso non personale nell'art. 171 *ter*, comma 2, lett. A *bis* l. aut. sopra richiamato per ciò che attiene la condivisione telematica di contenuti audiovisivi, oppure il fine di profitto (più ampio del lucro, poiché include il risparmio di spesa) congiunto allo scopo commerciale della condotta avente ad oggetto i programmi informatici nell'art. 171 *bis* l. aut.[16].

La tutela penale del diritto d'autore *online* non si ferma qui: pure l'*upload* senza carattere lucrativo costituisce delitto, ai sensi dell'art. 171, comma 1, lett. A *bis* l. aut., anche se si tratta di un reato punito con la sola pena pecuniaria, soggetto a un'oblazione

[14] M. FARINA, *Il dolo specifico e la tutela penale del diritto d'autore: il caso della pirateria altruistica* online, Nota a Cass., sez. III, 18 gennaio 2007, n. 149, in *Dir. pen. proc.*, 2007, n. 8, 1017 ss.; G. VACIAGO, *Sistemi* peer to peer: *rilevanza penale delle condotte in violazione dei diritti d'autore e diritti connessi*, *Dir. internet*, 2008, n. 3, 277 ss.; D. TERRACINA, *La detenzione per scopo commerciale o imprenditoriale di* software *costituisce sempre reato?*, *Dir. internet*, 2005, n. 4, 357 ss..

Gli autori appena citati fondano la loro critica sul confronto tra l'art. 171 l. aut., a tutela degli interessi personali e patrimoniali connessi alle opere letterarie e gli artt. 171 *bis* e 171 *ter* incentrati sulla mera tutela dello sfruttamento economico delle opere audiovisive e dei programmi informatici.

[15] Cfr. *retro* l'intervento precedente di Gianclaudio Malgieri.

[16] M. FARINA, *Il dolo specifico e la tutela penale del diritto d'autore: il caso della pirateria altruistica* online, Nota a Cass., sez. III, 18 gennaio 2007, n. 149, in *Dir. pen. proc.*, 2007, n. 8, 1017 ss.;

speciale prima dell'apertura del dibattimento. Infine, il semplice *download*, seppur a uso esclusivamente personale e privo del dolo specifico di lucro, integra un illecito amministrativo in forza dell'art. 174 *ter*, comma 1, l. aut.

Riassumendo, l'apparato repressivo penale, pur con una legislazione secondo taluni ipercasistica, contraddittoria e per certi versi sproporzionata per eccesso[17], persegue con severità il fenomeno della pirateria informatica quando essa assume le dimensioni di una vera e propria economia parallela illegale su scala internazionale, ponendosi in concorrenza sleale con l'industria discografica, cinematografica ed elettronica e ledendone così gli interessi patrimoniali.

In situazioni del genere soccorre la fattispecie dell'art. 171 *ter*, comma 2, lett. A *bis* l. aut., introdotta nell'ordinamento proprio per colpire le operazioni di scambio, trasferimento e *upload* mosse da una finalità di guadagno economico.

Se questa era l*'intentio legis,* va fatto un paio di appunti al testo letterale della disposizione, la quale richiede l'immissione oltre alla condivisione pubblica del *file*: teoricamente dovrebbe applicarsi la norma solo ai soggetti che mettono per la prima volta a disposizione *online* un'opera protetta, senza incriminare chi si limiti a far circolare un contenuto già abusivamente presente sulla rete; in secondo luogo, non è pacifico che lo scambio tra utenti privati in *peer to peer* sia qualificabile come comunicazione "pubblica".

Nonostante questi dubbi interpretativi, la fattispecie è stata comunque rielaborata nella prassi in modo da incriminare le condivisioni abusive di opere protette su reti *peer to peer.*

La pirateria cd. altruistica (ovverosia la diffusione abusiva senza il dolo specifico di lucro dell'art. 171 *ter*, comma 2, lett. A *bis* l. aut.) è un reato meno grave, punito con la sola pena pecuniaria dall'art. 171 *bis,* comma 1, lett. A *bis* l. aut., mentre la pirateria domestica, cioè la condotta di chi scarica a uso personale opere altrui, è alternativamente sussumibile sotto il citato art. 171 *bis,* comma 1, lett. A *bis* l. aut. oppure sotto l'illecito amministrativo *sub* art. 174 *ter* l. aut. se non vi è stata alcuna condivisione del *file* protetto – o meglio, se non ve n'è stata nessuna volontaria e consapevole[18].

Tutto ciò si ripercuote sui profili di responsabilità penale dei *provider* per i delitti di pirateria informatica e telematica: nel caso in cui esso offra o metta a disposizione dei propri utenti dei programmi di scambio *peer to peer* o, in generale dei *file transfer*

---

[17] S. SEMINARA, *La tutela penale del diritto d'autore tra normativa vigente e prospettive di riforma,* in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet,* Padova, 2004, 315 ss.; L. PICOTTI, *Fondamento e limiti della responsabilità penale dei* service-providers *in Internet*, *Dir. pen. proc.,* 1999, 379 ss.; altrettanto critico BELLANI, *Musica in rete tra pirateria e uso personale (la libera circolazione delle idee in rete è cosa troppo seria per lasciarla al diritto penale), Riv. dir. ind.,* 2007, II, 83 ss.; M. FARINA, *Il dolo specifico e la tutela penale del diritto d'autore: il caso della pirateria altruistica* online, Nota a Cass., sez. III, 18 gennaio 2007, n. 149, in *Dir. pen. proc.,* 2007, 1017 ss..

Ciò che viene contestato alla parte penalistica della l. aut. è il generale rigore repressivo a vantaggio dei produttori più che degli autori, cui si accompagna però uno scarso consenso sociale alla repressione penale della pirateria informatica, specialmente quando si tratta di comportamenti non lucrativi.

Gli stessi problemi erano peraltro già stati sollevati prima dell'avvento di Internet da C. PEDRAZZI, *Aspetti penali del diritto d'autore in Italia, Riv. it. dir. proc. pen.,* 1969, 687 ss.;

[18] Non si dimentichi sul piano pratico l'impossibilità ovvero la difficoltà tecnica di disattivare la condivisione dei file dopo il *download* nei *software peer to peer* da parte dell'utente privato.

protocol, per lo meno può concorrere nel delitto *sub* art. 171 *bis*, comma 1, lett. A *bis* l. aut., che incrimina la condivisione "non profit" di contenuti protetti.

Non è difficile prevedere, però, che tendenzialmente al *provider* verrà ascritta una responsabilità concorsuale per il più grave reato di cui all'art. 171 *ter*, comma 2, lett. A *bis* l. aut. (o art. 171 *bis* l. aut. se oggetto della condotta sono programmi per elaboratore invece di opere audiovisive), tenuto conto del lucro tratto dal *provider* a seguito dell'ingente traffico telematico generato dalla condivisione illegale di contenuti in violazione del diritto d'autore e dall'aumento di valore degli spazi concessi per le inserzioni pubblicitari sui siti stessi di scambio abusivo.

Peraltro, il *provider*, in quanto quasi sempre esercita l'attività in forma di ente collettivo, al di là delle persone fisiche imputabili ai fini del diritto penale, risponde inoltre anche *ex* d.lgs. 231/2001 dopo la l. 99/09 che vi ha inserito l'art. 25 *novies* per i reati presupposto dell'art. 171, comma 1, lett. A *bis* l. aut., dell'art. 171 *bis* l. aut. e dell'art. 171 *ter* l. aut., con le sanzioni pecuniarie fino a cinquecento quote e quelle interdittive fino a un anno.

In conclusione, la disciplina penale prevista per il *provider* rispetto ai reati in materia di diritto d'autore si mostra decisamente severa, ma si temono rischi di ineffettività dell'articolata risposta punitiva, a causa della costante evoluzione tecnologica in elusione delle misure tecniche di protezione delle opere dell'ingegno.

LE INDAGINI SVOLTE CON L'USO DI PROGRAMMI SPIA *(TROJAN HORSES)*

Marco Trogu

Sommario: 1. Introduzione: le attività in analisi come indagini atipiche. 2. La violazione del domicilio informatico e della riservatezza informatica. 3. I limiti alle indagini atipiche. Un parallelo con i casi della video-ripresa domiciliare e del pedinamento satellitare. 4. L'uso dei programmi spia garantisce risultati affidabili?. 5. Prevedibilità dei casi e degli effetti delle violazioni delle libertà fondamentali, diritto di difesa e accertamento della verità processuale.

1. Introduzione: le attività in analisi come indagini atipiche

Il tema della relazione che mi è stata affidata nasce da alcune vicende processuali nelle quali i magistrati inquirenti hanno svolto attività di indagine non disciplinate dal codice di rito, sfruttando alcuni *softwares* del tipo *trojan horse* dalle potenzialità enormi, che per comodità espositiva definisco "programmi spia"[1]. Esistono varie tipologie di questi programmi: alcuni consentono di intercettare le conversazioni intrattenute via VoIP, altri sono in grado di sorvegliare tutte le attività svolte in rete da un determinato computer (c.d. sorveglianza *on line*), altri ancora (d'ora in avanti "programmi copiatori") sono in grado di estrapolare in copia i dati e i documenti informatici già formati e custoditi all'interno della memoria del computer, nonché quelli che saranno formati in futuro, copiandoli contestualmente alla loro elaborazione. Le copie dei file e le informazioni relative agli altri dati vengono poi inviate agli investigatori ad un indirizzo internet prestabilito[2].

Io soffermerò la mia attenzione sulla c.d. sorveglianza *on line* e sulle indagini compiute mediante il programma copiatore, che, per quanto possano essere assimilate alle ispezioni, alle perquisizioni e al sequestro probatorio in ragione delle finalità perseguite (acquisizione di "tracce" dei movimenti telematici, dati e documenti), si svolgono con forme talmente eccentriche rispetto al modello normativo che devono essere considerate attività di indagine atipiche. Ciò è ancor più vero se si pensa al fatto che, dopo la riforma operata con la legge 18 marzo 2008 n. 48, ispezioni, perquisizioni e sequestri devono essere compiuti adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (cfr. artt. 244 comma 2, 247, comma 1-*bis*, 259, comma 2, c.p.p.)[3]. Così, ad esempio, una perquisizione informatica

[1] In dottrina la tematica è stata affrontata da S. MARCOLINI, *Le cosidette perquisizioni on-line (o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, 335; E. APRILE, Voce *Captazioni atipiche (suoni, immagini, segnali)*, in *Dig. proc. pen. on line;* S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen. Web*, 2014, 1.

[2] Questi programmi possono anche attivare il microfono del computer usandolo come "cimice" per intercettare le conversazioni tra presenti, e la webcam per riprendere ciò che accade davanti all'apparecchio. Si tratta però di funzionalità che pongono problematiche relative alle intercettazioni e alle video-riprese nel domicilio, non pertinenti nel presente lavoro.

[3] P. TONINI, *Manuale di procedura penale*¸ XII ed., Milano, 2011, 370 s. spiega che con la legge n. 48 del 2008 il legislatore ha previsto, in relazione ai mezzi di ricerca del documento informatico, una serie di «garanzie fondamentali, che dovrebbero esser attuate in ognuno dei mezzi di ricerca», al fine di assicurare

potrebbe essere eseguita mediante l'introduzione di un programma in un computer al fine di copiare tutti i dati e i documenti in esso presenti solo se venisse assicurato il rispetto di quelle misure che garantiscono l'attendibilità dell'elemento di prova.

Da un punto di vista squisitamente giuridico, assume rilevanza che i programmi spia sono installati e funzionano all'interno di un *computer* o di un altro sistema informatico senza che colui che lo usa se ne possa avvedere. Si tratta quindi di attività occulte, i cui risultati potranno essere conosciuti dall'indagato solo con la *discovery* disposta al termine delle indagini, stante l'assenza di regole particolari sulla partecpazione della difesa e sul deposito degli atti. Per contro, le ispezioni, le perquisizioni e i sequestri sono attività palesi e, anche quando sono compiute senza preavviso, il codice prevede che vengano dati in tempi celeri certi avvisi all'interessato ed al suo difensore[4].

Per questi motivi, nel caso in esame si deve sicuramente parlare di indagini atipiche[5].

2. La violazione del domicilio informatico e della riservatezza informatica

La prima problematica che si pone di fronte a queste indagini sta nel fatto che l'installazione del programma spia all'interno di un sistema informatico e di lasciarvelo ad oltranza in maniera occulta rappresenta violazione del domicilio informatico6, nella definizione che di questo da la giurisprudenza di legittimità fiorita attorno all'art. 615-ter c.p., ossia bene giuridico rientrante nell'ambito di tutela apprestato dall'art. 14 Cost.7. Ciò che più inquieta, però, non è tanto l'illiceità penale dell'attività d'indagine, ma è che la violazione descritta, in quanto *atipica*, non è inquadrabile in nessuno dei modi di limitazione della libertà domiciliare costituzionalmente ammessi: ispezioni,

---

la conservazione del dato informatico e scongiurarne l'alterazione. Tali garanzie sono: il dovere di conservare inalterato il dato informatico originale nella sua genuinità; il dovere di impedire l'alterazione successiva del dato originale; il dovere di formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale; il dovere di assicurare la non modificabilità della copia del documento informatico; l'installazione di sigilli informatici sui documenti acquisiti.

[4] In caso di ispezione cui debba partecipare l'indagato, l'art. 364 c.p.p. prevede il diritto ad un preavviso di almeno 24 ore per il suo difensore, salvo che ricorrano ragioni particolari. Quando si procede a perquisizione e sequestro, se l'imputato è presente ha diritto di partecipare con l'assistenza di un legale (art. 365 c.p.p.), ed in ogni caso ha diritto di visionare i verbali degli atti compiuti (art. 366 c.p.p.). In ogni caso sono dovuti l'informazione di garanzia e l'informazione sul diritto di difesa. Cfr. P. FELICIONI, *Le ispezioni e le perquisizioni*, Milano, 2004, 212 ss. Sottolinea la violazione delle garanzie difensive S. MARCOLINI, *Le cosidette perquisizioni on-line*, cit., 339.

[5] S. MARCOLINI, *Le cosidette perquisizioni on-line*, cit., 339 s., dimostra che le misure di indagine in esame non sono riconducibili neppure al *genus* delle intercettazioni di comunicazioni.

[6] Esula dalla presente trattazione la *querelle* se la tutela di cui all'art. 14 Cost. sia più ampia rispetto alla tutela del domicilio offerta dal codice penale. Nel nostro caso, infatti, vi è piena coincidenza tra i due momenti.

[7] Cass., sez. VI, 14 dicembre 1999, n. 3067, in *Cass. pen.*, 2000, 2990, con note di L. CUOMO, *La tutela penale del domicilio informatico*, e S. ATERNO, *Sull'accesso abusivo a un sistema informatico o telematico*; Cass., V, 21 ottobre 1998, n. 4389, in *Cass. pen.*, 2000, 870, con nota di S. ATERNO, *Aspetti problematici dell'art. 615-quater c.p.*; più recentemente Cass. S.U., 7 febbraio 2012, n. 4694, in *Cass. pen.* 2012, 3681, con nota di C. PECORELLA, *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*. Sul punto. Già nella Relazione al d.d.l. 1115/5 del 26 marzo 1993 (che sfociò nella menzionata legge n. 547/1993) si diceva che le nuove incriminazioni volevano assicurare «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 c.p.» (cito da F. MUCCIARELLI, Sub *art. 4 l. 23/12/1993 n. 547 (criminalità informatica)*, in *Legisl. pen.*, 1996, 98).

perquisizioni o sequestri, e dovrebbe pertanto ritenersi un'operazione vietata. Vero è che nel diritto vivente si considerano costituzionalmente conformi anche modi di compressione della libertà domiciliare non tipizzati dall'art. 14 Cost8, mentre in dottrina si sono sostenute tesi più rigoriste9; a mio avviso ammettere limitazioni delle libertà individuali non tipizzate dalla Costituzione significa attribuire al legislatore ordinario un potere senza limiti preventivamente definibili, negando gli stessi fondamenti dello Stato di diritto10. Anche quella dottrina che riconosce al legislatore la legittimazione a prevedere limitazioni della libertà domiciliare che non siano ispezioni, perquisizioni e sequestri, pretende che si tratti pur sempre di attività palesi e non occulte, in quanto in quest'ultimo caso si cela sempre il rischio di abusi[11]. Sta di fatto che nel caso che ci riguarda non esiste alcuna disposizione di legge che disciplini la materia e, dunque, vi è una chiara violazione della riserva di legge, a prescindere che vi sia intesa sulla sua ampiezza[12].

Una seconda problematica si innesca quando il programma spia inizia a funzionare, sorvegliando in maniera penetrante l'utente del computer. Tale forma di controllo viola apertamente il diritto alla riservatezza informatica, bene sicuramente tutelato dalla Costituzione (secondo la lettura combinata che la stessa Consulta fa degli artt. 13, 14, e 15 Cost.[13]), dall'art. 8 CEDU e, infine, dal diritto dell'UE (specialmente dagli artt. 7 e 8 Carta di Nizza, 16 TFUE, 5 e 15 Direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche[14]). Da tutte queste fonti si può trarre l'esigenza che la

[8]Corte cost. sent. 24 aprile 2002 n. 135, in *Cass. pen.*, 2002, 2285; Cass., sez. un., 28 luglio 2006, n. 26795, in *Dir. pen. proc.*, 2006, 1347, con nota di C. CONTI, *Le video riprese tra prova atipica e prova incostituzionale: le Sezioni unite elaborano la categoria dei luoghi "riservati"*, nonché *Cass. pen.*, 2006, 3937, con note di F. RUGGERI, *Riprese visive e inammissibilità della prova*, e M.L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, e *Arch. n. proc. pen.*, 2007, 494, con nota di L. PULITO, *Più garanzie per le video riprese nel «quasi domicilio»*, e *Riv. it. dir. e proc. pen.*, 2006, con nota di A. CAMON, *Le sezioni unite sulle videoregistrazioni come prova penale: qualche chiarimento e alcuni dubbi nuovi*. In passato, sullo stesso tema, L. FILIPPI, *L'*home watching*: documento, prova atipica o prova incostituzionale*?, in *Dir. pen. e proc.*, 2001. Sulla problematica generale cfr. M. SCAPARONE, *Procedura penale*, 2013, 64 s. e nota 53.

[9]Su tutti cfr. A. PACE, *Problematica delle libertà fondamentali. Parte speciale*, Milano, 1992, 223; tra i processualisti v. A. SCELLA, *Dubbi di legittimità costituzionale e questioni applicative in tema di intercettazioni ambientali compiute in luogo di privata dimora*, in *Cass. pen.*, 1995, 992.

[10]Non convince la motivazione di C. cost. sent. 24 aprile 2002 n. 135, cit., ove si legge che il novero ristretto di atti limitativi indicati dall'art. 14 Cost. «ben può trovare spiegazione nella circostanza che gli atti elencati esaurivano le forme di limitazione dell'inviolabilità del domicilio storicamente radicate e positivamente disciplinate all'epoca di redazione della Carta, non potendo evidentemente il Costituente tener conto di forme di intrusione divenute attuali solo per effetto dei progressi tecnici successivi». Una simile interpretazione abroga di fatto l'art. 14, comma 1, Cost., rendendo sempre violabile il domicilio previo soddisfacimento della doppia riserva di legge e di giurisdizione.

[11]M. SCAPARONE, *Elementi di procedura penale*, Milano, 1999, 152.

[12]S. MARCOLINI, *Le cosidette perquisizioni on-line*, cit., 342.

[13]Cfr. Corte cost., 24 aprile 2002, n. 135, cit..

[14]L'art. 5, par. 2, della Direttiva indicata nel testo prevede che «*Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1*». Quest'ultimo articolo stabilisce che «*gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6 … qualora tale*

riservatezza della vita privata delle persone, che oggi si esplica in misura considerevole mediante l'uso dei sistemi informatici e telematici, possa essere limitata solo in forza di una previsione legislativa che sia: chiara nell'individuazione dei casi e dei modi in cui la limitazione può avvenire[15] e nell'indicazione dei soggetti legittimati, proporzionata e necessaria[16] rispetto ai fini perseguiti. La Costituzione italiana e la CEDU esigono altresì che le misure ammesse da una simile norma di legge siano autorizzate motivatamente da parte dell'autorità giudiziaria.

3. I limiti alle indagini atipiche. Un parallelo con i casi della video-ripresa domiciliare e del pedinamento satellitare

Il codice di rito ammette senz'altro che il pubblico ministero e la polizia giudiziaria svolgano attività di ricerca della prova non tipizzate (si vedano, tra gli altri, gli artt. 55 e 358 c.p.p.). Ciò non significa che i loro poteri siano illimitati, anche se si pongono vari nodi da sciogliere, e tra questi: quali limiti normativi incontrano gli inquirenti nello svolgimento di attività atipiche; in quale misura può farsi un uso processuale dei risultati acquisiti per tale via; secondo quali criteri si deve valutare la loro capacità di dimostrare i fatti (su cui *infra*, par. 4).

Quanto al primo quesito, gli orientamenti emergenti nella giurisprudenza di merito e di legittimità rendono necessario rimarcare con forza un concetto che altrove sarebbe considerato fin troppo scontato: nessun pubblico potere può incidere sulle libertà fondamentali dell'individuo senza il rispetto delle garanzie costituzionali[17]. Pertanto, nel corso delle indagini non sono ammissibili attività che implicano limitazioni delle libertà di cui agli artt. 13, 14 e 15 Cost. in assenza di una disposizione di legge e di un provvedimento motivato dell'autorità giudiziaria. Elementi di prova raccolti in violazione dei divieti costituzionali non possono mai essere acquisiti nel corso del giudizio, né utilizzati per l'assunzione di alcuna decisione giudiziaria, salvi i casi di utilizzabilità *in bonam partem*. A tale conclusione si giunge, a mio avviso, in tre passaggi:

a) i divieti posti ai pubblici poteri dagli artt. 13, 14 e 15 Cost.[18] hanno una forza cogente superiore rispetto ai divieti probatori di cui all'art. 191 c.p.p., che gli deriva dallo stesso rango costituzionale della previsione. Pertanto, perché li si possa ritenere applicabili al processo penale, non è necessario ricondurli tra i divieti probatori di cui al menzionato art. 191 c.p.p.[19];

---

restrizione costituisca ... una misura necessaria, opportuna e proporzionata all'interno di una società democratica per ... la prevenzione, ricerca, accertamento e perseguimento dei reati».

[15]Corte cost. sent. 24 aprile 2002 n. 135, cit.. Analogamente, in tema di violazione della libertà personale, Corte cost., 27 giugno 1996 n. 238, in *Cass. pen.*, 1996, 3567. Corte EDU, 30 aprile 2013, causa n. 14064/07, *Cariello e altri c. Italia.*

[16]Corte EDU, 30 marzo 1989, causa n. 10461/83, *Chappel c. Regno unito*.

[17]F. SORRENTINO, *Lezioni sul principio di legalità*, II ed., Torino, 2007, 3, afferma che «per le pubbliche autorità, la legge rappresenta il *titolo* ed il fondamento per l'esercizio dei loro poteri autoritativi … condizione ineliminabile del loro agire».

[18]Così gli artt. 13 e 14 Cost.: "*non è ammessa forma alcuna di detenzione ...*" e "*non vi si possono eseguire ispezioni o perquisizioni...*", mentre l'art. 15 Cost. pone un divieto implicito "*la loro limitazione può avvenire soltanto per atto motivato...*".

[19]Percorre questo tentativo A. CAMON, *Le riprese visive come mezzo di indagine*: *spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. Pen.* 1999, 1200.

b) infatti, il costituzionalismo contemporaneo riconosce la diretta applicabilità delle norme costituzionali[20], senza che il giudice penale debba esercitare alcun potere discrezionale o para-legislativo per rilevare eventuali violazioni dei divieti espliciti posti dagli artt. 13, 14 e 15 Cost.;

c) il principio di tassatività delle cause di invalidità non rappresenta un limite alla configurazione dei divieti probatori di rango costituzionale, in quanto esso è posto da una fonte legislativa che è sotto-ordinata rispetto alla Costituzione stessa. Sarebbe paradossale sostenere che il legislatore, omettendo di codificare una determinata causa di invalidità imposta dalla Costituzione, possa assegnare validità ad atti che la fonte superiore vieta espressamente.

Nelle ipotesi oggetto di studio ci troviamo dinnanzi ad una palese violazione della riserva di legge a cui non si può rimediare invocando l'art. 189 c.p.p., disposizione del tutto inidonea a supplire alla mancanza di una norma di legge espressa che regoli in maniera determinata la limitazione dei diritti fondamentali. Ciò perché, da un lato, la formulazione dell'art. 189 c.p.p. è troppo generica[21] e non soddisfa i requisiti richiesti dalla stessa Corte costituzionale e, dall'altro lato, tale disposizione non può essere chiamata a regolare la fase di ricerca ed acquisizione dell'elemento di prova[22], come già affermato dalla sentenza Prisco delle Sezioni Unite.

In ragione di quanto precede, i mezzi di ricerca della prova di cui parlo devono essere considerati incostituzionali, in quanto mirano a raccogliere elementi di prova «con modalità non disciplinate dal codice di rito e lesive dei diritti dell'individuo» tutelati dalla Costituzione[23], e pertanto di essi non può essere fatto alcun uso nel corso del procedimento penale[24].

---

[20]Per una panoramica sul tema cfr. R. BIN, *L'applicazione diretta della costituzione, le sentenze interpretative, l'interpretazione conforme a costituzione della legge*, in *La circolazione dei modelli e delle tecniche del giudizio di costituzionalità in Europa*, Atti del XX Convegno annuale dell'AIC (Roma 27-28 ottobre 2006), Jovene, Napoli 2010, 201.

[21]C. CONTI, *Accertamento del fatto e inutilizzabilità*, Padova, 2007, 172. Analogamente Corte cost. 9 luglio 1996 n. 238, in G*iur. cost.*, 1996, 2142. Tale affermazione si fonda non solo sul chiaro disposto degli artt. 13, 14 e 15 Cost., ma anche sull'art. 111, comma 1, Cost., secondo il quale il giusto processo è regolato dalla legge.

[22]C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, testo della relazione tenuta al Convegno su *"Gli epiloghi decisori del processo penale in cassazione"*, Roma, 13 dicembre 2012, reperibile sul web all'indirizzo *www.cortedicassazione.it*, osserva che nel diritto vivente vengono offerte interpretazioni meno rigide del testo Costituzionale, volte a «stabilire la natura e il rango dell'interesse violato, oltre al grado di lesione che la tipologia di acquisizione de qua comporta», per poi giungere alla costruzione dei divieti probatori e dei relativi limiti, esercitando in definitiva un potere discrezionale che la Costituzione affida al legislatore e non al potere giudiziario.

[23]C. CONTI, *Accertamento del fatto e inutilizzabilità*, cit., 151, che a sua volta cita V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale*, in *Giur. cost.*, 1973, 341. L'Autrice mette in risalto le difficoltà connesse all'adozione del concetto di prova incostituzionale, ed in particolare la mancanza di una «norma interposta di rango ordinario, che sancisca espressamente l'inutilizzabilità degli elementi acquisiti *contra Constitutionem*, e la difficoltà di ravvisare una norma siffatta nell'art. 191 comma 1» (*ibidem*, 157).

[24]Il problema, più che giuridico, pare culturale, e vede contrapposti chi, con animo inquisitorio, si affida all'intuito dell'investigatore pur di acquisire elementi utili alla ricostruzione del fatto, senza preoccuparsi dei diritti individuali, e chi invece reputa che il processo penale sia deputato non solo all'accertamento del fatto di reato contestato, ma anche alla tutela di interessi e di diritti che potenzialmente entrano in conflitto con quel fine. Sul punto O. MAZZA, *I diritti fondamentali della persona come limite della prova nella fase di ricerca e in sede di assunzione*, testo della relazione tenuta

In giurisprudenza non mancano enunciazioni di principio che, se portate alle logiche conclusioni, consentirebbero di risolvere alla radice simili questioni. Oltre ad alcune storiche pronunce, per le quali «attività compiute in dispregio dei fondamentali diritti dei cittadini non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente abbia subito»[25] e secondo cui «non possono validamente ammettersi in giudizio mezzi di prova che siano stati acquisiti attraverso attività compiute in violazione delle garanzie costituzionali poste a tutela dei fondamentali diritti dell'uomo o del cittadino»[26], anche recentemente la Corte costituzionale ha affermato che «un processo non "giusto", perché carente sotto il profilo delle garanzie, non è conforme al modello costituzionale»[27], mentre per la citata sentenza Prisco delle Sezioni Unite «risulta difficile accettare l'idea che una violazione del domicilio che la legge processuale non prevede ... possa legittimare la produzione di materiale di valore probatorio».

È sulla base di questi principi che sono state dichiarate inammissibili le video-riprese di comportamenti non comunicativi all'interno del domicilio, osservando che in casi del genere assume rilievo una «intrusione nel domicilio in quanto tale» non prevista dalla legge, e non sarebbe possibile applicare in via estensiva la disciplina sulle intercettazioni di conversazioni tra presenti[28]. A ben vedere la sorveglianza *on line* è paragonabile alle video-riprese nel domicilio perché, come queste possono registrare anche il più intimo atteggiamento delle persone che vantano il diritto di escludere terzi da quel luogo, così quella da la possibilità «di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati»[29].

Sempre sul presupposto della violazione della riserva di legge, le Sezioni unite hanno dichiarato inutilizzabili le c.d. "intercettazioni epistolari", in quanto con tale pratica si andava a violare l'art. 15 Cost. senza rispettare le garanzie previste dalla legge[30].

Accanto a questo tipo di pronunce, però, crescono le prassi devianti che generano un

---

al Convegno su *"Garanzia dei diritti fondamentali e processo penale"*, Milano, 9-10 novembre 2012, reperibile sul web all'indirizzo *www.penalecontemporaneo.it*. Sul tema si veda anche A. SCALFATI-D. SERVI, *Premesse sulla prova penale*, in A. SCALFATI (a cura di), *Prove e misure cautelari*, Vol. I, in G. SPANGHER (diretto da), *Trattato di procedura penale*, Torino, 2009, 3 ss. C. CONTI, *Accertamento del fatto e inutilizzabilità*, cit., 11, rileva che «la verità processuale non è eticamente neutra. Esistono regole di esclusione poste a tutela dei fondamentali diritti della persona che impongono di rinunciare a determinati dati cognitivi, a prescindere dalla idoneità di tali strumenti a produrre risultati attendibili».

[25]Corte cost., 4 aprile 1973, n. 34, in *Giur. cost.*, 1973, 326.

[26]Corte cost., 26 febbraio 1993, n. 81, in *Giur. cost.*, 1993, 731.

[27]Corte cost., 30 novembre 2009, n. 317. Si veda anche, sotto il profilo della qualità della legge che deve prevedere le garanzie, Corte cost., 27 giugno 1996 n. 238, cit.

[28]Così, ancora, Corte cost., 24 aprile 2002 n. 135, cit..

[29]Corte giust., sent. 8 aprile 2014, *Digital Rights Ireland Ltd et al. c. Ireland et al.*, cause riunite C-293/12 e C-594/12, che ha dichiarato invalida la Direttiva 2006/24/CE.

[30]Cass., Sez. un., 18 luglio 2012, n. 28997, in *Guida dir.* 2012, n. 38, 68. In dottrina si vedano, tra gli altri, A. CHELO MANCHIA, *Acquisizione di corrispondenza o «intercettazione epistolare»*?, in *Dir. pen. Proc.*, 2007, 1051; G. LEO, *Le Sezioni unite escludono la legittimità di controlli occulti sulla corrispondenza dei detenuti e non solo*, in *www.penalecontemporaneo.it*; G. ROMEO, *Le Sezioni unite sull'applicabilità delle disposizioni relative alle intercettazioni, alla sottoposizione a controllo e all'acquisizione probatoria della corrispondenza epistolare del detenuto*, in *www.penalecontemporaneo.it*.

grave senso di incertezza sulla consistenza della legge applicabile al processo penale[31], nell'ambito del quale non è più prevedibile l'azione coercitiva dei pubblici poteri, in contrasto con le ripetute affermazioni della Corte EDU.

Sintomatica della diversa sensibilità che manifestano i giudici nazionali rispetto ai colleghi sovranazionali è l'annosa questione sull'ammissibilità dei pedinamenti tramite rilevatore satellitare GPS. Per la Corte di cassazione tale mezzo di indagine non violerebbe nessuna libertà fondamentale[32], e dunque non necessiterebbe né di una base legislativa determinata, né di un provvedimento autorizzativo dell'autorità giudiziaria[33]. Di tutt'altro avviso la Corte europea dei diritti dell'uomo, che ha rilevato come una simile attività di indagine incide sicuramente sul diritto al rispetto della vita privata sancito dall'art. 8 CEDU, anche se in misura ridotta rispetto alle intercettazioni di comunicazioni[34].

4. L'uso dei programmi spia garantisce risultati affidabili?

Il successivo nodo da sciogliere è relativo all'idoneità degli strumenti in esame ad assicurare l'accertamento dei fatti, problema che si pone sia in fase di ammissione della prova atipica, sia in sede di valutazione della prova. Infatti l'art. 189 c.p.p., codificando una regola implicita nel sistema delle prove tipiche, richiede che le prove non disciplinate dalla legge possono essere assunte se, tra le altre cose, risultano idonee ad assicurare l'accertamento dei fatti. È invece un canone della logica giuridica che il giudice possa valutare solo le prove connotate da un'effettiva capacità dimostrativa.

Ho detto sopra che le informazioni ottenibili con i due strumenti in esame potrebbero essere raccolte anche mediante una perquisizione sul sistema informatico, e ciò perché l'oggetto di questi mezzi di ricerca della prova sono elementi dematerializzati[35]: dati, documenti, e programmi informatici che, rispetto alle *res* materiali, possono essere modificati, alterati e cancellati con una facilità estrema, anche inavvertitamente a seguito di condotte errate sui medesimi[36]. Per questo, in ossequio alle disposizioni introdotte nel codice di rito con la l. n. 48 del 2008, è necessario che siano adottate tutte le procedure volte a garantire la conservazione del dato informatico originale nella sua genuinità, impedirne l'alterazione successiva, assicurare una copia conforme e non modificabile del dato informatico acquisito rispetto a quello originale, installare sigilli informatici sui documenti acquisiti[37].

Quando questi elementi di prova vengono acquisiti con modalità differenti, sorge il

---

[31]O. MAZZA, *op. cit.*

[32]Tra le tante pronunce conformi, si veda da ultimo Cass. Sez. I, 7 gennaio 2010, n. 9416, in *Cass. pen.*, 2012, 1062. In dottrina si vedano le analisi critiche di A. CHELO MANCHÌA, *Localizzazione tramite GPS: quali garanzie?*, in *Riv. giur. Sarda*, 2006, 432; D. GENTILE, Tracking *satellitare mediante gps: attività atipica di indagine o intercettazione di dati?*, in *Dir. pen. proc*, 2010, 1464; A. SERRANI, *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *Arch. pen. web*, n. 2003.

[33]Così Cass. Sez. I, 7 gennaio 2010, n. 9416, cit.

[34]Corte EDU, Sez. V, 2 settembre 2010, causa n. 35623/05, *Uzun c. Germania*.

[35]TONINI P., *Manuale di procedura penale*, cit., 370.

[36]F. GIUNCHEDI, *Le* malpractices *nella* digital forensic, in *Arch. pen.*, 2013, 834.

[37]TONINI, *Manuale di procedura penale*, cit., 370 s. Si veda anche G. COSTABILE, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e diritto*, 2010, p. 465 ss. F. GIUNCHEDI, *op. cit.*, 825.

problema dell'affidabilità del risultato probatorio apparentemente raggiunto[38]. Nel nostro caso, poco o nulla è dato sapere sulla capacità dei programmi spia di assicurare risultati analoghi. Così, mentre un sequestro di dati e *files* contenuti in un sistema informatico, eseguito secondo *standards* tecnici accreditati, consente di rappresentare, anche in futuro e con un buon margine di certezza, la consistenza di quel sistema informatico alla data del sequestro, la copia tramite il *trojan* non è in grado di fornire le medesime informazioni con lo stesso grado di certezza. Al contrario, trattandosi di un programma che modifica il sistema su cui viene installato, si ingenerano incertezze ulteriori. Ad esempio, tramite i programmi spia è possibile introdurre all'interno di un sistema informatico dati, files e programmi all'insaputa dell'utente: è evidente che un simile strumento non solo è occulto, ma può diventare subdolo, facendo riemergere in tutta la sua gravità il problema di assicurare il rispetto delle garanzie difensive a cui ho accennato nel primo paragrafo.

5. Prevedibilità dei casi e degli effetti delle violazioni delle libertà fondamentali, diritto di difesa e accertamento della verità processuale.

Ho cercato di illustrare sopra come la Corte EDU e la Corte di giustizia dell'Unione europea pretendono che l'individuo possa prevedere sia i casi e i modi in cui può subire limitazioni dei propri diritti e libertà fondamentali, sia gli effetti che possono scaturire da tali atti limitativi. Io credo che quando l'individuo assume la veste dell'imputato quella pretesa debba essere assolutamente soddisfatta. Ciò perché la possibilità di prevedere con un buon margine di certezza – fatto salvo un ineludibile margine di discrezionalità connesso all'arte dell'interpretazione – la validità di un atto investigativo, significa poter riporre fiducia nel fatto che quell'atto avrà o non avrà efficacia probatoria. Tale prevedibilità è coessenziale ad un corretto esercizio del diritto di difesa, soprattutto in un sistema come il nostro in cui si offre all'imputato la possibilità di scegliere, tra vari riti, quello con cui far accertare la verità processuale. Infatti, la verità processuale che può emergere all'esito di un giudizio abbreviato è sicuramente diversa da quella che può accertarsi all'esito di un dibattimento sullo stesso identico fatto, ed il codice rimette all'imputato la facoltà di scegliere tra queste vie. Ciò non toglie che, in ogni caso, si tratti pur sempre di verità processuali aventi pari dignità giuridica (che altrimenti non si spiegherebbe come lo Stato possa comunque esercitare il proprio potere punitivo all'esito di due processi strutturalmente diversi). La scelta del rito è un momento in cui la difesa tecnica e l'autodifesa si fondono in maniera inscindibile: il difensore deve essere in grado di illustrare gli sviluppi ipotizzabili in un caso o nell'altro, ma la scelta finale spetta solo all'imputato, il cui diritto di intervento personale e consapevole al processo sarà rispettato solo se le legittime aspettative di sviluppi procedimentali *secundum legem* si avvereranno. In particolare, la scelta per un rito o per l'altro è spesso determinata dalla *prevedibilità* di poter far escludere o ammettere una certa prova. Ma se in corso di giudizio quella previsione legittima non si avvera, ad esempio perchè il giudice ritiene utilizzabile una prova incostituzionale, si determina una violazione del diritto di difesa.

E si badi che con quella scelta il giudice non sta ampliando il suo patrimonio conoscitivo, ma lo sta semplicemente distorcendo, perché da quello stesso patrimonio

[38]G. COSTABILE, Computer forensics *e informatica investigativa*, cit., 465.

conoscitivo resteranno comunque fuori tutti gli altri elementi che in quel tipo di giudizio non hanno trovato ingresso. Si tratta di un tema che esula dall'oggetto della presente relazione, ma che meriterebbe un approfondimento maggiore.

DEPREDADORES, MONSTRUOS, CHIVOS EXPIATORIOS: UN ANÁLISIS DEL DELITO DE *CHILD GROOMING*

José Antonio Ramos Vázquez

Sumario: 1. Premisa 2. El nacimiento del sexual predator (I): histeria social 3. El nacimiento del sexual predator (II): histeria (mediática y) legislativa 4. (I)rrealidades del sexual predator y realidades del delito sexual con víctima menor de edad 5. Analizando el fenómeno (I): pánico, excepción, género 6. Analizando el fenómeno (II): el otro monstruoso, el chivo expiatorio y la violencia integradora 7. Lecciones de Derecho comparado para el Derecho penal español

1. Premisa

Es propósito de este trabajo hacer una serie de reflexiones sobre la actual política criminal acerca de delitos sexuales y menores.

Concretamente, a la luz de cuanto ha sucedido -y sigue sucediendo- con las políticas represivas en esta materia en los Estados Unidos (Estado que, como sabemos, marca de algún modo la pauta en cuanto a política criminal en muchos ámbitos), intentaremos, en primer lugar, vislumbrar qué subyace a esta creciente histeria alrededor de todo lo relacionado con esas dos variables (menores de edad y sexo) desde una perspectiva que intentará conjugar análisis de género y reflexiones desde una óptica de antropología jurídica.

Por último, intentaremos extraer conclusiones de todo lo anterior, proyectándolas sobre un ejemplo concreto de la reciente legislación penal española: la incorporación del delito de *child grooming* al Código penal (artículo 183*bis*).

2. EL nacimiento del *sexual predator* (i): histeria social

Fue en la década de los noventa del siglo pasado cuando emergió con fuerza en el imaginario social y jurídico de los Estados Unidos la figura del *sexual predator*, esto es, del delincuente sexual entendido como "depredador", como un ser ávido de conseguir nuevas presas y dominado por una suerte de sed insaciable[1].

Más aún, en la línea de la definición que la RAE nos ofrece de depredar ("dicho de un animal, cazar a otros de distinta especie para su subsistencia"), se le llega a considerar como una categoría antropológica de suyo, como un *otro* respecto de los ciudadanos *normales* (o, incluso, respecto del resto de delincuentes, sexuales o no)[2].

[1] E. HOROWITZ, "Growing media and legal attention to sex offenders: more safety or more injustice?", *Journal of the institute of justice and internacional studies*, 7, 2007, 143 y ss.; M. LYNCH, "Pedophiles and cyber-predators as contaminating forces: the language of disgust, pollution and boundary invasions in federal debates on sex offenders legislation", *Law and social inquiry*, 27, 2002, 529 y ss.

[2] Sobre esta cuestión nos detendremos más adelante.

Ciertamente, como señala JENKINS, "las imágenes del delincuente sexual han cambiado dramática y cíclicamente a lo largo de los años"[3], pero esta emergencia de la sombra (más que de la materialidad) del *sexual predator* goza de características propias muy distintivas, características que han marcado el devenir tanto de la legislación penal como de la percepción social sobre la delincuencia sexual con víctima menor de edad.

Esto último porque, a su vez, los Estados anglosajones vivieron en los años setenta del siglo pasado un aumento del interés social y de la atención legislativa respecto de los delitos sexuales frente a menores[4], llegando a adquirir esta cuestión toda una "función normativa en la vida de muchas personas"[5] y de esta conjunción entre el miedo al depredador sexual y la obsesión por el delito sexual con víctima menor de edad (con su consecuente sacralización de los niños[6]) ha nacido, en primer lugar, un *momentum* de histeria social que llegó a derivar incluso en episodios de violencia física frente a sospechosos de haber cometido dicha clase de delitos[7].

En segundo lugar, dicha histeria social se vio acompasada (y retroalimentada) por una intensa actividad legislativa, convirtiéndose la cuestión del depredador sexual en el "tema del año"durante toda la década de los noventa[8] y, consecuentemente, en una de las mayores prioridades del sistema penal hasta el día de hoy.

3. El nacimiento del *sexual predator* (ii): histeria (mediática y) legislativa

La llegada del *sexual predator* a la agenda punitiva de los Estados anglosajones en la década de los noventa fue fulgurante y durante estos años se han sucedido todo tipo de medidas legislativas que, teniendo a aquél como objetivo, han supuesto un considerable recorte de derechos y garantías para todos los que, de un modo u otro, puedan encajar en tan difusa categoría.

No es objeto de este trabajo hacer una enumeración de las mencionadas medidas, pero baste decir que, entre otras, se tomaron las siguientes:

-Castigo de quienes contactan con menores a través de internet con finalidad sexual, incluso cuando dichos menores no sean tales, sino agentes de policía encubiertos[9].

La paradoja, obviamente, es que, a la postre, se castiga como delincuentes sexuales a individuos que no han tenido contacto (ni sexual ni de ningún tipo) con un menor *real*.

---

[3] P. JENKINS, *Moral panic: changing concepts of the child molester in modern America*, Yale University Press, New Haven, 1998, 2.

[4] Sobre esta cuestión, ampliamente, vid., J. BEST, *Threatened children*, University of Chicago Press, Chicago, 1995.

[5] J. PRATT, "Child sexual abuse: purity and danger in an age of anxiety", *Crime, Law and social change*, 43, 2005, 263.

[6] Por usar la expresión de ZELIZER (V. ZELIZER, *Pricing the priceless child*, Basic books, New York, 1985). PRATT (PRATT, "Child sexual abuse", cit., 267 y s.) vincula esta nueva preocupación por los niños con el descenso de la natalidad (y, consecuentemente, con la revalorización -frente a épocas pasadas- del niño individual), pero, como veremos, quizá haya más de una razón en este renovado interés por su integridad física/sexual.

[7] Como relatan J. V. ROBERTS - L. J. STALANS - D. INDERMAUR / M. HOUGH, *Penal populism and public opinion*, Oxford University press, Oxford, 2003, 51.

[8] LYNCH, "Pedophiles and cyber-predators", cit., 529.

[9] Así sucede, por ejemplo, en la "Protection of children and prevention of sexual offences Act" escocesa de 2005.

Esto es, se castiga por "malas intenciones más que por algo que se haya hecho o haya dado la impresión que se iba a hacer"[10].

-Creación de comités civiles de salud mental que pueden determinar el confinamiento en centros de tratamiento psiquiátrico[11] de aquellos "depredadores" considerados demasiado peligrosos como para ir a prisión[12].

En la actualidad, hay hasta veinte Estados de los Estados Unidos con comités de este tipo[13] y están sujetos al mencionado internamiento, que puede ser de por vida, cerca de 3.000 ciudadanos[14].

-A la creación de los mencionados comités sucedieron las llamadas "leyes Megan"[15], mediante las que se obliga a las autoridades a hacer públicos los datos de todos los delincuentes sexuales, que, previamente, han debido ser inscritos en unos registros a*d-hoc*. Entre dichos datos se incluye su foto, nombre, tipo de delito, detalles sobre éste, etc[16].

En la actualidad, todos los Estados de Estados Unidos cuentan con previsiones legales semejantes y hay alrededor de 700.000 ciudadanos inscritos en los mencionados registros[17].

-Otras restricciones más específicas son, por ejemplo, que los registrados como delincuentes sexuales no puedan registrarse en redes sociales *on line*[18], estén sujetos a restricciones sobre dónde pueden tener su domicilio[19] o, incluso, no puedan salir a la calle en la noche de Halloween (!), por entenderse que se trata de una fecha propicia para que los pedófilos entren en contacto con niños[20].

Como vemos, se trata de una larga serie de medidas que suponen un coste en derechos altísimo que, a la postre, no se tradujo en ningún resultado sustancial, ni en términos de bajada en las tasas de delincuencia sexual, ni como medio para satisfacer las continuas reclamaciones de más normas frente a los depredadores sexuales.

---

[10] J. FULDA, "Internet stings directed at pedophiles: a study in Philosophy and Law", *Widener Law Journal*, 15, 2005, 49. Este autor, acto seguido, subraya que este tipo de acciones policiales "no son más que simples (y epistemológicamente injustificadas) prisiones preventivas" (FULDA, "Internet stings", *ibid.*).

[11] Más adelante comentaremos acerca de la visión *patologizante* del delicuente sexual.

[12] Sobre esta cuestión, vid. ampliamente E. S. JANUS - R. A PRENTKY, "Sexual predator laws: a two-decade retrospective", *Federal sentencing reporter*, 21 (2), 2008, 90 y ss.

[13] JANUS - PRENTKY, "Sexual predator laws", cit., 91.

[14] J. PETRILA, "Sexually violent predator laws: going back to a time better forgotten", en B. MCSHERRY - P. KEYZER, *Dangerous people: policy, prediction and practice*, Routledge, New York, 2011, 63.

[15] Por referencia a que fueron todas ellas creadas a raíz de la muerte de Megan Kanka, una niña de siete años, asesinada por un delincuente sexual reincidente que vivía en su vecindario.

[16] Sobre esta cuestión, resulta imprescindible la obra de LOGAN: W. A. LOGAN, *Knowledge as power: crminal registration and community notification laws in America*, Stanford law Books, Stanford, 2009.

[17] PETRILA, "Sexually violent predator laws", cit., 63.

[18] Sobre esta cuestión, J. S. WYNTON, "Myspace, yourspace, but not their space: the constitutionality of banning sex offenders from social networking sites", *Duke Law Journal*, 60, 2011, 1859 y ss.

[19] Fundamentalmente, lejos de colegios, piscinas, parques infantiles y otros lugares frecuentados por niños (críticamente, M. TROIA, "Ohio's sex offenders residency restiction law: does it protect the health and safety of the state's children or falsely make people believe so?", *Journal of Law and Health*, 19, 2006, 331 y ss. –con un estudio de las medidas en concreto en 335 y ss.).

[20] Vid. M. CHAFFIN - J. LEVENSON - E. LETORNEAU - P. STERN, "How safe are trick-or-treaters?: an analysis of child sex crime rates on Halloween", *Sexual abuse: a journal of research and treatment*, 21(3), 2009, 363 y ss.

Más aún, la doctrina es unánime en considerar las leyes estadounidenses contra los *sexual predator* como un "experimento (…) que ha sido un abismal y costoso error"[21].

Pero, antes de entrar en la discusión sobre el *cómo* y el *por qué* de esta clase de normativa, un aspecto importante a tratar es el nexo entre la histeria social y este abismal y costoso error legislativo; es decir, los medios de comunicación.

En efecto, "el proceso de moldear y conformar los temas [de política criminal] está conducido por aquellos actores que han conseguido acceso al poder político y a los medios de comunicación"[22]. Y, claro está, "publicitando repulsivos delitos sexuales contra los niños, los medios han creado la demanda y la aparente necesidad de incrementar el control frente a los delincuentes sexuales"[23].

El aumento nivel de publicitación de casos de violencia sexual contra menores durante las últimas dos décadas en Estados Unidos es más que evidente, como lo es el auge del término *sexual predator* para referirse a sus autores.

Así, mientras que durante los años 80 no hubo ni una sola noticia en los medios de comunicación que incluyese la expresión *sexual predator*[24], en el año 1995 hubo 453; ascendiendo a 2.227 en 1999 y a un total de 5.006 en el año 2006[25].

Aunque es discutido cuál sea el mecanismo exacto a través del que se produce la interrelación entre medios de comunicación y opinión social[26], un dato es claro: cerca del 81% de los encuestados en Estados Unidos señalaron que su percepción del delito como problema social se derivaba de lo que habían visto en las noticias[27]. Esto, por supuesto, no es privativo de aquel Estado, sino que lo mismo podemos decir que sucede en el nuestro[28], donde los ciudadanos que afirman recibir noticias sobre delitos casi a diario son los que en mayor medida opinan que la delincuencia ha aumentado considerablemente[29] (algo que, como sabemos, es incierto).

Esta sobreexposición a las noticias sobre delincuencia supone una sobredimensión del peligro (y un aumento de su gran correlato: el miedo) en la ciudadanía[30], algo que resulta particularmente claro en el caso de los delincuentes sexuales, especialmente de aquéllos que tienen por víctima niños.

---

[21] J. Q. LAFOND, "Sexual offender commitment laws in the USA: the inevitable failure of misusing civil commitment to prevent future sex crimes", en MCSHERRY / KEYZER, *Dangerous people*, cit., 61. Añade a renglón seguido este autor que "otros países deberían aprender de nuestros terribles errores" (*ibid.*).

[22] N. V. DEMLEITNER, "First peoples, first principles: the sentencing comission's obligation to reject false images of criminal offenders", *Iowa Law review*, 87, 2002, 569.

[23] DEMLEITNER, "First peoples, first principles", cit., *ibid.*

[24] ROBERTS / STALANS / INDERMAUR / HOUGH, *Penal populism*, cit., 132.

[25] HOROWITZ, "Growing media", cit., 146.

[26] Sobre esta cuestión, ampliamente y aportando un comentario sobre las teorías más relevantes surgidas al respecto, vid. A. C. THOMPSON, "From sound bites to sound policy: reclaiming the high ground in criminal justice policy-making", *Fordham urban Law journal*, 38, 2011, 789 y ss.

[27] S. S. BEALE, "The news media's influence on Criminal Justice policy: how market-driven news promotes punitiviness?", *William and Mary Law Review*, 48, 2006, 441.

[28] Sobre las interrelaciones entre medios de comunicación, política criminal y actividad legislativa en nuestro Estado, vid. M. GARCÍA ARÁN – J. BOTELLA CORRAL, *Malas noticias*: *medios de comunicación, política criminal y garantías penales en España*, Tirant lo Blanch, Valencia, 2009.

[29] J. L. DÍEZ RIPOLLÉS / E. GARCÍA ESPAÑA (dirs.), *Encuesta a víctimas en España*, Instituto andaluz interuniversitario de Criminología, Málaga, 2009, 156 y 157.

[30] En este sentido, relacionando la cantidad de consumo televisivo en general y del de violencia televisada en particular, vid. S. ESCHHOLZ "The media and fear of crime: a survey of the research", *University of Florida Journal of Law and Public Policy*, 9, 1997, 50-51.

En este sentido, la figura mediática del depredador sexual que, como vemos, ha supuesto un punto de inflexión en el devenir de la política criminal estadounidense, ha calado también en el imaginario social, de suerte que, encuestados al respecto, los ciudadanos muestran un gran desconocimiento de la realidad de los delitos sexuales.

En efecto, los medios "sustentan mitos, retratando a los delincuentes sexuales como un grupo homogéneo de delincuentes, incurables y altamente predatorios"[31], cuando, como veremos inmediatamente, esta visión no se compadece en absoluto con la realidad.

Es esa noción de "mito" la que nos servirá de hilo conductor a lo largo de las siguientes páginas, pues toda la iconografía que rodea al *sexual predator* es profundamente mitológica.

Por eso, un seguimiento de los medios de comunicación nos muestra que los periodistas *narran* esta cuestión en términos de mito (una clase de narrativa particularmente cara a la ciudadanía)[32]. Por eso, podemos rastrear el *cómo* y el *por qué* del advenimiento de la figura del *sexual predator* desde el punto de vista de la antropología.

Veamos, pues, algunos datos que nos sirvan para desenmascarar lo *apócrifo*[33] de ese espectro del depredador sexual, en el que tantos miedos y ansiedades está depositando, a día de hoy, la sociedad.

4. (I)Rrealidades del *sexual predator* y realidades del delito sexual con víctima menor de edad

En el mismo trabajo en el que HOROWITZ llama la atención acerca del aumento exponencial de noticias en los medios de comunicación incluyendo la expresión *sexual predator*, dicho autor muestra gráficamente un *fenómeno* inversamente proporcional a aquél: el continuo y pronunciado descenso de los delitos sexuales contra menores en aquellos años (de una *ratio* de 2,3 abusos por cada 1.000 niños en 1991 se pasa a una de 1,2 en 2003)[34], lo que sin duda muestra no sólo que para la escalada mediática (y legislativa) que acabamos de exponer existen razones ajenas a un efectivo aumento de los delitos[35], sino que existe una realidad de los delitos sexuales y, especialmente, de los cometidos contra menores, que no se ve correctamente reflejada ni en los medios de comunicación, ni en el imaginario social, ni en todo el aparato legislativo destinado a combatir aquella clase de delitos.

El primer dato sobre el que debemos centrar nuestra atención es el mismo que nos servirá para, más adelante, enlazar con cuánto de antropológicamente condicionado hay en esta histeria social por la delincuencia sexual contra menores: hablamos de la construcción de un *otro* como autor de estos delitos, cuando, en realidad, la realidad es abrumadora en el sentido de que quienes atentan contra la libertad/indemnidad sexuales

[31] S. KATZ SCHIAVIONE - J. S. LEVENSON - A. R. ACKERMAN, "Myths and facts about sexual violence: public perceptions and implications for prevention", *Journal of Criminal Justice and Popular Culture*, 15 (3), 2008, 306.

[32] THOMPSON, "From sound bites to sound policy", cit., 815.

[33] "Apócrifo en el sentido de que no hay ni de lejos tantos como aparentemente estamos deseando creer que hay" (J. E., KENNEDY "Monstrous offenders and the search for solidarity through modern punishment", *Hastings Law journal*, 51, 2000, 883).

[34] HOROWITZ, "Growing media", cit., 146.

[35] Como indica agudamente el propio HOROWITZ ("Growing media", cit., 147).

de los menores son, mayoritariamente, sus familiares o, en todo caso, personas directamente vinculadas a los menores.

En efecto, todos los estudios indican que el porcentaje de desconocidos (esto es, de personas ajenas al ámbito familiar o educativo del menor) dentro de los autores de delitos sexuales con víctima menor de edad es muy escaso, rondando –según los estudios- entre un 3%[36] y un 7%[37] del total. Es más, no sólo se trata de individuos conocidos por el menor, sino que, dentro de este último grupo, destacan sobremanera los familiares (especialmente, sus progenitores), que cometen más de la mitad de los delitos sexuales que sufren los menores[38], incluso aquéllos cometidos a través de internet[39], aparte de cometer el 65% de todos los infanticidios[40].

Tenemos aquí armoniosamente unidas dos grandes mitificaciones: la del extraño peligroso y la de la familia segura.

Sobre lo primero nos extenderemos más adelante; baste poner de relieve que el "no hablar con extraños" forma parte del aprendizaje social de todo niño y que un eventual ataque por parte de un extraño no sólo genera los mayores sentimientos de vulnerabilidad y miedo[41] sino que es tenido comúnmente como más lesivo que el llevado a cabo por un conocido[42].

Sobre lo segundo, nos topamos con una idea enraizada en lo más hondo de nuestro ser social y que COLLINS ha trabajado magníficamente, denominándola la "romantización de la relación padres-hijos".

De acuerdo con esta autora, uno de los ejemplos más evidentes de dicha romantización es, precisamente, nuestra percepción del abuso sexual intrafamiliar: si ya el propio fenómeno de la delincuencia sexual contra menores nos resulta difícil de aceptar e intentamos, de un modo u otro, no confrontarlo directamente[43], el hecho de que sean los propios familiares del menor los que perpetren los actos delictivos nos produce todavía mayor desconcierto. Esto, que podríamos considerar común en nuestras sociedades actuales, se traduce, en el ámbito estadounidense, en penas inferiores para

---

[36] LYNCH, "Pedophiles and cyber-predators", cit., 545; J. M. COLLINS, "Lady Madonna, children at your feet: the criminal justice system's romanticization of the parent-child relationship", *Iowa Law Review*, 93, 2007, 150.

[37] En un 6,7% lo cifra FULDA, "Internet stings directed at pedophiles", cit., 76. En un 7% lo sitúan tanto C. B. HESSICK, "Disentangling child pornography from child sex abuse", *Washington University Law review*, 88, 2011, 887 como WYNTON, "Myspace, yourspace, but not their space", cit., 1894. En cuanto a España, de acuerdo con algunos estudios, estaríamos igualmente ante una cifra rondando el 6% de delitos cometidos por extraños al entorno del niño (vid. V. GARRIDO GENOVÉS – P. STANGELAND – S. REDONDO ILLESCAS, *Principios de criminología*, 3ª edición, Tirant lo Blanch, Valencia, 2006, 733 y ss.).

[38] COLLINS, "Lady Madonna", cit., 150. En España, un estudio cifra también el porcentaje de abusos por parte de los familiares en un 50% (M. L. SUÁREZ SOLÁ / F. J. GONZÁLEZ DELGADO, "Estadisticas y trascendencia de la violencia sexual en menores", *Cuadernos de medicina forense*, 32, 2003, 56).

[39] WYNTON, "Myspace, yourspace, but not their space", 1894.

[40] COLLINS, "Lady Madonna", cit., 133.

[41] R. J. SAMPSON, "Personal violence by strangers: an extension and test of the opportunity model of predatory victimization", *Journal of Criminal Law and Criminology*, 78, 1987, 328.

[42] C. B. HESSYCK, "Violence between lovers, strangers and friends", *Washington University Law Review*, 85, 2007, 346.

[43] "El conocimiento de la existencia de abuso sexual de niños es muy doloroso y demasiado amenazante para hacerle frente sin intermediarios: por lo tanto, unas respuestas que sean totalmente comprensibles incluyen no pensar en ello, no buscar una explicación, o negar de plano su existencia" (L. HENDERSON, "Without narrative: child sexual abuse", *Virginia Journal of Social Policy & the Law*, 4, 1997, 481).

los familiares de los menores, al ser condenados no por abuso de menores, sino por incesto (y eso cuando llega a existir condena, pues en muchos casos les resulta mucho más fácil a los juzgadores creer "que el niño está confuso y malinterpreta un tocamiento inocente"[44] antes que de verdad haya podido suceder semejante cosa en el seno de una familia)[45].

Este cambio en la calificación jurídica de los hechos supone, en primer lugar, como se acaba de mencionar, una pena inferior (por ejemplo, en California, la condena por un delito de *lewd acts involving children* conlleva una pena de un mínimo de tres años de prisión, mientras que el incesto no está castigado con pena privativa de libertad[46]-!). En segundo lugar, mientras que se veta el acceso a la *probation* a los condenados por delitos sexuales relacionados con menores, existe una excepción precisamente para los casos en que quien ha cometido el delito sea familiar del menor[47]. En tercer lugar, a los familiares les puede ser concedida su exclusión de ser inscritos en los registros de delincuentes sexuales que mencionábamos páginas atrás[48].

La existencia de estas disparidades en el régimen jurídico de los delitos sexuales contra menores cometidos por familiares de éstos "envía un poderoso mensaje normativo: el abuso sexual por parte de un miembro de la familia es un delito menos serio que otros tipos de delitos sexuales"[49].

Este mensaje, desde luego, es completamente falso: de hecho, los estudios muestran que, debido a la confianza y a la dependencia intrínseca a la relación entre progenitores e hijos, el abuso sexual intrafamiliar produce mayores daños psicológicos y sociales a quienes lo sufren[50].

Detrás de todo ello está, insistimos, la mitología del *otro* y una absoluta desfiguración de las dinámicas de los delitos sexuales contra menores, lo que lleva a una sobrevaloración positiva de la familia como lugar seguro y, sobre todo, a bajar la guardia sobre el auténtico problema, que no es, ciertamente el del extraño[51].

No obstante, antes de diseccionar esta cuestión, conviene poner de relieve, siquiera sea brevemente, otros dos grandes malentendidos derivados de esta visión distorsionada del fenómeno del abuso sexual en la infancia.

El primer malentendido es negar la presencia, no mayoritaria, pero sí en todo caso significativa, de mujeres como autoras de esta clase de delitos.

En efecto, se suele visualizar al autor como un *extraño*, y un *extraño* de género masculino. Incluso en las medidas legislativas existe la tendencia a referirse a los autores como exclusivamente masculinos[52]. En cambio, las estadísticas demuestran que

[44] COLLINS, "Lady Madonna", cit., 152.

[45] Más aún, incluso se llega a culpabilizar a la propia víctima: vid. ROBERTS / STALANS / INDERMAUR / HOUGH, *Penal populism* , cit., 137.

[46] L. R. ANDREW, "Child sexual abuse and the State: applying critical outsider methodologies to legislative policymaking", *U.C. Davis Law review*, 39, 2006, 1871.

[47] ANDREW, "Child sexual abuse", 172.

[48] COLLINS, "Lady Madonna", cit., 149.

[49] COLLINS, "Lady Madonna", cit., 148 y 149.

[50] ROBERTS / STALANS / INDERMAUR / HOUGH, *Penal populism* , cit., 137.

[51] S. KATZ SCHIAVIONE - J. S. LEVENSON - A. R. ACKERMAN, "Myths and facts", cit., 305.

[52] LYNCH, "Pedophiles and cyber-predators", cit., 545.

las mujeres sí cometen estos delitos[53], y en una medida nada desdeñable: entre un 10 y un 25% de los casos conocidos[54].

Esto choca con la creencia social respecto de la inexistencia de mujeres que atenten contra la libertad/indemnidad sexual de los menores y contra la idea de que, en caso de que lo haya, es menos lesivo que el llevado a cabo por hombres. Todo ello, unido a otras consideraciones *de género* similares que no son de este caso (pues merecerían un trabajo en sí mismas) convierten esta problemática en uno de los tabúes por antonomasia[55].

Por otra parte, hay que tener muy en cuenta, a la hora de deconstruir esta imagen distorsionada de la que venimos hablando, que hay un alto porcentaje de menores que son autores de delitos sexuales frente a otros menores[56]. De hecho, los estudios sitúan la cifra de delitos sexuales cometidos de menor a menor en alrededor de un 10 y un 20% del total[57].

Esto, aparte de ayudarnos a desdibujar la figura del *sexual predator* y a redibujar el retrato robot de cómo es el autor de esta clase de delitos, debe hacernos reflexionar sobre una problemática que ya surgió en su día en Estados Unidos: leyes pensadas para proteger a los menores frente a extraños adultos y que terminan castigando –y con una gran dureza- a otros menores.

Como afirma JANUS, "no está claro que el Derecho pueda sustentar un sistema que trata a los niños como víctimas inocentes y puras mientras reserva sus más duras y punitivas respuestas para el comportamiento adolescente"[58].

La paradoja del menor sobrevictimizado y sobrecastigado es otro de los puntos que conviene estudiar con detenimiento y que aquí intentaremos exponer en el apartado 6 de este trabajo.

Baste, de momento, su mención para cerrar el círculo de impropiedades en la figura del depredador sexual con respecto a la realidad del abuso sexual de menores y para enlazar con el siguiente apartado, en el que intentaremos analizar cómo es que una idea tan ayuna de realidad material ha funcionado tan bien a nivel social y legislativo.

---

[53] Vid., por ejemplo, el estudio de E. PELUSO – N. PUTNAM, "Case study: sexual abuse of boys by females", *Journal of the American academy of child and adolescent psychology*, 35, 1996, 51 y ss.

[54] En un 11% lo cifra HAFEMEISTER (LT. L. HAFEMEISTER, "Castles made of sand? Rediscovering child abuse and society's reponse", *Ohio Northern University Law Review*, 36, 2010, 827). En un 23% lo sitúan S. R. DUBE, *et al*., "Long-term consequences of childhood sexual abuse by gender of victim", *American journal of preventive medicine*, 28, 2005, 430 y ss.. En casi un 14% lo sitúan estudios realizados en España (V. GARRIDO GENOVÉS – P. STANGELAND – S. REDONDO ILLESCAS, *Principios de criminología*, cit., 732).

[55] Sobre esta cuestión, vid., por todos, M. ELLIOT, *Female sexual abuse of children: the ultimate taboo*, Guilford Press, New York, 1994.

[56] Esto es particularmente notorio en el ámbito de internet, donde casi la mitad de solicitudes sexuales a menores agresivas o intimidatorias son llevadas a cabo por otros menores (WYNTON, "Myspace, yourspace, but not their space", cit., 1899).

[57] Un 18% de acuerdo con los estudios manejados por ROBERTS / STALANS / INDERMAUR / HOUGH, *Penal populism*, cit., 138. En España esta cifra estaría en torno al 12% (V. GARRIDO GENOVÉS – P. STANGELAND – S. REDONDO ILLESCAS, *Principios de criminología*, cit., 732).

[58] E. S. JANUS, "Sexual violence, gender politics, and outsider jurisprudence: lessons from the american experience in prevention", en B. MCSHERRY – P. KEYZER, *Dangerous people: policy, prediction and practice*, Routledge, New York, 2011, 82.

5. Analizando el fenómeno (i): pánico, excepción, género

"La pedofilia es el nuevo imperio del mal en la imaginación cotidiana: ahora que el comunismo ha sido debilitado, parece ocupar un similar estatus metafísico como el mal de todos los males"[59]. Tal es, como hemos intentado transmitir hasta ahora, la situación en Estados Unidos, donde esta temática se ha convertido no sólo en uno de los grandes *moral panics*[60], sino en una auténtica "adicción cultural"[61].

La cuestión ahora es cómo analizar este fenómeno, que presenta tantas aristas y que, a mi juicio, es susceptible de ser enfocado desde muy diversos prismas.

Un primer punto de vista interesante es el de aquellos autores que vinculan el auge de la cuestión de los delitos sexuales con víctima menor de edad con los conceptos de modernidad, riesgo y excepción.

En este sentido, por ejemplo PRATT señala que todo este fenómeno debe ser contextualizado en el seno de los profundos cambios políticos, económicos y sociales de las últimas décadas, los cuales han provocado una permanente sensación de inestabilidad y de riesgo, magnificado por el declinar de la confianza y la sociabilidad[62].

Es en este mundo de profundos miedos, incomodidades y ansiedades donde surge la figura retórica del *sexual predator* y, en la lucha frente a él, la idea de excepción[63] (que aquí podemos entender como la "eliminación (...) de categorías enteras de ciudadanos que por cualquier razón no sean integrables en el sistema político"[64]) viene a cumplir una doble función: de un lado, estabiliza y cohesiona y, de otro, victimiza como forma de inclusión, esto es, se entiende la victimización infantil como un nuevo tipo de ciudadanía, "un emblema de los mayores daños e inseguridades"[65].

Es posible que todo lo anterior sea cierto, pero, a mi juicio, es sólo parte de un enfoque más amplio: no se trata de un riesgo o de un miedo cualquiera, sino uno que pone en jaque nuestras seguridades sobre sexualidad, familia (infancia) y género y, en este sentido, creo que hay que avanzar en estas ideas para poder entender en su plenitud la cuestión.

La esencial relación entre delitos sexuales y roles de género es suficientemente conocida, como lo es que toda regulación en este ámbito viene lastrada por el legado de normas culturales que caracterizan ciertas formas de ejercicio de la sexualidad como normativas y otras como transgresoras.

En este sentido, me parece muy sugerente la propuesta de JANUS de entender como un factor relevante del advenimiento del *sexual predator* el antifeminismo de los

---

[59] L. KIPNIS, *Bound and gagged: pornography and the politics of fantasy in America*, Grove Press, New York, 1996, 5.

[60] Como es bien sabido, la primera formulación del *moral panics* la debemos a S. COHEN, *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, Martin Robertson, Oxford, 1972, 9.

Enfatizando esta idea de pánico respecto al abuso sexual de menores, vid. LYNCH, "Pedophiles and cyber-predators", cit., 530; D. L. SCHOTTENFELD, "Witches and communist and internet sex offenders", *Saint Thomas Law Review*, 20, 2008, 368; JANUS, "Sexual violence", cit. p. 76, entre otras muchas referencias posibles.

[61] A. ADLER, "The perverse Law of child pornography", *Columbia Law review*, 101, 2001, 229.

[62] PRATT, "Child sexual abuse", cit., 265 y ss.

[63] Idea que está plasmada normativamente, por ejemplo, en los comités *civiles* de salud mental (subrayo *civiles*, es decir, más allá de los confines del Derecho penal) a los que se hizo mención en el apartado 3 de este trabajo.

[64] G. AGAMBEN, *Estado de excepción*, Pre-textos, Valencia, 2004, 11.

[65] PRATT, "Child sexual abuse", cit., 280.

sectores más conservadores de Estados Unidos. En efecto, este autor comienza recalcando que fue el feminismo de mediados de los años setenta del siglo XX el que logró del legislador una refomulación de las definiciones de violación y de agresión sexual, poniendo de relieve que esta clase de delitos tenía más que ver con una estructura social y unos valores patriarcales que con cuestiones biopsicológicas[66].

A esta reformulación de la visión normativa de los delitos sexuales vino, además, unida "una modificación de las normas procesales, en orden a erradicar presunciones tradicionales acerca de la naturaleza de la violencia sexual, a menudo referidas a mitos sobre la violación"[67].

Esta "gran narrativa"[68] feminista supuso una revolucionaria oposición al orden patriarcal y, a pesar de los intentos de la doctrina conservadora por combatirla, lo cierto es que cuajó en la legislación y resulta, a día de hoy, difícil de rebatir.

Esto sentado, JANUS argumenta que la función que cumplía la violación como fuerza motriz del patriarcado en la legislación penal viene ahora a ser desempeñada por el depredador sexual.

"Para los conservadores" –señala este autor- "devino imperativo encontrar un modo de reafirmar la tradicional visión patriarcal sobre la violencia sexual sin dar la impresión de ser blandos en delitos sexuales. Las emergentes y novedosas leyes sobre depredadores sexuales proporcionaron un paradigma ajustado a esta agenda conservadora. Ofrecieron una poderosa y segura manera de cambiar el rumbo de la política antiviolencia en una dirección mucho más compatible con las tradicionales visiones patriarcales sobre relaciones de género y violencia sexual"[69]. Y ello porque las nuevas leyes sobre depredadores sexuales "están basadas en y reforzadas por un arquetipo que refleja y refuerza visiones tradicionales sobre género y violencia sexual"[70].

De nuevo a mi juicio, este análisis ofrece sugerentes perfiles, pero no es suficiente para captar toda la esencia de esta cuestión.

En efecto, la entronización del depredador sexual como figura básica en el imaginario social y legislativo tiene que ver no sólo con políticas de género y más concretamente, como JANUS pone de relieve, con la lucha por la conservación del patriarcado como forma de dominación social masculina, sino -y especialmente en lo que respecta a su versión pedófila- con otra serie de consideraciones que ya hemos venido apuntando hasta ahora y que desarrollamos seguidamente.

6. Analizando el fenómeno (ii): el otro monstruoso, el chivo expiatorio y la violencia integradora

Enlazando con lo comentado en los anteriores apartados, si hay algo esencial a la figura del *sexual predator* es la idea de ajenidad. El depredador sexual es un *otro*. Y, como todo *otro*, delimitar sus contornos implica, a su vez, delimitar los de un *nosotros*.

Esta idea lleva a JANUS, en su análisis de la legislación anti-depredadores sexuales como elemento antifeminista, a señalar que dicha normativa supone un "exilio ritual de

[66] JANUS, "Sexual violence", cit., 77.
[67] JANUS, "Sexual violence", cit., *ibid.*
[68] JANUS, "Sexual violence", cit., *ibid.*
[69] JANUS, "Sexual violence", cit., *ibid.*
[70] JANUS, "Sexual violence", cit., 78.

la violencia sexual, enviando a los autores fuera de nuestro medio. Habiendo realizado este ritual de limpieza, en palabras de KAREN FRANKLIN, podemos decirnos a nosotros mismos que la sociedad ha cumplido su obligación de protección y que ésta no necesita de ningún cambio ni en nuestros valores ni en la propiedad de los orígenes de la violencia sexual"[71].

Pero, siendo esto en mi opinión radicalmente cierto, no es suficiente para aprehender todos los matices de la cuestión: no es sólo que la idea de un *otro* nos lleve a una tranquilidad basada en una situación ficticia o que –como el propio JANUS apunta- nos haga aceptar con menor grado de protesta legislaciones de excepción[72] (después de todo, ¿qué nos importa tener normas exasperadamente punitivas si no son para sernos aplicadas a *nosotros*, sino a *otros*?), sino que la auténtica cohesión, la auténtica cesura entre ese binomio *nosotros-ellos* acaece cuando se categoriza al *otro* como un *monstruo*.

En efecto, "crímenes monstruosos y monstruosos criminales proporcionan un apetitoso bocado para una sociedad hambrienta de consenso y cohesión"[73] y es, según creo, esta noción de monstruosidad la que nos permite encaminarnos hacia un análisis más profundo de la cuestión (no en vano *depredador* es un "primo semántico"[74] de *monstruo*).

Esta visión del depredador como un monstruo más allá de la comprensión, presocializado, diabólico y elusivo[75] y todo el aparato lingüístico que acompaña esta configuración (esto es, considerarlos como enfermos, malvados, astutos etc.)[76] implican, en el caso concreto de los autores de delitos sexuales contra menores, una idea que nos permite cerrar completamente el círculo teórico para comprender esta cuestión: la amenaza que supone el depredador, el *otro*, procede de "fuera del reino de la pureza y la inocencia"[77].

En este sentido, serán los conceptos antitéticos de monstruosidad y de pureza los que constituyan el estadio final de nuestro análisis.

Comencemos por un hecho histórico (o antropológico, si se quiere): el concepto "monstruo", dentro de sus cualidades en cuanto que "producción contra el orden regular de la naturaleza"[78] contiene una esencial: la de ser objeto sacrificial y purificador[79], especialmente en lo que respecta al sexo, del que el monstruo simboliza sus más terroríficos matices.

A su vez, "las historias sobre crímenes y castigos están profundamente entrelazadas con una secular búsqueda social de un sentido colectivo de lo sagrado, pues las más poderosas historias sobre lo sagrado tienden a ser historias sobre la violación de lo sagrado"[80].

---

[71] JANUS, "Sexual violence", cit., *ibid.*

[72] JANUS, "Sexual violence", cit., 81 y 82.

[73] KENNEDY, "Monstrous offenders", cit., 830.

[74] J. DOUARD, "Sex offender as scapegoat: the monstruous other within", *New York Law School Law review*, 53, 2009, 35.

[75] J. MARGULIES, "Deviance, risk and Law", *Journal of Criminal Law and Crimonology*, 101, 2011, 752 y ss.

[76] LYNCH, "Pedophiles and cyber-predators", cit., 544 y ss.

[77] LYNCH, "Pedophiles and cyber-predators", cit., 545.

[78] Así define la RAE este concepto en su acepción primera.

[79] DOUARD, "Sex offender as scapegoat", cit. 35.

[80] KENNEDY, "Monstrous offenders", cit., 846.

Precipitando estos elementos (monstruosidad, violencia *sagrada*, purificación) alcanzamos el de chivo expiatorio.

En este sentido, creo fundamental hacer referencia al pensamiento de RENÉ GIRARD, cuya influencia en el mundo de la sociología y la antropología en este ámbito son indiscutibles.

GIRARD ha aportado una teoría vasta y coherente (aunque, a mi juicio, discutible en muchas de sus conclusiones) sobre la realidad de las relaciones humanas. Esta visión, que tiene una tendencia globalizante[81], gravita sobre diversos conceptos, entre los que destacaría dos: la mímesis (o, mejor dicho, el *deseo mimético*) y el chivo expiatorio. Es esto último, lógicamente, lo que más nos interesa en este momento.

La tesis de GIRARD, en muy pocas palabras, es la siguiente: en las sociedades primitivas, la fuerza antagónica del deseo mimético (esto es, la fuerza del conjunto de deseos humanos que vienen referidos a los deseos de los demás) conduce a una situación de violencia que requiere, para evitar la destrucción de la comunidad en su conjunto, una salida a través de la *violencia sagrada*, de la violencia ritual ejercida sobre un chivo expiatorio que sirva para purificar la violencia de la sociedad entera. "Allí donde dos, tres mil acusaciones simétricas e invertidas se cruzaban" –nos dice GIRARD- "predomina una sola de ellas, y en torno a ella todo el resto calla. El antagonismo de cada cual contra cada cual es sutituido por la unión de todos contra uno"[82].

En efecto, de acuerdo con este autor, toda sociedad sumida en crisis y problemáticas graves sufre una amenaza de desintegración que se conjura a través de la "crisis sacrificial", esto es, del momento en que la violencia de todos contra todos se convierte en violencia de todos contra uno[83].

Y para ello, aunque "no hace falta nada o muy poco para que la sospecha de cada cual contra todos se convierta en la convicción de todos contra uno solo"[84], resulta sumamente útil achacar a quien va a devenir chivo expiatorio crímenes que "lesionan los fundamentos mismos del orden cultural, las diferencias familiares y jerárquicas sin las cuales no habría orden social"[85].

De este modo, "los perseguidores siempre acaban por convencerse de que un pequeño número de individuos, o incluso uno solo, puede llegar pese a su debilidad relativa a ser extremadamente nocivo para el conjunto de la sociedad. La acusación estereotipada permite y facilita esta creencia y desempeña un papel mediador: sirve de puente entre la pequeñez del individuo y la enormidad del cuerpo social"[86].

Así pues, el ser que carga con las culpas de todo(s) le confiere a la sociedad la referencia perdida[87], pues "todos los rencores dispersos en mil individuos diferentes, todos los odios divergentes, convergerán a partir de ahora en un individuo único: la *víctima propiciatoria*"[88].

---

[81] De ahí, precisamente, algunas de sus debilidades, pues, a mi juicio, toda teoría que intente explicar el conjunto de la vida humana está condenada al fracaso.

[82] R. GIRARD, *La violencia y lo sagrado*, 3ª edición, Anagrama, Barcelona, 1998, 87.

[83] A. LLANO, *Deseo, violencia, sacrificio*, EUNSA, Pamplona, 2004, 63.

[84] GIRARD, *La violencia y lo sagrado*, cit. 87.

[85] R. GIRARD, *Chivo expiatorio*, 2ª edición, Anagrama, Barcelona, 2002, 25.

[86] GIRARD, *Chivo expiatorio*, cit., *ibid.*

[87] LLANO, *Deseo, violencia, sacrificio*, cit., 65.

[88] GIRARD, *La violencia y lo sagrado*, cit. 88. Cursiva en el original.

Localizada la víctima propiciatoria, ha llegado el momento climático y catárquico de la inmolación. Y "en la inmolación de esa víctima, en su sacrificio, ha de participar –real o simbólicamente- todo el pueblo, para que todos sus miembros queden purificados por la acción sacrificial. Su ejecución o expulsión de la comunidad es como un mecanismo de descarga social que abre un ciclo de conciliación y de paz"[89].

Añade GIRARD como colofón que, con frecuencia, en las sociedades primitivas se acababa sacralizando o incluso divinizando a la víctima propiciatoria y que el rastro de la violencia sagrada puede seguirse por los mitos, leyendas y prohibiciones de dichas sociedades.

Expuesta así la teoría de GIRARD[90], me gustaría llamar la atención sobre esto último, esa sacralización de la víctima propiciatoria que podemos fácilmente rastrear en la figura del depredador sexual que centra este trabajo y que viene configurada como extremadamente inteligente, que puede adoptar mil personalidades y formas, que acecha sin cesar…de suerte que esta visión del depredador sexual no sólo sirve a los efectos de generar mayor miedo y angustia en el medio social sino que, en cierto modo, también mitifica su figura.

No sólo en este sentido puede percibirse una similitud entre la figura antropológica descrita por GIRARD y el rol que desempeña el depredador sexual (especialmente el pedófilo) en la actualidad: así, podemos decir que nuestros monstruos actuales cumplen exactamente la misma función que han asumido en sociedades anteriores, esto es, servir como chivos expiatorios de comunidades humanas en crisis, de modo que, en el caso concreto de los depredadores sexuales, se les castiga no tanto "con el objetivo legal de regular una conducta desaprobada" [91] cuanto para afirmar la ortodoxia en el orden moral[92].

Esto sentado, creo que podemos, en el caso concreto del pedófilo, encontrar mucho de este mecanismo descrito de violencia (legal) sobre una víctima propiciatoria. En este sentido, señala KENNEDY lo siguiente:

"La esencia del chivo expiatorio radica en la atribución de un problema interno a una fuente externa. En el miedo contemporáneo al abuso infantil, el violento depredador sexual de niños, cuyos apetitos sexuales y tendencias violentas son tan desviadas respecto de las normas sociales que se le sitúa fuera de la sociedad normal, es esa fuente externa.

El violento depredador sexual deviene un chivo expiatorio, en cambio, cuando el alcance del sufrimiento social que se le achaca es mucho mayor de lo que los hechos merecen y cuando un problema que es en realidad interno a la sociedad, viene proyectado sobre alguien que está claramente fuera de la sociedad en un sentido importante de la palabra"[93].

De este modo, un chivo expiatorio se identifica con un portador del mal pero también con alguien que aleja de la comunidad el deseo autodestructivo de ésta[94], de modo que

[89] LLANO, *Deseo, violencia, sacrificio*, cit., 102.

[90] Como el lector se imaginará, hay muchos matices en la propuesta de este autor, y los anteriores párrafos son sólo una mínima aproximación a una teoría mucho más rica de lo que aquí podamos transmitir. Por ello, nos remitimos a las obras citadas de GIRARD para una profundización en la cuestión.

[91] DOUARD, "Sex offender as scapegoat", cit. 39.

[92] DOUARD, "Sex offender as scapegoat", cit., *ibid.*

[93] KENNEDY, "Monstrous offenders", cit., 882.

[94] DOUARD, "Sex offender as scapegoat", cit., 43 y 44.

la sociedad se salva a sí misma proyectando sus deseos impuros sobre la víctima propiciatoria.

Por usar de nuevo las palabras de GIRARD: "en la crisis sacrificial, todos los antagonistas se creen separados por una diferencia formidable. En realidad todas las diferencias desaparecen paulatinamente. En todas partes aparece el mismo deseo, el mismo odio, la misma estrategia, la misma ilusión de formidable diferencia en una uniformidad cada vez más total. A medida que la crisis se exaspera, todos los miembros de la comunidad se convierten en gemelos de la violencia (…)

Si la violencia uniformiza a los hombres, si cada cual se convierte en el doble o en el gemelo de su antagonista, si todos los dobles son idénticos, cualquiera de ellos puede convertirse, en cualquier momento, en el doble de todos los demás, es decir, en el objeto de una fascinación y de un odio universales.

Una sola víctima puede sustituir a todas las víctimas potenciales, a todos los hermanos enemigos que cada cual se esfuerza en expulsar, esto es, a todos los hombres sin excepción, en el interior de la comunidad"[95].

Llegados a este punto del análisis, varios autores identifican nítidamente cuál es el oscuro objeto de deseo de la sociedad, transformado en pecado a expiar por el *sexual predator*.

"Sugiero" –dice DOUARD- "que el delincuente sexual, si bien ciertamente no se trata de alguien inocente, está siendo usado también como un chivo expiatorio de nuestras ansiedades acerca del rol sexualizado de los niños en la sociedad americana"[96]. En similar sentido, ADLER llama la atención sobre "el intenso fervor con el que se escudriña la sexualidad infantil"[97] en una sociedad en la que a una ubicua erotización de la infancia se añade una ubicua negación de este fenómeno[98].

En mi opinión, aquí radica, efectivamente, gran parte del problema, que esta última autora une con la cuestión de la pornografía infantil, resumiéndolo del siguiente modo:

"CHARLES TAYLOR escribe que el discurso produce una nueva clase de temas y nuevos tipos de deseo y de comportamiento que le pertenecen. Junto al resto de discursos acerca del abuso sexual infantil, las leyes sobre pornografía infantil han venido a determinar quiénes son los niños. Los constituye como una categoría que es simultáneamente sexual y no sexual, tan inocente como provocadora.

Al intentar liberar a los niños de la opresión sexual, la ley también reinscribe a los niños como sexualmente violables. Y este nuevo entendimiento de los niños abre el camino a lo que FOUCAULT describe como otras tecnologías del poder disciplinario, a la "vigilancia" y a la "normalización""[99].

Sexualidad y menores, en este sentido, se entrelazan de un modo altamente problemático, algo a lo que hay que añadir una nueva mitología: la de la pureza. Así, hay que tener en cuenta no sólo ese binomio sexo/menores sino el hecho de que, como afirma HACKING, los niños se han convertido en "símbolos de pureza, de origen, de identidad, de lo que preserva las fronteras contra las trasgresiones"[100]. Esto es, las

[95] GIRARD, *La violencia y lo sagrado*, cit. 87.
[96] DOUARD, "Sex offender as scapegoat", cit. 44.
[97] ADLER, "The perverse Law of child pornography", cit., 229.
[98] ADLER, "The perverse Law of child pornography", cit., 253.
[99] ADLER, "The perverse Law of child pornography", cit., 270.
[100] I. HACKING, "Risk and dirt" en R. ERICSON / S. DOYLE (eds.), *Risk and morality*, University of Toronto Press, Toronto, 2003, 40.

nociones de "pureza" e "inocencia" referidas a nuestros menores tienen mucho de construcción social y pueden esconder muchas tensiones subyacentes[101].

Sólo así alcanzamos, finalmente, el núcleo de la problemática que venimos analizando. A los pánicos morales y el control sobre todo aquello que subvierta la jerarquía entre géneros debemos unir el mecanismo del chivo expiatorio como catarsis de nuestras tensiones sobre los menores y su/nuestra sexualidad y, por último, la creciente obsesión por un ideal de pureza que no sólo tiene como objeto la (sobre)protección de los menores (como podríamos suponer en una primera impresión) sino también el control sobre su propia sexualidad (e, incluso, la configuración de nuestra propia identidad, como diremos inmediatamente).

En este sentido, creo que FOUCAULT nos puede ofrecer claves de entendimiento, especialmente cuando, analizando las estrategias de saber y de poder respecto del sexo surgidas en el siglo XVIII e imperantes hasta el día de hoy, afirma clara y sintéticamente lo siguiente:

"[Se establece una] doble afirmación de que casi todos los niños se entregan o son susceptibles de entregarse a una actividad sexual y de que, siendo esa actividad indebida, a la vez natural y *contra natura*, trae consigo peligros físicos y morales, colectivos e individuales; los niños son definidos como seres sexuales "liminares", más acá del sexo y ya en él, a caballo en una peligrosa línea divisoria: los padres, las familias, los educadores, los médicos y, más tarde, los psicólogos, deben tomar a su cargo, de manera continua, ese germen sexual precioso y peligroso, peligroso y en peligro"[102].

Aquí tenemos presente otra gran pulsión antropológica: la del tabú, que, ya desde las culturas primitivas, implica una relación paradójica de peligro y peligrosidad.

Ya FRAZER en "La rama dorada" (sobre cuyo carácter de hito histórico en el devenir de la antropología cultural no cabe discusión) nos llamaba la atención acerca de que "en la sociedad primitiva las reglas de pureza ceremonial observadas por los reyes divinos, jefes y sacerdotes concuerdan en muchos respectos con las reglas observadas para los homicidas, enlutados, parturientas, púberas, cazadores, pescadores y otros.

A nosotros estas personas de clases tan variadas nos parecen diferir totalmente de carácter y condición; a unos, los denominaríamos sagrados y a los otros, manchados, polutos, impuros. Pero el salvaje no hace entre ellos tal distinción moral; los conceptos de santidad e impureza no están aún diferenciados en su mente. Para él, el rasgo común de todas estas personas es que son peligrosas y están en peligro"[103].

Creo que esta idea subyace, entre otras cosas y aunque no sea objeto de este trabajo, a la creciente tensión entre menor socialmente concebido como peligroso (la mitología del delincuente juvenil) y como vulnerable (la mitología de la víctima infantil). Pero, en lo que aquí nos importa, me parece claro que el Derecho penal y su lucha contra el monstruo pedófilo, el depredador de niños, forma parte de ese conjunto de dispositivos institucionales y estrategias discursivas que rodean la sexualidad de los menores,

[101] S. OST, *Child pornography and sexual grooming: legal and societal responses*, Cambridge University Press, Cambridge, 2009, 178 y ss.

[102] M. FOUCAULT, *Historia de la sexualidad. 1. La voluntad de saber*, 14ª edición, Siglo XXI, Madrid, 1987, 127.

[103] J. G. FRAZER, *La rama dorada: magia y religión*, 8ª reimpresión, Fondo de Cultura Económica, México D. F., 1981, 267.

siempre desde la perspectiva dialéctica entre decir y no decir, prohibir y no prohibir, proteger y poner en peligro.

De nuevo, FOUCAULT:

"Es bien posible que [a partir del siglo XVIII] se haya despojado a los adultos y a los propios niños de cierta manera de hablar del sexo infantil, y que se la haya descalificado por directa, cruda, grosera. Pero eso no era sino el correlato y quizá la condición para el funcionamiento de otros discursos, múltiples, entrecruzados, sutilmente jerarquizados y todos articulados con fuerza en torno de un haz de relaciones de poder.

Se podrían citar otros muchos focos que entraron en actividad a partir del siglo XVIII o del XIX para suscitar los discursos sobre el sexo (…) También la justicia penal, que durante mucho tiempo había tenido que encarar la sexualidad, sobre todo en forma de crímenes "enormes" y *contra natura*, y que a mediados del siglo XIX se abrió a la jurisdicción menuda de los pequeños atentados, ultrajes secundarios, perversiones sin importancia (…) Todos esos controles sociales que se desarrollaron a fines del siglo pasado y que filtraban la sexualidad de las parejas, de los padres y de los niños, de los adolescentes peligrosos y en peligro –emprendiendo la tarea de proteger, separar y prevenir, señalando peligros por todas partes (…) irradiaron discursos alrededor del sexo, intensificando la consciencia de un peligro incesante que a su vez reactivaba la incitación a hablar de él"[104].

Así ha sido, en efecto, la historia del control de la sexualidad en los últimos siglos. Y una forma particularmente reforzada de control sobre la sexualidad de los menores (y sobre la nuestra propia) está siendo esta creciente obsesión por los delitos sexuales con víctima menor de edad; quizá porque no sea sólo esto lo que está en juego en este momento, sino también una cuestión identitaria.

En este sentido, creo que la pureza de los menores (ese constructo relativamente novedoso y extrapotenciado en los últimos tiempos) se ha situado como uno de los grandes fetiches sociales, en cuanto que transmite una sensación de orden y de corrección en unos tiempos en los que las certezas y seguridades escasean[105]. Y ello porque pureza e impureza, contaminación y abusos, son un modo de organizar los límites de una sociedad[106], de determinar qué somos nosotros mismos en cuanto individuos y en cuanto comunidad social.

Este discurso de poder de control sexual y de construcción identitaria, como muy bien pone de relieve ADLER, "no sólo afecta a niños, sino también a adultos. Rige nuestro comportamiento con los niños y también afecta a nuestra relación con nosotros mismos. FREUD puso de manifiesto que la sexualidad infantil guardaba la llave de las neurosis adultas. Desde esta perspectiva, cuando repensamos el significado de la sexualidad infantil, también podemos repensar nuestras propias historias y, por tanto, nuestras propias "identidades""[107].

Esta línea de argumentación puede, desde luego, ser profundizada, con indudables consecuencias para muchos aspectos de la configuración de nuestros ordenamientos jurídicos, pero excedería con creces del objeto (más modesto) del presente trabajo.

Baste concluir, en suma, que pureza, peligro, contaminación, riesgo e indefensión se unen –del modo que acabamos de describir- en un magma de ideas que amenaza no sólo

[104] FOUCAULT, *Historia de la sexualidad*, cit., 40 y 41.
[105] PRATT, "Child sexual abuse", cit., 266.
[106] HACKING, "Risk and dirt", cit., 35.
[107] ADLER, "The perverse Law of child pornography", cit., 270, nota al pie 340.

con llenar los ordenamientos jurídicos de regulaciones excepcionales que buscan apresar la sombra de una figura inexistente, sino también con generar una creciente tensión entre protección del menor y autodeterminación sexual de éste[108].

7. Lecciones de derecho comparado para el derecho penal español

Si atendemos a todo lo anteriormente expuesto, si aceptamos que los delitos sexuales con víctima menor de edad han devenido "la principal narrativa de nuestra cultura"[109] y que las ideas de pureza y de peligro que la figura del delincuente pedófilo lleva aparejadas son elementos discursivos con fines no de protección sino de control, creo que tenemos elementos de juicio suficientes para extraer brevemente algunas lecciones para aplicar a un caso concreto de nuestra más reciente reforma penal.

En efecto, señala PRATT que "el abuso sexual infantil se ha convertido en un camaleón salvaje, capaz de cambiar su forma y colorido a gran velocidad"[110] y que "recientemente, en otro repentino cambio, existe preocupación acerca de los abusadores en el ciberespacio acosando[111] a niños potenciales víctimas"[112].

Pues bien, esa preocupación ha sido importada a nuestro Estado y ha motivado la ya habitual "reacción espasmódica del legislador a la actualidad informativa"[113], que ha derivado en la introducción en nuestro ordenamientio de un artículo 183*bis* del Código penal del siguiente tenor literal:

"*El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos.*

Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño".

No es mi pretensión realizar aquí un comentario a dicho precepto[114], sino trasladar a él el enfoque que hemos perfilado en los apartados anteriores de este trabajo.

En efecto, ante todo, cabría preguntarse si de verdad existe –como dato criminológico- una realidad de menores de 13 años que aceptan un encuentro con un

[108] OST, *Child pornography*, cit., 148 y ss.

[109] ADLER, "The perverse Law of child pornography", cit., 227.

[110] PRATT, "Child sexual abuse", cit., 264.

[111] En realidad, PRATT utiliza el término *grooming*, que será el que utilicemos aquí como denominación genérica del delito previsto en el artículo 183*bis* del Código penal. No obstante, su utilización como verbo en este fragmento nos obliga a traducirlo de la manera más aproximada (aunque inapropiada) posible a nuestro idioma.

[112] PRATT, "Child sexual abuse", cit., 264.

[113] M. CANCIO MELIÁ "Delitos sexuales", en J. DÍAZ MAROTO Y VILLAREJO (dir.), *Estudios sobre las reformas del Código penal operadas por las LO 5/2010, de 22 de junio y 3/2011, de 28 de enero*, Civitas, Madrid, 2011, 373.

[114] Algo que ya he tenido oportunidad de hacer, rastreando la regulación existente en otros Estados (J. A. RAMOS VÁZQUEZ, "El nuevo delito de ciberacoso de menores a la luz del Derecho comparado", *Diario la Ley*, 29 de noviembre de 2011).

adulto con el que han contactado vía internet y que tiene la intención de llevar a cabo sobre ellos algún tipo de delito sexual.

Desconozco la existencia de datos en España, pero, por ejemplo, en Estados Unidos las estadísticas muestran que la cifra *real* de casos es insignificante, al menos en comparación con la preocupación social y del legislador por esta cuestión[115]. Es más, la gran mayoría de menores que aceptan solicitudes sexuales a través de la red están cercanos a cumplir la mayoría de edad y lo hacen voluntariamente[116] y los que rechazan dicha solicitud no sufren ningún tipo de estrés o trauma por ello[117].

Podría preguntarse qué sucede no con estos adolescentes sino, precisamente, con los menores de trece años, que son a los que se refiere la regulación de nuestro Código penal.

Pues bien, no me consta ningún estudio ni ninguna resolución jurisprudencial de nuestro Estado en los que aparezca reflejado ni un solo caso que pudiese ser integrado en el tipo penal del artículo 183*bis*. Ni siquiera en los discursos públicos reclamando la introducción de este delito se ha llegado a mencionar ni un solo supuesto real que haya sucedido en nuestro Estado.

La situación no es muy distinta en los Estados Unidos, donde, a pesar de que existe un mayor desarrollo tecnológico y un mayor acceso de los menores a Internet, los contactos de contenido sexual con menores de 13 años constituyen un pequeño porcentaje–en torno al 11%- de los acaecidos respecto del global de menores[118]. No sólo eso, sino que, en la inmensa mayoría de supuestos, el contacto de contenido sexual consistió simplemente en preguntas sobre el cuerpo de los menores, sin que hubiese una solicitud de encuentro.

Más aún, en aquellos supuestos en los que el contactante solicitó al menor[119] una fotografía de contenido sexual, ni uno solo de los menores aceptó[120]. Y en los casos en los que sí hubo una propuesta de encuentro aceptada por el menor (ninguno de ellos, por cierto, menor de trece años) –supuesto que tuvo lugar en sólo un 2% de los casos- no se llevó a cabo ningún delito sexual sobre el menor con el que se tuvo el encuentro[121].

Contrastemos estos datos con la justificación que el Partido Popular dio a su enmienda al Proyecto de Ley de Reforma del Código penal de la que trae causa la incriminación del *grooming* en nuestra legislación penal

Como justificación de dicha enmienda, se argumentaba que:

"Las nuevas tecnologías han supuesto la mayor dificultad de los padres para la vigilancia de las personas adultas con quienes sus hijos se relacionan. Internet permite que los menores de edad se relacionen, sin salir de una habitación, con cualquier desconocido de cualquier parte del mundo. En ocasiones, los pederastas actúan bajo el anonimato que proporciona esta red global.

[115] Pone de manifiesto esta desproporción entre realidad criminológica y percepción mediática, B. STONE, "Report calls online threats to children overblown", *New York Times*, 13 de enero de 2009.

[116] STONE, "Report calls online threats", cit., *ibid.*

[117] C. CHANG, "Internet safety survey: who will protect the children?", *Berkeley technology Law journal*, 25, 2010, 514.

[118] J. WOLAK - M. MITCHELL - D. FINKELHOR, *Online victimization of youth: five years later*, National Center for missing and exploited children, Alejandria, 2006, 43.

[119] Aquí las estadísticas incluyen a todos los menores, hasta los 18 años, no sólo los menores de 13, que son los que más nos interesan a los efectos de este apartado.

[120] WOLAK - MITCHELL - FINKELHOR, *Online victimization of youth*, cit., 44.

[121] WOLAK - MITCHELL - FINKELHOR, *Online victimization of youth*, cit., *ibid.*

Cada vez es más frecuente que los pederastas sustituyan las visitas a los parques infantiles por las pantallas de los ordenadores, desde sus casas, para buscar a sus víctimas.

Ello da lugar a nuevas formas delictivas como el "grooming informático", esto es, el acoso a menores online o "ciber-acoso". El nuevo tipo de pederasta busca a su víctima menor por esta vía, visitando espacios personales o chats a los que acuden los menores y adolescentes, seleccionan a su víctima, se ganan progresivamente su confianza y de este modo, en ocasiones, consiguen el contacto personal con ellos y llevar a cabo el abuso, o consiguen fotos pornográficas de ellos que se integran en la red" [122].

Me gustaría insistir en este último inciso: si recordamos el estudio sobre victimización de menores en internet que hemos citado anteriormente, ninguno de los menores requeridos *on line* para enviar una fotografía pornográfica propia a su contactante lo hicieron. Del mismo modo, la enmienda no aporta ningún dato de que haya sucedido semejante cosa en nuestro Estado, convirtiendo la propuesta en una auténtica petición de principio.

Pero es que, además, ¿no es la figura del depredador sexual a la que hemos dedicado el grueso de nuestro estudio la que vemos al trasluz de esta enmienda?

Volvamos un instante a ella: "cada vez es más frecuente que los pederastas sustituyan las visitas a los parques infantiles por las pantallas de los ordenadores, desde sus casas, para buscar a sus víctimas", señala la citada enmienda, añadiendo que "el nuevo tipo de pederasta busca a su víctima menor por esta vía, visitando espacios personales o chats a los que acuden los menores y adolescentes, seleccionan a su víctima, se ganan progresivamente su confianza".

Esta es la visión concordante con el mito del depredador sexual como persona siempre a la búsqueda de menores, astuto, que se permite utilizar el mejor *modus operandi* e, incluso, "seleccionar" a sus víctimas.

Pero la realidad es muy terca. No sólo desde el momento en que no puede aportarse ni un solo caso como el que se apunta en la propuesta legislativa, sino porque la lección del Derecho comparado nos muestra cuán lejos está de ser una realidad.

No quisiera aburrir al lector retomando las aporías de la figura del depredador sexual, pero recordemos que en absoluto se compadece con los datos que poseemos sobre la realidad de los autores de delitos sexuales con víctima menor de edad, de modo que si lo que se desea es tomar medidas frente a éstos, el enfoque en el pederasta que visita chats en vez de parques infantiles para atacar a sus presas es decididamente erróneo.

Más aún: es contraproducente porque focaliza todos los esfuerzos en perseguir un espectro, en vez de centrarnos en la auténtica realidad del abuso sexual infantil: el intrafamiliar y el llevado a cabo por conocidos del menor. Esto es tanto más cierto cuanto que el artículo 183*bis* se centra en menores de trece años quienes, mucho más que los mayores de esa edad, se ven especialmente vulnerables no frente a las tecnologías y a los supuestos monstruos acechándoles detrás de ellas, sino a los adultos de su entorno que se supone (y se da por supuesto) que deben cuidar de ellos.

Sin ánimo de ser redundantes, consideremos el absurdo siguiente: un profesor se gana la confianza de su alumno menor de 13 años y, con fines sexuales, concierta con él (en persona, no a través de internet) una cita, llega incluso a presentarse y el menor no acude, por la razón que sea. No habrá cometido el delito del artículo 183*bis* (al contrario de lo que sucedería si hubiese contactado por la red). Enfatizar el elemento tecnológico y centrarse en los desconocidos lleva a estas paradojas de desprotección.

[122] Enmienda número 351 – Boletín oficial de las Cortes Generales de 18 de marzo de 2010.

Esto último tiene, no obstante, cierto sentido: la fantasía, el juego de rol, tiene una importancia fundamental en el mundo de internet, pero también en el mundo de la política legislativa, en la medida en que lo fantaseado se halle inscrito en el imaginario social.

Y, en mi opinión, en la línea expuesta en las páginas anteriores, hay al menos dos fantasías asociadas a esta incorporación del *grooming* a nuestra regulación de los delitos sexuales.

En primer lugar, la fantasía de la existencia de un *otro*, de alguien a quien podamos culpar de los abusos sexuales de menores que son, desde luego, una realidad *nuestra*, de nuestras familias y de nuestros entornos más próximos. Como hemos intentado poner de manifiesto, el artículo 183*bis* constituye una de esas regulaciones legales que, más que un objetivo real de protección, suponen una suerte de exorcismo de nuestra propia realidad criminológica.

En segundo lugar, existe también en todo este entramado legislativo una fantasía de control.

En efecto, el tipo penal propuesto por el Partido Popular extendía el castigo a todo contacto con menores de edad, es decir, no sólo con aquellos sujetos que no tuviesen la edad mínima de consentimiento de las relaciones sexuales, sino con todo menor de 18 años.

Al final, aunque fuese por un mínimo de coherencia con el resto de la regulación de los delitos sexuales en nuestro Código, se restringió el delito de *grooming* a los menores de trece años, pero la idea de ampliar el tramo de edad punible hasta los dieciocho tiene un sentido disciplinario, de vigilancia y control, en la línea expuesta en el apartado precedente de este trabajo.

De lo que se trata, en resumidas cuentas, no es ya de proteger a los menores, sino de controlarlos, de escudriñar su sexualidad y sus ámbitos de intimidad, con quién hablan y qué hacen cuando navegan por la red.

Quizá por eso, en las estadísticas de los Estados Unidos podemos apreciar que un significativo porcentaje de los menores que han sufrido algún tipo de contacto *on line* de contenido sexual no contaron nada a nadie "por miedo a meterse en problemas"[123]. Quizá son perfectamente conscientes de que la presión legal sobre los contactantes de menores por internet es, en gran medida, una presión legal destinada, de un modo más o menos sutil, a someterlos a ellos mismos.

Por todo ello, la conclusión es clara: como señalaba NIETZSCHE en su "Más allá del bien y del mal", quien combate monstruos tiende a convertirse él mismo en un monstruo. El combate contra el depredador sexual es, en este sentido, un combate contra una sombra (no contra una materialidad) pero una sombra de nosotros mismos.

Y esto, sobre todo si, haciendo la paráfrasis, nos creemos más allá del bien y del mal, lo único en que redunda es en la asfixia de la libertad de los menores en el ámbito sexual.

[123] WOLAK - MITCHELL - FINKELHOR, *Online victimization of youth*, cit., 44.

LA SICUREZZA INFORMATICA COME BENE COMUNE
IMPLICAZIONI PENALISTICHE E DI POLITICA CRIMINALE

Chiara Bigotti[1]

Sommario: 1. Premessa: l'interdipendenza dalla tecnologia digitale 2. La criminalità informatica: un fenomeno in espansione e l'inefficacia delle politiche di autoregolamentazione 3. Il paradigma penale tra repressione e prevenzione 3.1 La responsabilità penale dell'internet service provider 4. La sicurezza informatica come bene comune: una concezione socio-economica 5. La Proposta di direttiva UE sulla sicurezza delle reti e dell'informazione 6. Criticità del diritto penale della sicurezza 7. Verso la definizione giuridica di un concetto nebuloso? La sicurezza informatica nella proposta di direttiva sulla sicurezza delle reti e dell'informazione 8. Le molteplici declinazione del diritto fondamentale alla riservatezza: dal consenso al trattamento dei dati, allo ius excludendi alios, al diritto all'oblio 9. Il principio di proporzione come criterio del bilanciamento tra riservatezza e sicurezza informatica 10. Conclusioni.

1. Premessa: l'interdipendenza dalla tecnologia digitale

Le economie mondiali e la società hanno subìto radicali trasformazioni per effetto dell'espansione della Rete. Quest'ultima riveste ormai importanza strategica in ogni settore. Le imprese hanno colto ben presto le potenzialità del commercio elettronico, tanto che, nonostante la crisi che attanaglia i paesi dell'area europea, l'*e-commerce* è in costante crescita e sottrae fette sempre più importanti al mercato reale[2]. L'abbattimento dei costi relativi alle barriere spazio-temporali di trasmissione dei dati, la digitalizzazione dei documenti e l'utilizzo di software aziendali costituiscono innovazioni che hanno interessato tutti i settori produttivi. Le pubbliche amministrazioni hanno progressivamente cominciato ad adottare i sistemi informatici, in ossequio al processo di modernizzazione della macchina burocratica, nella speranza di un risparmio di spesa imposto dalla *spending review*.

Da Internet dipende, altresì, la funzionalità delle infrastrutture critiche degli Stati, come la rete idrica, elettrica, le telecomunicazioni e i mezzi di *intelligence* a difesa della sovranità nazionale[3].

Il *web* ha modificato le abitudini relazionali diffuse tra la collettività: incontri, scambi e nuove forme d'interazione avvengono e si sviluppano in misura massiccia nella realtà virtuale, attraverso le platee artificiali costituite dai *social networks*, *forum*,

[1] Un ringraziamento speciale va ai miei Professori Lucio Monaco, Alessandro Bondi e Gabriele Marra per gli insegnamenti di scuola e di vita, per i consigli, per la pazienza e l'attenzione con cui seguono il mio percorso di studi. Un 'grazie' di cuore anche ai miei colleghi Dott. Giulio Vanacore, Dott. sse Chiara Battaglini e Cecilia Ascani e – *last but not least* - al DiPLaP, fucina di idee e nuove amicizie.

[2] Il dato è stato ricavato dal rapporto e-commerce 2014, presentato il 17 aprile 2014 in Italia, pubblicato su: www.casaleggio.it

[3] I. KALFIN, *Relazione sulla protezione delle infrastrutture critiche informatizzate – Realizzazioni e prossime tappe: versi una sicurezza informatica mondiale (2011/2284(INI))*, Commissione UE per l'industria, la ricerca e l'energia, Strasburgo,16 maggio 2012, su www.europarl.europa.eu

blog[4]. Ciò ha comportato la creazione di multiple identità digitali, quali frammenti e proiezioni delle molteplici sfaccettature di personalità degli utenti in carne ed ossa[5]. Dunque, la tecnologie informatiche interconnesse permeano ogni ambito delle attività umane: da quello pubblico alla sfera più intima della persona. Tale caratteristica è indicata con il termine 'pervasività'.

La Rete è stata concepita come strumento per la circolazione di dati e delle informazioni, fino ad assumere, al nostro tempo, il ruolo di volano della conoscenza e catalizzatore dei principi di democraticità ed uguaglianza, laddove concede l'accesso indiscriminato al sapere su scala globale[6]. Da questo punto di vista, essa si atteggia a fattore di globalizzazione, dal momento che annulla le distanze. La disponibilità degli studi e la condivisione dei risultati delle ricerche sullo spazio cibernetico non ha semplicemente incentivato e dilatato i confini del dialogo accademico, ma ha soprattutto prodotto i vertiginosi progressi scientifici degli ultimi anni[7].

Sul fronte economico, inoltre, l'accessibilità a un'enorme mole di informazioni sui consumatori crea asimmetrie informative a favore dei più grandi providers che gestiscono il traffico telematico rispetto alle imprese concorrenti e agli utenti finali. La peculiare collocazione di questi intermediari della società dell'informazione favorisce la creazione di vere e proprie 'rendite di posizione', attributive di un grande potere, nella misura in cui i dati acquisiti, oltre ad essere suscettibili di impiego a fini di *marketing*, sono esposti a gravi rischi di abuso a scopo di profitto[8].

Ad accentuare l'importanza strategica di Internet contribuisce la sua configurazione come 'bene non rivale': la navigazione e la fruizione dei servizi *online* generalmente non dipendono dal numero e dal tipo di attività degli altri utenti, sicché ciascuno potrà trarne vantaggio a prescindere dal contestuale utilizzo da parte di altri. La sua vitalità è amplificata in forza del fenomeno noto come 'effetto di rete': quanto più una rete è estesa e altamente utilizzata, tanto più acquista valore, perché cresce l'utilità che ciascuno può ricavarne ed incentiva al suo utilizzo gli altri internauti e i profani[9].

---

[4] L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, giur. merito, 12/2012, 2522 ss..

[5] A. C. AMATO MANGIAMELI, *Sul diritto alla privacy. Variazioni sul tema e spunti normativi*, in A. C. AMATO MANGIAMELI, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, Torino, 2010, 300.

[6] G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Torino, 2010, 201 ss.. Dopo aver ripercorso la storia della nascita di internet, l'A. riporta la definizione di internet, estrapolata dal documento sulle regole e procedure per stabilire gli standard della Rete, come: "*una collaborazione internazionale dotata di un'organizzazione non-rigida tra reti autonome interconnesse, sostiene la comunicazione da host a host mediante l'adesione volontaria a protocolli aperti e procedure definite mediante Standard di Internet*".

[7] Si pensi alle innovazioni tecnologiche e ai traguardi raggiunti in medicina, come la scoperta di nuovi farmaci, il tracciamento del genoma umano, etc.. Cfr. AA. VV., *Understanding Knowledge As a Commons*, (a cura di Hess C. e Ostrom E.), Massachusets, 2007; trad. it. KATERINOV, *La conoscenza come bene comune. Dalla teoria alla pratica*, (a cura di C. HESSE e E. OSTROM), Torino, 2009, 83 - 125.

[8] E. GRAZZINI, *L'economia della conoscenza oltre il capitalismo. Crisi dei ceti medi e rivoluzione lunga*, Torino, 2008.

[9] G. SARTOR, *L'informatica giuridica*, cit., 9 - 13; D. BOLLIER, *Lo sviluppo del paradigma dei beni comuni*, in AA. VV., *La conoscenza come bene comune*, cit., 39.

Alla luce di queste considerazioni si può affermare che la salvaguardia della Rete e delle informazioni riveste un ruolo chiave per la preservazione del sapere ed il progresso dell'umanità.

2. La criminalità informatica: un fenomeno in espansione e l'inefficacia delle politiche di autoregolamentazione

La traslazione della vita reale su quella virtuale per effetto dell'utilizzo massivo di Internet ha inevitabilmente comportato l'incremento del suo impiego anche per fini illeciti (c.d. *dual use*). Secondo il rapporto 'CLUSIT 2013', il *cybercrime* è diventato la causa di oltre il 50% degli attacchi ai sistemi informatici nel 2012, con una crescita annua di oltre il 270%[10].

Dal punto di vista penale, la Rete può essere inquadrata sotto una duplice angolazione: 1) come fattore criminogeno, perché crea nuove occasioni di delitto (circolazione di materiale pedopornografico; frode informatica; danneggiamenti di dati, informazioni, programmi; incitamento all'odio etnico-razziale; propaganda di partiti vietati per legge, etc.); 2) come mezzo che può fornire un importante contributo nella prevenzione del crimine (terrorismo, traffico di stupefacenti, etc.). In tale ultima accezione, Internet è un formidabile strumento che arricchisce anche l'arsenale a disposizione delle autorità inquirenti. Tuttavia, le apparecchiature, i software e Internet devono trovare ancora nel nostro codice di rito una capillare ed organica disciplina che consenta di sfruttarne tutte le potenzialità.

Quanto al primo profilo, il *web*, per effetto delle sue caratteristiche endogene, rappresenta un terreno fertile per la proliferazione dei reati. La deterritorializzazione e l'ubiquità hanno comportato l'annientamento delle limitazioni temporali, nonché dei confini spaziali sui quali si reggeva la sovranità territoriale. Sicchè la realizzazione di crimini a rilevanza sovranazionale può rivelarsi estremamente semplice nelle modalità di estrinsecazione. Al contrario, può essere molto complicato, se non talvolta impossibile, arrestare l'autore del reato, a causa dell'eterogeneità della normativa penale e processuale a livello internazionale[11]. Paradossalmente le normative nazionali fungono da principale barriera che assicura l'impunità. Giovandosi della legge di un determinato stato quale scudo protettivo, il *cyber* criminale resterà a piede libero ed avrà tutto il tempo per occultare il profitto derivante dall'illecito.

La neutralità è un'altra caratteristica dell'architettura di Rete concepita per ottimizzarne le prestazioni: i *router* o *gateway*, vale a dire le apparecchiature che governano il traffico virtuale, tendenzialmente si limitano ad assolvere la funzione di inoltro o mero avanzamento dei pacchetti verso la loro destinazione, in modo tale che "*tutto il traffico riceva lo stesso trattamento, senza discriminazioni, restrizioni o interferenze, indipendentemente dalla fonte, dalla destinazione, dal tipo, dai contenuti,*

[10] Si tratta del rapporto annuale sulla sicurezza informatica in Italia dell'associazione italiana per la sicurezza informatica (CLUSIT) che prende in considerazione gli anni 2011, 2012 e i primi sei mesi del 2013. E' possibile consultare il rapporto CLUSIT al sito: www.assintel.it

[11] G. AMATO - V. S. DESTITO - G. DEZZANI - C. SANTORIELLO, *I reati informatici*, Milano, 2010, 123 - 189.

dal dispositivo, dal servizio o dall'applicazione" [12] . Declinata come libertà di circolazione dei dati e indifferenza verso i contenuti veicolati, la neutralità si traduce in un ricettacolo per i malintenzionati, a causa dell'assenza di autorità o soggetti terzi preposti al controllo[13]. A questi rilievi si accompagnano una bassa percezione del rischio di essere presi ed una diffusa convinzione circa l'ineffettività della sanzione, che spingono a credere che sul web tutto sia lecito[14].

Il mantenimento del principio di neutralità quale valore intrinseco della Rete è argomentazione ricorrente tra coloro che sono contrari ad una sua massiccia regolamentazione. Fintanto che la realtà virtuale era un fenomeno circoscritto, anche il diritto rivestiva una funzione marginale, in relazione alla proprietà dell'hardware e ai diritti fondamentali (libertà di manifestazione del pensiero, di iniziativa privata, etc.). Ma il suo peso crescente in ambito economico e sociale ha reso necessaria l'introduzione di normative *ad hoc* per disciplinare specifici settori: si pensi, una per tutte, alla direttiva sul commercio elettronico (2000/31/CE) attuata in Italia con il d. lgs. 70/2003.

Sulla dilatazione degli ambiti d'intervento della regolamentazione si registrano posizioni molto diversificate: ad un estremo, si collocano i sostenitori delle tesi libertarie, per i quali Internet, essendo un'entità separata dal mondo reale, non dovrebbe essere assoggettata alle scelte espressione della volontà dei governi o dei poteri forti[15]. Ciò per evitare di lasciare in mano al potere politico uno strumento di monitoraggio occulto delle attività dei cittadini molto invasivo e suscettibile di contenere e soffocare il dissenso.

Avverso tali posizioni autonomistiche si oppongono però considerazioni di ordine economico: la neutralità della Rete può trasformarsi in un fattore d'incertezza per il mercato, cui corrispondono stime di riduzione degli investimenti nei servizi e nelle infrastrutture della società dell'informazione.

Tra i sostenitori della necessità di una maggiore regolazione giuridica, il costituzionalista statunitense Lawrence Lessig pone l'accento sulla stretta correlazione tra regolamentazione e libertà: la seconda sarebbe direttamente proporzionale alla prima. Secondo lo studioso, il diritto costituisce la via per affrancarsi dall'imperio del 'codice' quale vero *dominus* della realtà virtuale, che stabilisce cosa l'utente possa fare e che pertanto, in ultima istanza, comprime la libertà[16].

---

[12] Commissione di studio per la redazione di principi e linee guida in tema di garanzie, diritti e doveri per l'uso di Internet, *Relazione*, *Elementi di documentazione n. 132*, 25 luglio 2014, 19, su: http://documenti.camera.it/leg17/dossier/Testi/GI0250.htm

[13] Per una più ampia disamina del principio di neutralità della rete si veda: AGICOM, *Delibera n. 40/11/CONS, Consultazione pubblica sulla neutralità della rete*, Allegato B, su www.agcom.it.

[14] S. W. BRENNER / L. CLARKE, *Distributed security: a new model of law enforcement*, su: www.papers.ssrn.com

[15] J. P. BARLOW, *A declaration of the Independece of Cyberspace"*, su http://w2.eff.org/Misc/Publications/John_Perry_Barlow/barlow_0296.declaration.txt

[16] Il 'codice' sarebbe l'insieme di vincoli su come il cyberspazio si deve comportare, ossia le condizioni per accedere al cyberspazio: ad esempio, l'autenticazione mediante credenziali e la password per accedere ad un determinato sito sono dei vincoli. L. LESSIG, *Code V2*, New York, su: www.codev2.cc/download+remix/

3. Il paradigma penale tra repressione e prevenzione

Al di là dell'ampio dibattito sull'opportunità di regolamentazione di Internet, i dati statistici sopra riportati segnalano la vulnerabilità dei sistemi informatici e della Rete.

Il legislatore italiano, fin dal 1993, ha deciso di apprestare specifica tutela penale a determinati beni giuridici traslati sulla realtà virtuale[17].

E' opportuno premettere alcuni cenni sulle caratteristiche dei contenuti digitalizzati. *Online*, le tipologie di manifestazione del pensiero sono appiattite, perché tutto è ridotto a dato informatico: una ripresa audiovisiva, un articolo di giornale, un blog risultano dalla combinazione prestabilita di segni secondo uno specifico protocollo. Lo scambio telematico, inoltre, non conosce barriere linguistiche, dal momento che i pacchetti di dati sono organizzati attraverso il linguaggio universale dei simboli alfanumerici. Così, la stessa frode informatica, a ben vedere, si trasforma ontologicamente da azione fisica a forma di comunicazione mediante la quale il truffatore richiede lo spostamento virtuale di una somma da un conto ad un altro[18].

Perciò, la criminalizzazione dei reati informatici è avvenuta secondo due linee direttrici: mediante la mera estensione di talune fattispecie già esistenti, laddove possibile (art. 491-*bis* c.p.); attraverso la creazione di ipotesi specifiche, in considerazione delle peculiarità intrinseche della dimensione virtuale (es.: 615-*ter*, 617-*quater*, c.p., etc.)[19]. Questo modo di procedere rispecchia la classificazione dei reati informatici nelle due categorie di: - reati informatici in senso ampio, comprensivi di tutti gli illeciti comuni commessi mediante lo strumento informatico (per esempio, la diffamazione sul *blog*); - reati informatici in senso stretto, in riferimento a quelle figure di reato nelle quali l'elemento informatico – la connessione, l'elaboratore, i sistemi informatici e telematici, il software - si presenta come elemento imprescindibile e caratterizzante della fattispecie, sicché le esigenze di tassatività delle norme incriminatrici impongono la creazione di apposite ipotesi delittuose (ad esempio, l'accesso abusivo a sistema informatico o telematico, ex art. 615-*ter*, c.p., la frode informatica, ex art. 640-*ter* c.p.) [20].

Il ricorso al diritto penale e, in molti casi, l'inasprimento sanzionatorio sono altresì giustificati dalla maggior carica lesiva delle violazioni commesse *online* rispetto a quelle realizzate nel mondo reale. Si pensi all'amplificazione del disvalore penale prodotta dall'effetto eco con la quale l'informazione si propaga nei *social networks*[21]. La potenziale pericolosità della fonte-realtà virtuale si evince, inoltre, dalla circostanza che i materiali pubblicati, quando non sottoposti a restrizione all'accesso, si indirizzano ad un numero indeterminato di destinatari. Emblematica, in proposito, è l'evoluzione del fenomeno della pedopornografia, il cui livello di pericolosità prima dell'avvento di Internet era pressoché minimo, mentre oggi assume

---

[17] Il primo intervento in materia è avvenuto con la legge 23 dicembre 1993, n. 547, "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*", adottato a seguito della raccomandazione del Consiglio d'Europa del 13 settembre 1989 sulla criminalità informatica.

[18] G. PICA, "*internet*" voce, *dig. disc. pen.*, Torino, agg. 2004, 425- 483.

[19] Sul classico tema del discrimine tra interpretazione estensiva ed analogia: T. D'AGUANNO, "*Legge penale (interpretazione della)*", *dig. disc. pen.*, Torino, agg. 2004, 530 - 546.

[20] L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, Milano, 4/2011, 827 ss.

[21] S. W. BRENNER / L. CLARKE, *Distributed security*, cit., 30.

dimensioni elefantiache, tanto da aver originato un vero e proprio mercato occulto di scambi. Il legislatore ha pertanto ritenuto di dover punire, seppur in maniera più tenue rispetto alla pornografia minorile (art. 600-*ter*), anche le ipotesi in cui le condotte di cui agli artt. 600-*ter* e 600-*quater* si attuino mediante *immagini virtuali* ritraenti *immagini di minori degli anni diciotto o parti di essi* (art. 600-*quater*1.)[22]. La norma si preoccupa di precisare che per immagini virtuali devono intendersi "*le immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di realizzazione fa apparire come vere situazioni non reali*"[23].

Per reprimere e prevenire le nuove e più insidiose forme criminali, ecco allora che si ricorre allo schema dei reati di pericolo[24]. S'introducono fattispecie prodromiche ad accessi abusivi o all'intercettazione di comunicazioni informatiche (artt. 615-*quater* e 615-*quinquies*, artt. 617-*quinquies* e 617-*sexies* c.p.). Tali ipotesi delittuose sono cioè strutturate come reati di pericolo concreto e astratto. In quest'ultimo caso, il pericolo non è elemento esplicito della fattispecie, bensì è ritenuto sussistente in via implicita, sulla base di massime di esperienza che inducono ad anticipare la soglia di punibilità. Ben noti sono i rilievi critici sull'ammissibilità di queste incriminazioni rispetto al principio di necessaria offensività: da un lato, le massime di derivazione sociale potrebbero condurre ad aporie di sistema, laddove risultassero niente meno che false credenze. Dall'altro lato, si rischia di reprimere la mera disobbedienza ad una norma, a fronte di un'azione del soggetto attivo in realtà priva dell'effettiva messa in pericolo del bene protetto[25]. Si pensi all'art. 615-*quinquies* c.p. ("*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*"): il delitto si consuma nel momento in cui il soggetto attivo abusivamente si procura, ad esempio, un programma nocivo, pur se non ancora inserito in alcun sistema informatico. Dunque, si finisce per punire il mero possesso o disponibilità di un *software* dotato di potenzialità distruttive, pur se non installato o attivato (*virus* a tempo o ad attivazione subordinata a precise condizioni)[26].

---

[22] F. MANTOVANI, *Diritto penale. Parte speciale*, vol. I, Milano, 2008, 424 - 425, dove l'A. ricorda che la disposizione è attuazione, con alcune varianti, del disposto della Convenzione sul *Cybercrime* del 2002, poi ripresa dalla Decisione Quadro 2003/68/GAI del Consiglio d'Europa del 22 dicembre 2003, relativa alla *Lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile*. Quest'ultima ricomprende nel *genus* pornografia minorile, sia la pornografia reale (ossia realizzata con un bambino reale coinvolto o implicato in una condotta sessuale), sia la pornografia realizzata con una persona che sembra un bambino o con un bambino inesistente, in modo da ritenere penalmente rilevante anche l'ipotesi di elaborazione grafica parziale di minori esistenti e adulti fatti apparire come minori.

[23] Tribunale di Milano, 11 novembre 2010, con la quale è rigettata l'eccezione d'incostituzionalità dell'art. 600 quater1, in considerazione del fatto che "*Da una lettura costituzionalmente orientata dell'art. 600 – quater 1 CP discende che il bene giuridico protetto da tale norma, collocata tra i delitti contro la persona è quello sviluppo fisico, psicologico, spirituale, morale e sociale delle persone fisiche minorenni e innanzitutto del minore ivi realmente rappresentato perché la sua immagine, nella specie proprio la fotografia della sua testa, è stata associata a contesti sessuali quali quelli oggetto del presente giudizio".* Su: www.penale.it/page.asp?IDPag=932

[24] E. CORN, *Il principio di precauzione nel diritto penale. Studio sui limiti dell'anticipazione della tutela penale*, in *Itinerari di Diritto Penale*, Collana diretta da E. DOLCINI, G. FIANDACA, E. MUSCO, T. PADOVANI, F. PALAZZO, F. SGUBBI, Torino, 2013, 84 – 99.

[25] G. FIANDACA – E. MUSCO, *Diritto penale. Parte generale*, Bologna, 2010, 205; G. MARINUCCI – E. DOLCINI, *Manuale di diritto penale. Parte generale*, Milano, 2012, 207-210.

[26] G. AMATO - V. S. DESTITO - G. DEZZANI - C. SANTORIELLO, *I reati informatici*, cit., 97; C. SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, Milano, 2010, 67 ss., sulle forme di offesa tipiche commesse in rete.

L'arretramento della soglia di punibilità è determinato dal paradigma preventivo oggi dominante[27]. Il terreno d'intervento è quello farraginoso della società del rischio: attività lecite e/o autorizzate potenzialmente pericolose. Se il fine del diritto penale è impedire eventi dannosi o pericolosi, è necessario anticipare la soglia della risposta punitiva allo stadio della realizzazione di atti idonei a determinare tali esiti infausti o addirittura a quella del presunto pericolo derivante da un comportamento. Ma tale operazione collide con l'assunto per il quale la sanzione maggiormente afflittiva della libertà personale dovrebbe sopraggiungere soltanto ove si accerti un fatto materiale connotato da reale disvalore e a condizione che non sia rintracciabile, nell'ordinamento giuridico nel suo complesso, un altro strumento in grado di arrecare efficace e pronta risposta al di fuori del diritto penale (principio del diritto penale del fatto e necessaria offensività in combinato disposto con il principio di *extrema ratio*). In sostanza, si dovrebbero tendenzialmente evitare i reati di mera disobbedienza e trovare rimedi giuridici alternativi per arginare certe pratiche o comportamenti.

I reati di evento, invece, sembrano confliggere ontologicamente con l'idea preventiva. Questi, infatti, presuppongono per definizione che sia stata arrecata una lesione al bene giuridico protetto, postulando con ciò il superamento della soglia della mera esposizione a pericolo. Tale tipologia di reato non garantisce pertanto alcun risultato pratico dal punto di vista della prevenzione.

Così pure se si considera il versante processuale, molteplici sono le criticità che fanno apparire il ricorso al diritto penale un'alternativa tutt'altro che efficace dal punto di vista della prevenzione: basti pensare al tempo necessario per la celebrazione di un processo penale che possa dirsi rispettoso delle garanzie cristallizzate nel dettato costituzionale (artt. 24, 110, 111 Cost.); all'innesco di meccanismi perversi che, grazie a cavilli procedurali o altri espedienti, permettono la maturazione del termine di prescrizione del reato. E si tratta di evenienze tutt'altro che rare, dalle quali deriva una diffusa sfiducia verso il sistema 'giustizia'.

Diverse considerazioni discendono invece dall'opzione del diritto penale in chiave repressiva e per finalità simboliche. In questa accezione, però, l'attenzione sarà riposta nella prontezza ed efficacia della risposta punitiva. La reale vulnerabilità della Rete rischia di essere amplificata per effetto della notizia della realizzazione di un fatto lesivo al quale non consegua una pronta risposta sanzionatoria.

La teoria assoluta della pena è stata però da tempo ritenuta incompatibile con uno Stato democratico di diritto, laico e rispettoso dei diritti umani[28].

Si può allora sostituire la prospettiva meramente repressiva con quella di prevenzione generale positiva, in forza della quale la minaccia della sanzione penale dovrebbe fungere da pungolo della coscienza morale del cittadino, sì da farla convergere attorno ad un nucleo forte di valori socialmente condivisi[29].

---

[27] M. DONINI, *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà*, in *Diritto penale comparato, internazionale ed Europeo*, a cura di A. BERNARDI – M. DONINI – V. MILITELLO – M. PAPA – S. SEMINARA, Milano, 2004, 104 ss.

[28] L. MONACO, *Prospettive dell'idea dello 'scopo' nella teoria della pena*, Napoli, 1984, 3 ss.

[29] L. FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, Roma, 2008, 239 -270; G. FIANDACA – G. DI CHIARA, *Una introduzione al diritto penale. Per una lettura costituzionalmente orientata*, Napoli, 2003, 15 - 40.

3.1 La responsabilità dell'internet service provider

Dalle prassi emerge poi un problema di carattere culturale connesso al coordinamento tra le logiche tradizionali con le quali lavora il penalista e la dimensione comportamentale generata dalla tecnologia[30]. Emblematica, a tal proposito, è la tesi che ritiene penalmente responsabile, per i fatti posti in essere dagli utenti, l'internet service provider (ISP), in quanto garante ai sensi dell'art. 40 capoverso del codice penale in combinato disposto con le singole fattispecie incriminatrici di parte speciale[31]. In pratica, i prestatori di servizi della società dell'informazione assumerebbero il ruolo di tutori e garanti della legalità, in virtù del ruolo rivestito e per la vicinanza con le fonti del rischio-reato[32]. Si ritiene che questa impostazione tradisca alla radice la conoscenza della stessa architettura di Rete, paragonata a corsie autostradali sulle quali viaggiano i pacchetti di dati[33]. Il suo utilizzo per fini illeciti dipende dal contenuto e dai fini perseguiti dall'utente che mette in circolazione i dati, effettua operazioni o in generale svolge determinate attività. Gli ISP sono neutrali rispetto ai contenuti che veicolano, almeno fintanto che assolvono funzioni meramente tecniche di inoltro e avanzamento dei dati e non sono mittenti o destinatari del traffico, o non compiono attività di manipolazione o selezione (c.d. indicizzazione). Addebitare una responsabilità penale per omesso impedimento dell'evento significa travolgere e azzerare l'essenza stessa del principio basilare di neutralità, come terzietà e indipendenza rispetto ai contenuti. Per operare un parallelismo con il mondo reale, sarebbe come incriminare il postino per concorso nella diffamazione per aver consegnato una lettera infamante.

Almeno tre sono le argomentazioni adducibili contro la qualifica di garante in capo al provider[34]. In primo luogo, sulla base dell'attuale sviluppo della tecnologia, si deve

---

30 G. PICA, "*internet*", cit., 430, suggerisce il ripensamento di talune categorie della dogmatica, come il concetto di "azione" ed "evento".

31 U. SIEBER, *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, riv. trim. dir. pen. econ., 1997, 755 e ss.; Id., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Parte seconda*, riv. trim. dir. pen. ec., Milano, 1997, 1193 e ss.

32 A. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano*, su: www.penalecontemporaneo.it; D. DE NATALE, *Responsabilità penale dell'internet service provider per omesso impedimento e per concorso nel reato di pedopornografia*, in *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, a cura di G. GRASSO – R. SICURELLA, Giuffrè, 2011.

33 G. Pica, «*internet*», cit., 430 ss..

34 In giurisprudenza, celebre è il caso Google vs Vividown, ove la procura della Repubblica ha tentato di attribuire al provider la titolarità di una posizione di garanzia: Tribunale di Milano, sentenza 24 febbraio – 2 aprile 2010, n. 1972, est. MAGI; F. SGUBBI, *Parere pro veritate*, *Dir. inf.*, Milano, 2009, 746 ss..; A. ALBAMONTE, *La responsabilità penale dell'internet provider tra libertà di comunicazione e tutela dei singoli*, *Quest. giust.*, Torino, 2010, 184 ss.; L. BUDESCHI, *Caso Google: libertà di espressiome in internet e tutela penale dell'onore e della riservatezza*, *Corr. merito*, 2010, 960 ss.; F. DI CIOMMO, *Programmi filtro e criteri di imputazione/esonero della responsabilità on line. A proposito della sentenza Google/Vivi Down*, in *Dir. inf.*, 2010, 829 ss.; V. PEZZELLA, *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, in *Giur. merito*, Milano, 2010, 2232 ss.
Corte di Appello, sentenza 21 dicembre 2012 – 27 febbraio 2013, n. 8611, est. MILANESI, che conferma la ricostruzione del giudice di prime cure in ordine alla carenza di un obbligo giuridico di impedimento dell'evento-reato in capo al provider della posizione di garanzia. F. G. CATULLO, *Atto secondo dell'affaire google vividown: società della registrazione e consenso sociale*, *Cass. pen*., Milano, 2013/9, 3256 ss.; A. PIROZZOLI, *La responsabilità dell'internet service provider. Il nuovo orientamento giurisprudenziale nell'ultimo caso google*, su: www.rivistaaic.it

constatare l'irrealizzabilità pratica di controllo della gigantesca mole di dati che transita ogni minuto nei server.

In secondo luogo, pur ammettendo che una simile opzione fosse tecnicamente possibile, occorre segnalare che gli ISP dovrebbero integrare il proprio organico con personale dotato di competenze giuridiche necessarie per individuare la sussistenza di un fatto di reato. Senza considerare che, nei casi dubbi, per non incorrere in alcun addebito penale, gli ISP probabilmente sarebbero inclini a riversare ogni comunicazione sospetta sulle procure della Repubblica, con conseguente sovraccarico e collasso dell'operatività di queste ultime.

Ma il problema cruciale risiede nell'individuazione della legittimazione dell'obbligo di prevenire la commissione di reati e del corrispondente esercizio di poteri impeditivi[35]. A fronte di tali obblighi di neutralizzazione delle fonti di rischio si dovrebbero attribuire ai providers effettivi poteri d'azione. In proposito, sono già emerse perplessità legate alla direttiva europea che imponeva, ai fornitori delle comunicazioni, la raccolta dei dati sulla navigazione per esigenze investigative, di prevenzione e repressione dei reati, trasfusa in Italia nell'art. 132 d.lgs. 196/2003 e sfociata nella pronuncia della Corte di Giustizia dell'8 aprile 2014 (vedi, infra, paragrafo 9). Questa normativa imposta da una direttiva UE (dir. 2006/24/UE) ha legittimato un'enorme accumulazione di informazioni sul traffico delle comunicazioni. A causa della genericità delle prescrizioni di legge, questi dati restavano esposti a elevati rischi di indebiti utilizzi per fini di profitto: si pensi alle diffuse pratiche commerciali di compravendita per finalità di *marketing*. In sostanza: *Quis custodiet ipsos custodes*[36]?

Per negare la titolarità della posizione di garanzia in capo ai providers, la giurisprudenza si è limitata a richiamare le disposizioni del d. lgs. 70/2003 sull'*e-commerce* (artt. 14 - 17), che negano l'esistenza di un obbligo generale di sorveglianza ed ogni profilo di responsabilità fin tanto che il provider non interferisca con il contenuto delle comunicazioni o non sia mittente o destinatario delle stesse o non abbia avuto piena conoscenza dell'illiceità delle stesse. Sussiste, invece, un dovere di collaborazione con l'autorità giudiziaria a fronte della conoscenza di notizie di reato[37].

Cassazione penale, sez. III, sentenza 17 dicembre 2013 (dep. 3 febbraio 2014), n. 5107, Rel. ANDRONIO, conferma la sentenza di secondo grado ed afferma che, pur non sussistendo alcun obbligo preventivo di impedimento degli illeciti commessi dagli utenti, resta comunque il dovere di segnalazione all'autorità giudiziaria. A. INGRASSIA, *La sentenza della Cassazione sul caso Google*, su: www.penalecontemporaneo.it

[35] Sulla sussistenza dell'obbligo di garanzia ex art. 40, co. 2 c.p., parte della prassi resta fedele alle teorie formali: vedi, *supra*, caso Google vs. Vividown. Altra parte ha preferito aderire alla teoria funzionale, che individua la titolarità della posizione di garanzia in capo a determinate categorie di soggetti, in virtù della vicinanza alle fonti di pericolo e della possibilità di controllo su queste (criteri fattuali): Cassazione penale, sentenza 4 luglio 2007, n. 25527; Cassazione penale, Sez. IV, ud. 29 gennaio 2013 (dep. 19 febbraio 2013), n. 7967, in ambito medico.

[36] GIOVENALE, *VI Satira*. Si tratta del classico problema del controllo di chi dovrebbe esercitare ruoli di vigilanza. Chi può infatti essere sicuro che, una volta proclamati tutori dell'ordine sulla Rete, gli ISP non si lascino sopraffare dal potere e si trasformino in una minaccia ancor peggiore di quella che si voleva contrastare? Forti sono le analogie di situazione rispetto agli esperimenti compiuti agli inizi degli anni sessanta da S. MILGRAM o di quelli condotti a Stanford nel 1971 da P.G. ZIMBARDO. S. MILGRAM, *Obedience to Authority*, HarperCollins Publisher, 1974, trad. It. R. BALLABENI, *Obbedienza all'autorità*, Torino, 2003; P. G. ZIMBARDO, *The Stanford Prison Experiment a Simulation Study of the Psychology of Imprisonment*, P. G. ZIMBARDO Inc., 1972.

[37] Gli artt. 14 – 15 – 16, d. lgs. 70/2003, in relazione alle attività di mero trasporto (*mere conduit*), di memorizzazione temporanea di informazioni (*caching*) e di memorizzazione di informazioni (*hosting*),

Rispetto all'obiettivo di tutela della sicurezza delle reti e delle informazioni, la sola sanzione penale è un'arma spuntata, perché il paradigma preventivo necessita dell'elaborazione di modelli organizzativi basati su meccanismi di collaborazione multilivello tra i soggetti che interagiscono nell'ambiente virtuale.

4. La sicurezza informatica come bene comune: una concezione socio-economica

La sicurezza del *web* è *"precondizione per la creazione di un ambiente virtuale affidabile per lo scambio di servizi su scala mondiale*"[38]. Nella ricerca di una strategia efficace di tutela può essere utile richiamare il concetto di bene comune[39]. Si tratta di una categoria che ha conosciuto una nuova fioritura a seguito delle ricerche condotte dal premio nobel Elinor Ostrom, sulle capacità di autogestione di determinate risorse naturali soggette ad esaurimento, da parte delle popolazioni locali (corsi d'acqua, fauna acquatica, etc.)[40]. L'aggettivo 'comune' sta ad indicare la libera accessibilità al bene, la gestione condivisa e la sua utilità per la comunità[41].

Molteplici sono le ragioni per le quali scomodare questa teoria. Parlare di 'beni comuni' in luogo di beni pubblici consente di fuoriuscire dagli schemi tradizionali di classificazione economica e giuridica[42]. La dicotomia beni pubblici o privati viene così spezzata e ciò stimola a pensare ad una disciplina giuridica alternativa, che tenga conto delle caratteristiche dei nuovi fenomeni[43]. In questo senso, i *Commons* costituirebbero una "*tipologia di diritti fondamentali di ultima generazione*" finalmente emancipata sia dal diritto di proprietà, sia dal modello pubblicistico autoritario. L'etichetta 'bene comune' non è, a ben vedere, espressione ricercata che designa un nuovo diritto fondamentale, ma si riferisce ad un ambiente particolarmente favorevole allo sviluppo di un complesso di diritti e libertà fondamentali, vecchi e di nuovo conio: si pensi alla

---

affermano che il prestatore è esente da responsabilità fintanto che non interferisca con i contenuti o non sia mittente o destinatario degli stessi e non abbia effettiva conoscenza dell'illiceità delle informazioni o delle attività. L'art. 17 prevede l'assenza di un obbligo generale di sorveglianza e di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecite.

[38] Relazione alla proposta di direttiva COM (2013) 48 final – 2013/0027 (COD).

[39] 'Beni comuni' è la traduzione italiana di '*Commons*': il vocabolo inglese riesce meglio ad esprimere l'essenza di questi beni in termini di condivisione da parte di comunità più o meno ampie. Volendo prospettare una definizione di sintesi, si può descrivere i Commons come: "beni *utilizzati da più individui, rispetto ai quali si registrano - per motivi diversi - difficoltà di esclusione e il cui "*consumo*" da parte di un attore riduce le possibilità di fruizione da parte degli altri: sono generalmente risorse prive di restrizioni nell'accesso e indispensabili alla sopravvivenza umana e/o oggetto di accrescimento con l'uso*". Definizione presa in prestito da Wikipedia.

[40] E. O*STROM, Governing the Commons: the Evolutions of Institutions for Collective Action*, Cambridge, 1990; trad. it. *Governare i beni collettivi*, Marsilio, 2006; S. RISTUCCIA, *L'importanza di una riflessione sui commons. A proposito del premio Nobel a Elinor Ostrom*, Su: http://www.jus.unitn.it

[41] Cfr. Commissione Rodotà 2007 incaricata di riformare il libro terzo del codice civile sulla proprietà nelle parti relative alla proprietà pubblica, *sub* U. MATTEI, *Beni comuni. Un manifesto*, Bari, 82.

[42] C. IANNELLI, *Beni pubblici versus beni comuni*, nel quale l'A. precisa che la categoria nasce come critica dei beni pubblici in particolare, perché Demanio e beni pubblici altro non sarebbero che una mera variante del diritto di proprietà, che da questo si distinguerebbe solo per il dato soggettivo, ossia per essere imputato, invece che a un soggetto privato, ad un ente pubblico. Su: http://www.forumcostituzionale.it

[43] U. MATTEI, *Beni comuni*, cit., VII; D. BOLLIER, *Lo sviluppo del paradigma dei beni comuni*, cit., 34 ss.

libertà di manifestazione del pensiero, al diritto all'informazione, al diritto di critica e di cronica, di riunione, all'autodeterminazione informativa, alla libertà informatica intesa come libertà di accesso al *web*, etc[44]. La Rete appartiene, in questo senso, alla categoria dei beni collettivi strumentali: mediante la loro tutela si ottiene indirettamente protezione anche per i beni giuridici finali[45]. Analogamente la sicurezza delle reti e delle informazioni si atteggia a bene comune, in considerazione della rilevanza del suo oggetto (la Rete e le informazioni, appunto) e pur essendo un bene immateriale e artificiale.

L'accezione che qui si sposa di bene comune è di tipo costruttiva, non polemica e distruttiva, come qualche autore ha prospettato ravvisando nei *Commons* una strutturale incompatibilità con la gerarchia[46]. Si vuole piuttosto porre l'attenzione sul peculiare modello di gestione incentrato sul rapporto d'indispensabilità tra il bene e la collettività. Note comuni ai vari modelli di sfruttamento razionale e sostenibile delle risorse soggette ad esaurimento analizzati da Elinor Ostrom sono: la cooperazione, l'affidamento reciproco fra gli appartenenti della comunità e una certa dosa di dinamismo e pragmaticità necessaria per far fronte alle contingenze. Queste qualità, in particolari, appaiono assenti nella legge, quale entità statica e monolitica che fatica a tenere il passo con la realtà, tanto più se in costante e rapidissimo divenire come il cyberspazio[47].

La sicurezza del *web* è inoltre un bene non escludibile, perché a prescindere dal soggetto che la garantisce e ne sopporta i relativi costi, tutti gli utenti ricevono vantaggi dall'utilizzo di una Rete sicura. Non è però possibile quantificare l'esatto beneficio che ciascuno trae da una navigazione esente da rischi e pericoli, né risulta agevole escluderne dal godimento taluni soggetti, a meno di non voler sopportare ulteriori elevatissimi costi. Dunque alla non escludibilità del bene corrisponde l'indivisibilità dei benefici addotti alla collettività. Questa caratteristica mal si concilia con la logica di mercato che impone l'estromissione degli individui che non sono disponibili a pagarne il prezzo.

Lo schema dei beni comuni non adotta semplicemente un punto di vista alternativo, ma presuppone individui molto diversi dal *homo oeconomicus* della *Economic Analysis of Law*[48]. Quest'ultimo individuo orienta le proprie scelte unicamente in base a

---

[44] M. BETZU, *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, AIC, 2012/4, su: http://people.unica.it/marcobetzu/files/2013/09/Interpretazione-e-sovra-interpretazione-dei-diritti-costituzionali-nel-cyberspazio.pdf

[45] Si pensi all'ambiente, la cui tutela consente anche di preservare la salute. G. MARINUCCI – E. DOLCINI, *Manuale*, cit., 207 ss.; E. CORN, *Il principio di precauzione*, cit., 87 ss.

[46] Cfr. U. MATTEI, *Beni comuni*, cit., 81.

[47] T. PADOVANI, *Alla ricerca di una razionalità penale*, *Riv. it. dir. pen. proc.*, 3/2013, 1087 – 1092, sul carattere rigido del diritto penale come tecnica coercitiva.

[48] Questo movimento, nato a cavallo tra gli anni cinquanta e sessanta del Novecento, presso la scuola di Chicago, ha elaborato una concezione economica del reato. Essa interpreta il diritto come insieme di incentivi indirizzati ai consociati, i quali decidono se conformarsi o meno ad una norma giuridica, sulla base di un razionale calcolo costi/benefici. In sostanza, nella valutazione della preferenza del comportamento da seguire, al criterio della giustizia si sostituisce quello dell'efficienza: soltanto dopo aver stimato il prezzo della disobbedienza rispetto ai vantaggi ottenibili dai possibili comportamenti alternativi, gli individui decideranno se adeguarsi al precetto o violarlo. G. BECKER, *Crime and Punishment: An Economic Approach*, 16 *Journal of Politics and Economics* 169 (1968); R. A. POSNER, *The Economic Approach to Law*, *Texas Law Review* 757 (1975).

considerazioni perfettamente razionali, improntate alla logica costi-benefici[49]. In assenza di prospettive di guadagno, egli sarà portato a rifiutarsi di contribuire alla sicurezza di Internet senza coercizione[50].

Il prototipo di uomo disponibile a sobbarcarsi parte dei costi per la sicurezza è più simile a quello descritto dalla psicologia cognitivista[51]. In particolare, l'uomo cognitivista è un essere diviso in due componenti: una intuitiva, spontanea, automatica, irrazionale, deputata alle azioni meccaniche e dominata dalle emozioni; l'altra, lenta e riflessiva, impegnata nelle valutazioni orientate a criteri logici e razionali e protesa al controllo delle emozioni. Nelle attività quotidiane e poco complesse, la prima componente domina sulla seconda che rimane sopita, fintanto che non si riscontri l'esigenza di compiere operazioni di ragionamento. Tuttavia, questo soggetto, quando si trova a dover assumere una decisione, non si attiene sempre al criterio dell'invarianza della scelta razionale, come vorrebbe la componente razionale del suo essere. Al contrario, la sua scelta risulta influenzata da molteplici fattori, soprattutto inconsci e irrazionali. Importanti studi hanno dimostrato come la mente umana cada in veri e propri *bias* cognitivi, che fanno apparire come migliore un'opzione che, in base alla logica costi/benefici, in realtà, non lo è[52]. Per esempio, un grande peso hanno le modalità con le quali sono formulati i quesiti: a seconda dei presupposti maggiormente posti in evidenza possono aversi distinte preferenze. Si pensi, alla diversa capacità di accettazione tra la prospettazione di una spesa come perdita non compensata, piuttosto che come polizza assicurativa.

Il merito principale degli studi di Elinor Ostrom consiste nella dimostrazione pratica dell'inesistenza di un sistema di *governance* predefinito, valido per tutte le situazioni. Ciascun bene comune necessita di un modulo organizzativo specifico, che tenga conto delle sue peculiarità. La sua ricerca fornisce inoltre una base empirica cui ancorare la sostenibilità di un paradigma di collaborazione collettiva per raggiungere standard elevati di sicurezza della Rete e delle informazioni.

5. La Proposta di direttiva UE sulla sicurezza delle reti e dell'informazione

Orientata verso un sistema di gestione condivisa tra pubblico e privato, la recente proposta di direttiva dell'Unione europea mira a garantire la sicurezza delle reti e delle

---

[49] A. BONDI, *La ricchezza delle sanzioni*, in *Il prezzo del reato*, a cura di A. BONDI, GA. MARRA e P. POLIDORI, Torino, 2010,103 – 130.

[50] F. A. VON HAYEK, *Legge, legislazione e libertà. Critica dell'economia pianificata*, trad. Milano, 2010, 417 ss., il quale, parlando di beni collettivi, osserva come "*(..) si può pensare che (...) la coercizione non sia necessaria, perché il riconoscimento di un interesse comune soddisfacibile soltanto con un'azione comune porterebbe un gruppo di persone ragionevole ad aderire volontariamente in vista dell'organizzazione di tali servizi. Sebbene ciò possa avvenire in gruppi relativamente piccoli non è certamente vero in quelli più numerosi. Trattandosi di grandi numeri, molti individui, per quanto desiderino l'attuazione dei servizi in questione, pensano, a ragione, che i risultati non varieranno se loro contribuiranno o meno alle spese. Né un individuo che acconsente a contribuire avrà l'assicurazione che gli altri faranno altrettanto, e che quindi si raggiunga lo scopo. Invero, considerazioni perfettamente razionali porteranno ogni individuo a rifiutarsi a contribuire, sperando però che gli altri lo facciano*".

[51] D. KAHNEMAN, *Thinking, Fast and Slow*, 2001, trad. it. L. SERRA, *Pensieri lenti e veloci*, Milano, 2012.

[52] D. KAHNEMAN - A. TVESKY, *Scelte, valori e frame*, in id. *Pensieri lenti e veloci*, 511.

informazioni, nell'ambito della politica di "*mantenimento e sviluppo di uno spazio di libertà, sicurezza e giustizia*"[53].

L'Unione europea si era già dimostrata consapevole delle potenzialità offensive scaturenti da un uso distorto di Internet, amplificato dalla sua dimensione reticolare e globale. La Convezione di Lisbona ha infatti previsto l'inserimento della criminalità informatica tra le nove materie tassative che consentono l'adozione di norme penali (art. 83 TFUE)[54]. Inoltre, la direttiva relativa agli attacchi contri i sistemi di informazione (dir. 2013/40/UE) sostituisce la decisione quadro 2005/222/GAI ed enuncia una serie di obblighi di criminalizzazione coincidenti con le fattispecie introdotte dal legislatore italiano nel 1993 e nel 2008.

La proposta di direttiva del 2013 assume come presupposto imprescindibile per una strategia efficace di contrasto al *cybercrime* la dimensione ultrastatuale del fenomeno, dalla quale deriva la necessità di armonizzare le discipline penalistiche sostanziali e processuali nazionali. In effetti, gravi incidenti al sistema informatico di un paese possono ripercuotersi avverso i sistemi degli altri stati membri o delle strutture istituzionali dell'Unione[55].

Il legislatore UE delinea un sistema preventivo basato sulla predisposizione di adeguate misure di gestione del rischio-reato, che richiede il diretto contributo dal basso, da parte degli operatori del mercato e delle pubbliche amministrazioni[56]. Questo aspetto avvicina la proposta alle teorie sul bene comune, nell'enfatizzazione del ruolo attivo riservato a taluni componenti della comunità virtuale. Le analogie si arrestano qui. Infatti, a differenza dei modelli di gestione dei *Commons* non è previsto un diretto coinvolgimento di tutti gli utenti della Rete, ma soltanto di quelli che la popolano e sfruttano per fini economici. Un motivo di tale opzione politica può essere intravisto nella posizione che rivestono gli operatori del mercato, quali snodi ove si concentrano elevate quantità di comunicazioni e, in quanto tali, possono essere veicoli o occasioni di delitto.

Il progetto di direttiva non abbandona la ripartizione gerarchica dei compiti, ma disegna una struttura organizzativa piramidale, nella quale la creazione di un circuito di scambio sicuro delle informazioni sensibili e riservate tra autorità competenti costituisce uno degli elementi centrali nel coordinamento dell'azione di prevenzione del *cybercrime* a livello dell'Unione. Alla Commissione europea, in posizione di vertice e raccordo con le Autorità nazionali competenti, è conferito il potere di adottare, mediante atti di esecuzione, un piano unionale di collaborazione in materia di sicurezza delle reti

---

[53] Considerando n. 2, proposta di direttiva, COM (2013) 48 final – 2013/0027 (COD), sulla sicurezza delle reti e delle informazioni.

[54] La Commissione europea ha emanato la comunicazione JOIN(2013)1 del 7 febbraio 2013, la quale pone, tra gli obiettivi primari dell'azione dell'Unione indicati nella Strategia di sicurezza interna (SSI) 2010-2014, l'aumento dei livelli di sicurezza per i cittadini e le imprese nel ciberspazio costituisce uno degli obiettivi.

[55] Al Considerando 3 della proposta di direttiva si afferma: "*gravi perturbazioni di tali sistemi in uno Stato membro possono ripercuotersi sugli altri Stati membri e avere conseguenze in tutta l'UE. La resilienza e la stabilità delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno.*".

[56] M. DONINI, *Il volto attuale dell'illecito penale*, cit., 107, il quale rileva come l'emergenza legislativa del rischio, a partire dal diritto penale del lavoro, fa riferimento al criterio della 'riduzione al minimo del rischio' (concetto introdotto dalla giurisprudenza nella concretizzazione degli obblighi di aggiornamento tecnologico del datore di lavoro genericamente dettati dall'art. 2087 c.c., imposti dalla UE).

e delle informazioni (SRI), con l'obiettivo di minimizzare l'impatto d'incidenti a carico delle reti e dei sistemi informativi relativi ai servizi principali prestati. Compete ad essa anche il compito di emanare linee guida e buone pratiche organizzative uniformi per tutti gli Stati UE e può concludere accordi con altri stati o organizzazioni internazionali (art. 13). Deputata all'assistenza tecnica degli Stati membri e della Commissione, l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) agevola la diffusione e lo scambio di buone pratiche (considerando 13). Inoltre, in seno ad Europol opera, a partire dagli inizi del 2013, il Centro europeo per la lotta alla criminalità informatica.

A livello statale, Autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi verranno dotate dei poteri necessari per indagare i casi di mancato rispetto, da parte delle amministrazioni pubbliche o degli operatori del mercato, degli obblighi organizzativi loro imposti (art. 14) e degli effetti sulla sicurezza delle reti e dei sistemi informative. Infine, squadre di pronto intervento informatico (CERT), operanti sotto la supervisione dell'Autorità nazionale competente, assolveranno il compito di trattare gli incidenti e i rischi secondo una procedura precisa, avvalendosi di un'infrastruttura di informazione e comunicazione sicura e resiliente a livello nazionale, a sua volta compatibile e interoperabile con il sistema sicuro di scambio di informazioni[57].

Il fulcro del funzionamento del complesso sistema è costituito però dalle imprese e dalle pubbliche amministrazioni, paragonabili a sentinelle che devono allertare i livelli superiori in relazione ai rischi o incidenti coi quali vengono in contatto.

L'allegato 2 si preoccupa di specificare quali siano i soggetti qualificati come operatori di mercato: si tratta essenzialmente dei fornitori di servizi dell'informazione[58]. Essi dovranno ottemperare a due obblighi: da un lato, sono tenuti a dare comunicazione ai livelli gerarchici superiori degli incidenti informatici nei quali incorrono; dall'altro, devono predisporre misure tecniche e organizzative tendenti a "*prevenire e minimizzare l'impatto di incidenti a carico delle reti e dei sistemi informativi relativi ai servizi principali prestati, assicurando in questo modo a continuità dei servizi supportati da tali reti e sistemi informativi*"[59]. Gli operatori di mercato e le p.a. non sono soltanto destinatari di meri obblighi di astensione o di divieti, ma sono chiamati all'individuazione delle cautele da osservare per prevenire i rischi d'incidenti e sono tenuti a trasfonderli nei propri modelli organizzativi. In questo senso, la proposta sembra suggerire la scelta di un modello preventivo basato su una sorta di 'autoregolamentazione regolata', nella misura in cui la legge impone che siano gli stessi attori che agiscono sul mercato virtuale a dotarsi di regole da osservare. La

---

[57] L'art. 10 della proposta di direttiva istituisce la procedura di preallarme, ossia la segnalazione da parte delle autorità nazionali competenti e della Commissione, attraverso la rete di collaborazione facente capo ad ENISA di rischi o incidenti di portata sovranazionale.

[58] "Allegato 2. - *Elenco degli operatori del mercato*
Operatori di cui all'articolo 3, paragrafo 8, lettera a):
1. Piattaforme di commercio elettronico
2. Portali di pagamento su internet
3. Reti sociali
4. Motori di ricerca
5. Servizi nella nuvola (cloud computing)
6. Negozi online di applicazioni."

[59] Art. 14 § 1, proposta di direttiva COM (2013) 48 final – 2013/0027 (COD).

Commissione avrà il compito di coordinare e rendere uniforme ed omogeneo il panorama europeo delle prescrizioni a contenuto cautelare e precautelare, mediante l'emanazione di linee guida e buone pratiche; le Autorità nazionali indipendenti, infine, saranno deputate, tra le altre cose, alla sorveglianza del corretto adempimento e osservanza degli obblighi prescrizionali prescritti agli attori privati.

La proposta si preoccupa, tuttavia, di specificare che l'adozione delle misure tecniche e tecnologiche non deve tradursi in un onere di spesa troppo gravoso per le imprese. Si vuole così evitare di comprimere la libera concorrenza e la libertà d'iniziativa economica sul mercato del *web*, a favore della creazione di oligopoli o monopoli da sempre nemici delle politiche economiche dell'Unione europea[60]. Si suggerisce piuttosto all'operatore di valutare la scelta delle misure organizzative e tecnologiche da adottare in base al criterio di proporzione rispetto al rischio cui sono esposti la Rete o il sistema informativo, alla luce dello stato dell'arte. In sostanza, trasmigra verso il settore della sicurezza delle Reti e delle comunicazioni il modello preventivo caratterizzato dall'osservanza di protocolli, linee guida e buone pratiche già sperimentato in altri ambiti, come quello medico, lavoristico, etc.[61].

Questo sistema che introduce il diretto coinvolgimento degli attori principali che gestiscono i servizi nel *web* dovrebbe scongiurare il rischio di far ricadere il costo della sicurezza sull'utente finale. Ma di riflesso potrebbe determinarsi un aumento dei costi dei servizi erogati. L'internauta, ad ogni modo, non è del tutto estromesso dall'attività di contrasto del *cybercrime*: si pensi alla necessaria dotazione delle misure di sicurezza quale condizione obiettiva di punibilità del reato di accesso abusivo a sistema informatico (art. 615-*ter*). Sicchè l'accesso al sistema informatico privo di tali misure non può configurarsi come reato. E' evidente tuttavia come i modelli preventivi siano pensati soprattutto per le società o gli enti, ossia per strutture organizzative complesse, caratterizzate da una ripartizione dei ruoli e delle responsabilità e non per monadi isolate che popolano la Rete.

La generalizzazione dell'obbligo di adozione delle misure organizzative per gli operatori compresi nell'elenco di cui all'allegato 2 dovrebbe poi servire a contenere il numero dei c.d. *free riders*, ossia di quei fornitori che non apprestano alcuna precauzione o protezione del sistema, ma sfruttano i benefici di una Rete sicura ottenuta attraverso il comportamento virtuoso degli altri concorrenti diretti o indiretti, senza assumersi alcuna parte dei costi.

6. Criticità del diritto penale della sicurezza

L'assetto organizzativo delineato si chiude con la previsione dell'apparato sanzionatorio. E' imposto un generico obbligo di adozione di sanzioni dissuasive, efficaci e proporzionate, demandando alla valutazione discrezionale di ciascuno stato l'opzione relativa al ricorso allo strumento penale[62].

---

[60] Considerando 25, proposta di direttiva COM (2013) 48 final – 2013/0027 (COD).

[61] Sulla storia delle *check list*, A. GAWANDE, *Check list. Come fare andare meglio le cose*, Torino, 2011.

[62] Capo V –Disposizioni finali

Art. 17 - Sanzioni

1.Gli Stati membri stabiliscono le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e prendono tutti i provvedimenti

Quali spazi può ritagliarsi il diritto penale in questo quadro organizzativo?

In un simile modello di gestione condivisa, sorretto da regole cautelari e precauzionali, la sanzione penale potrebbe fungere da deterrente, da prevenzione generale positiva e da incentivo alla loro osservanza[63].

Ma occorre che il legislatore nazionale sia molto cauto nell'opzione di politica criminale, poiché, come acutamente osservato, "*l'incertezza è un tratto strutturale della strategia di prevenzione dell'insicurezza*"[64]. Si tratterebbe di una strada già battuta nei settori della sicurezza nei luoghi di lavoro, alimentare e nella disciplina della responsabilità degli enti da reato. Questi sono ambiti nei quali la dinamicità sociale richiede risposte immediate in termini di presidi per la sicurezza, che soltanto gli attori che vivono e si muovono in quella realtà sono in grado di apprestare con un maggior margine di efficacia, efficienza e completezza[65]. Ma proprio in questi settori, dove le scienze non forniscono risposte esatte e non esistono teoremi perfetti, a causa di una mescolanza di variabili pressoché imprevedibili, si devia verso il criterio della minimizzazione del rischio affiancato dalla proliferazione di obblighi da cui scaturisce una eterogeneità di risposte sanzionatorie (in sede civile, amministrativa e penale)[66]. Emergono preoccupanti profili di tensione con la riserva di legge, laddove sono i modelli organizzativi a descrivere la tipicità della condotta illecita; con la causalità che risulta fortemente rimodellata in senso normativo ed è sempre meno accertata facendo ricorso a rapporti di causa-effetto scientificamente fondati[67]. Infine, rischia di perdersi alla deriva il principio di responsabilità penale personale, sospinto verso l'incerto dalle onde prodotte dall'ascrizione della responsabilità penale per eventi nè voluti né preveduti *hic et nunc*.

---

necessari per la loro applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano tali disposizioni alla Commissione entro la data di attuazione della presente direttiva e provvedono a dare immediata notifica di ogni successiva modifica.

2. omissis

[63] Relazione alla proposta di direttiva COM (2013) 48 final – 2013/0027 (COD). Ga. Marra, *Prevenzione mediate organizzazione e diritto penale. Tre studi sulla tutela della sicurezza sul lavoro*, Giappichelli, 2009, 114, il quale precisa: "*La sanzione è efficiente quando è in grado di rimarcare la differenza tra soggetti cooperativi e soggetti non cooperativo*". Sul principio di precauzione come concretizzazione dell'attuale diritto penale della sicurezza: E. CORN, *Il principio di precauzione*, cit., 38 - 59.

[64] GA. MARRA, *Prevenzione mediate organizzazione*, cit., 102.

[65] GA. MARRA, *Prevenzione mediante organizzazione*, cit., 113 - 114, il quale acutamente osserva come "*in un quadro conoscitivo imperfetto e instabile*", "*il diritto penale è efficiente solo quando la maggioranza dei destinatari volontariamente si comporta nel senso voluto dalla norma. (…). La capacità di vincolo delle prescrizioni normative anche penalmente sanzionate dipende molto di più dal timore reverenziale indotto dalla minaccia di pena, dall'autorevolezza della richiesta di azione, dall'utilità e dalla giustificazione del comportamento richiesto in rapporto ai problemi collettivi che si dichiara di voler risolvere"*.

[66] M. DONINI, *Il volto attuale dell'illecito penale*, cit., 104 -117. "*Il rischio non si limita a precedere il pericolo, ma assume un altro oggetto e un altro criterio di valutazione*". "*L'oggetto del rischio non è un fattore determinato, ma l'interazione dinamica dei fattori presenti in una situazione data*".

[67] GA. MARRA, *Verso un diritto penale sperimentale? Metodo ed empiria del canone dell'extrema ratio*, Fano, 2012, 103 - 104.

7. Verso la definizione giuridica di un concetto nebuloso? La sicurezza informatica nella proposta di direttiva sulla sicurezza delle reti e dell'informazione

La proposta di direttiva formula un'espressa definizione della sicurezza informatica[68]. In effetti, quest'ultima, di per sé presa, si risolve in un'espressione di sintesi incapace di esprimere contenuti giuridici immediatamente identificabili[69]. L'Unione colloca la sicurezza in generale tra gli obiettivi della sua azione e ne impone uno standard elevato, da raggiungere attraverso l'adozione di "*misure di prevenzione e lotta contro la criminalità (...) e, se necessario, il ravvicinamento delle legislazioni penali*" (art. 67 TFUE)[70].

Il termine sicurezza isolatamente considerato evoca una condizione e, al tempo stesso, un sentimento, che si ricollega alla percezione di essere esenti da situazioni pericolose o rischiose, o comunque, come capacità di prevenire, fronteggiare, o attenuare evenienze spiacevoli. Nell'ambito dell'informatica, essa designa "*l'insieme delle tecniche e dei dispositivi, sia software sia hardware, mediante i quali si attua la protezione di dati e sistemi informatici*"[71].

Secondo l'art. 3 n. 2 della proposta di direttiva, la sicurezza informatica consiste nella "*capacità di una rete o di un sistema informativo di resistere, a un determinato livello di riservatezza, a eventi imprevisti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi offerti o accessibili tramite tale rete o sistema informativo*"[72]. In sostanza, essa mira alla conservazione del sistema, della sua funzionalità e all'integrità dei dati in essa contenuti. Il grado di sicurezza si valuta in base alla capacità di resistenza agli attacchi esterni: tale caratteristica è nota come resilienza. Procedendo con l'ausilio dell'analisi semantica, in informatica quest'ultima caratteristica indica la "*capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati*"[73]. Essa implica una certa dose di flessibilità da ricavare mediante l'adozione di adeguate misure tecniche e tecnologiche, che comunque non possono oltrepassare il limite del rispetto della riservatezza. Quest'ultimo diritto fondamentale circoscrive il perimetro della capacità adattativa del sistema.

---

[68] Si noti che si è cercato, fino a questo punto, di evitare il più possibile, soprattutto in taluni passaggi chiave, il ricorso al sintagma 'sicurezza informatica' prima di averlo contestualizzato. A tal fine, si è preferito utilizzare le parole della proposta di direttiva: 'sicurezza delle reti e dell'informazioni'.

[69] S. W. BRENNER - L. CLARKE, *Distributed security*, cit., ritengono che la sicurezza informatica sia troppo sfumata ed effimera per permettere una regolamentazione legislativa effettiva. Tuttavia, ricordano che sicurezza inadeguata si traduce in ciò che gli economisti chiamano esternalità negativa, ossia in un costo. Se questa esternalità fosse addossata a carico dei singoli utenti, ad avviso degli Autori, l'utilizzo della Rete diverrebbe molto costoso e sarebbe pertanto destinata a cadere in declino.

[70] "*Art. 67 TFUE.*

1. L'Unione realizza uno spazio di libertà, sicurezza e giustizia nel rispetto dei diritti fondamentali nonchè dei diversi ordinamenti giuridici e delle diverse tradizioni giuridiche degli Stati membri."

[71] Enciclopedia giuridica Treccani, «*sicurezza*» (voce), disponibile al seguente link: http://www.treccani.it/enciclopedia/sicurezza/

[72] Art. 3, n. 2 proposta di direttiva COM (2013) 48 final – 2013/0027 (COD).

[73] Wikipedia, "*resilienza*" (voce), disponibile al seguente link: http://it.wikipedia.org/wiki/Resilienza

La citata definizione fornisce altresì le coordinate interpretative utili per fare chiarezza in merito alle implicazioni penalistiche e di politica criminale circa la qualifica della sicurezza informatica come bene giuridico meritevole di protezione. Secondo la proposta di direttiva, misura della sicurezza informatica è la compromissione della disponibilità, autenticità, integrità e riservatezza dei dati. A ben vedere, la nozione rimanda alle quattro macro-aree di tutela in cui si è soliti distinguere gli attacchi a sistemi informatici e telematici, fin dal primo intervento del legislatore italiano del 1993 e ribadite dalla Convenzione di Budapest[74]: 1) i reati che tutelano la riservatezza dei dati informatici e delle comunicazioni elettroniche (artt. 615-*ter*; art. 615-*quater*; 615-*quinquies*, a tutela del domicilio informatico; art. 617-*quater*; 617-*quinquies*, 617-*sexies* a tutela della interferenza illecita nelle comunicazioni private); 2) i reati che tutelano l'integrità dei dati informatici e delle comunicazioni elettroniche (artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*, sul danneggiamento d'informazioni, dati e programmi); 3) i reati che proteggono la veridicità dei dati informatici (art. 491-*bis* documento informatico e 495-*bis* falsa dichiarazione o attestazione al certificatore di firma digitale sull'identità o qualità personali proprie o di altri); 4) più in generale, i c.d. reati ad alta tecnologia, ossia quei reati che sono commessi mediante l'utilizzo dello strumento informatico o telematico e che sono suscettibili di arrecare grave nocumento e intaccare la fiducia nei sistemi di comunicazione virtuale (ad esempio, la frode informatica, il riciclaggio di capitali, al terrorismo via internet, etc.).

In secondo luogo, emerge l'attualissimo problema del potenziale conflitto tra sicurezza e riservatezza, che investe la scelta delle misure tecniche e tecnologiche[75]. La sicurezza delle reti e delle informazioni è un'esigenza indispensabile per la preservazione dell'ambiente virtuale ove trovano nuovi spazi di affermazione quegli stessi diritti fondamentali, tra i quali la riservatezza, che si pone come suo limite.

Dietro il tema del conflitto di principi si cela quello scontro tra valori che costituisce l'emblema del tempo presente, caratterizzato dal pluralismo etico delle odierne società aperte e multietniche[76].

---

[74] Convenzione del Consiglio d'Europa sulla lotta al *cybercrime,* 23 novembre 2001, Budapest.

[75] Si pensi al caso Snowden, (ex tecnico della CIA) che ha rivelato pubblicamente l'esistenza e i dettagli di diversi programmi di sorveglianza di massa del governo statunitense e britannico, fino ad allora tenuti segreti o al recente scandalo dei *Trojan horses* in grado di intercettare le telefonate effettuate attraverso *Skype*, all'insaputa degli utenti impiegati dalle autorità di polizia tedesche e giustificati per esigenze di sicurezza.

[76] G. ZAGREBELSKY, *Il diritto mite*, Torino, 1992, 13, il quale precisa che "*ciascun principio e ciascun valore, se intesi nella purezza di un loro concetto assoluto, si risolverebbero nell'impossibilità di ammetterne altri*". L. BEDUSCHI, *Rassegna delle pronunce della Corte EDU del triennio 2008 – 2010 in tema di art. da 8 a 11 Cedu*, la quale sottolinea come gli artt. 8 - 11 CEDU presentino clausole derogatorie, che consentono di bilanciare questi diritti ogni qualvolta sia ravvisabile "*uno scopo legittimo*" che lo giustifichi. Su: http://www.europeanrights.eu/public/commenti/Beduschi_-_rassegna_Corte_EDU_art._8_-_11_Cedu_-_dpc.pdf. In giurisprudenza: Corte europea dei diritti dell'uomo, Grande Camera, 4 dicembre 2008, C- 30562/04 e 30566/04, S. e MARPER c. Regno Unito, in *Riv. it. dir. pen. proc.,* Milano, 2009, 346 ss.; Corte europea dei diritti dell'uomo, 17 giugno 2009, C-5335/06, BOUCHACOURT c. Francia, in *Riv. it. dir. pen. proc.*, Milano, 2010, 325 ss.

8. Le molteplici declinazione del diritto fondamentale alla riservatezza: dal consenso al trattamento dei dati, allo *ius excludendi alios*, al diritto all'oblio

La sicurezza informatica comprende in sé: 1) la potenziale compromissione della riservatezza, come esposizione dei dati a rischi di una loro apprensione ad opera di terzi; 2) la semplice perdita di disponibilità dei dati da parte del suo titolare; 3) la compromissione della loro autenticità e integrità.

Della polivalenza contenutistica del diritto fondamentale alla riservatezza si è occupata anche la giurisprudenza sovranazionale, attraverso il riferimento agli artt. 7 (vita personale e familiare) e 8 (protezione dei dati personali) della Carta di Nizza e all'art. 8 (diritto al rispetto della vita privata e familiare) della CEDU.

Tale diritto fondamentale non implica semplicemente il consenso al trattamento dei dati personali richiesto per l'accesso ad un sito o per la creazione di un account. Traslato sulla dimensione digitale, esso è stato declinato, in un primo momento, come 'diritto ad essere lasciati soli', nel senso di preservare l'esistenza di una sfera 'intima' del soggetto dalle intrusioni esterne.

Con la diffusione degli strumenti di monitoraggio dei dati di navigazione che consentono di creare profili piuttosto definiti per ciascun utente, alla riservatezza come *ius excludendi alios* si sovrappone il diritto alla protezione dell'integrità, autenticità e soprattutto disponibilità dei dati personali da parte del titolare. Basti pensare alla frequenza con la quale su Internet sono richiesti, per l'accesso, per compiere determinate attività o operazioni, informazioni e dati personali dei quali l'utente è destinato a perdere il controllo non appena li trasmette: egli, pur avvertito dall'informativa sulla privacy, non è in grado di controllare la sorte effettiva di tali dati presso i terzi. Celebre, a tal proposito, la pronuncia della Corte costituzionale tedesca del 2008, sulla pratica del monitoraggio indiscriminato. In tale sentenza, sono stati evidenziati i legami tra garanzia di integrità dei dati e la c.d. autodeterminazione informativa, intesa come diritto ad essere informati e decidere consapevolmente in merito alla raccolta, alla gestione e all'utilizzo, da parte di terzi, dei propri dati personali[77]. In quell'occasione, la Corte, ancorando la propria valutazione al principio di proporzionalità, ha ritenuto che il monitoraggio indiscriminato dell'attività degli utenti sulla Rete costituisse una misura eccessiva e troppo invasiva della sfera personale perfino rispetto ai fini di contrasto e prevenzione del terrorismo internazionale e del crimine transnazionale.

Ancor più drastica è la situazione nel caso in cui le informazioni sono pubblicate su siti privi di restrizioni all'accesso: l'utente perde la disponibilità del dato, nel senso che esso è potenzialmente suscettibile di apprensione da parte di qualsiasi utente si colleghi alla fonte in cui sono riportati i dati. A tal proposito, la Corte di Giustizia ha di recente incluso nella tutela della riservatezza, il c.d. diritto all'oblio, quale pretesa del cittadino di rimozione dalla Rete delle informazioni ritenute dannose per la sua reputazione o comunque pregiudizievoli, in mancanza di un interesse di natura pubblica all'accesso generalizzato[78]. In sostanza, la deindicizzazione dei link di ricerca sarebbe necessaria

[77] Corte costituzionale tedesca, 27 febbraio 2008, BvR 370/07. Vedi infra il contributo di Flor.

[78] Corte di Giustizia, sentenza 13 maggio 2014, Google Spain SL, Google Inc. contro Agencia Espanola de Proteccion de Datos (AEPD), MARCO COSTEJA GONZALE. Vedi infra il contributo di Flor.

quando i dati relativi alla persona non si presentano più adeguati all'identità virtuale nella propria attualità[79].

Di queste evoluzioni della prassi occorre ormai tenere conto, da quando la giurisprudenza delle Corti sovranazionali è divenuta, nei fatti, vera e propria fonte di diritto: in particolare, la forza propulsiva dei diritti fondamentali nell'interpretazione evolutiva della Corte EDU - cui si ispira anche la Corte di Giustizia - è capace di penetrare nelle trame del tessuto normativo ed innovarne il contenuto prescrittivo.

9. Bilanciamento tra riservatezza e integrità dei dati *versus* sicurezza informatica

La scelta e l'utilizzo di determinate misure tecniche e tecnologiche è questione centrale per definire i rapporti di forza tra sicurezza informatica e il diritto fondamentale alla riservatezza nelle molteplici accezioni elaborate per via giurisprudenziale. Le tecniche di monitoraggio, elevate emblematicamente a strumento di prevenzione e contrasto del terrorismo internazionale dopo i fatti dell'undici settembre, possono rivestire un ruolo ambivalente: come strumento necessario per presidiare la sicurezza delle reti e delle informazioni, o quale mezzo invasivo della sfera personale che lede la riservatezza. Oltre al monitoraggio invasivo praticato dallo Stato e giustificato dalla finalità di prevenzione e repressione dei reati, anche le grandi multinazionali delle telecomunicazioni dispongono di *software* o apparecchiature in grado di produrre risultati simili ad un controllo costante. Esistono, infatti, molti sistemi che consentono di accumulare ogni genere di informazione sugli utenti o sui cittadini, sui loro gusti, sulle loro abitudini, senza alcun garanzia e controllo circa la sorte cui tali dati vengono destinati[80]. Non è un caso che oggi si parli di 'società della sorveglianza' per sottolineare come quelle stesse tecnologie che hanno recato grandi vantaggi e sono divenute indispensabili per l'uomo, celino un elevato rischio di invasione della sfera personale. In tal senso, possono perpetrarsi abusi di vario genere mediante: 1) l'identificazione dei singoli utenti a partire dai loro profili virtuali; 2) la registrazione dei loro comportamenti attraverso la sorveglianza[81].

---

[79] Merita di essere sottolineato come sulla *homepage* delle società sia comparso quasi subito un modulo che consente ai cittadini di richiedere la rimozione dei dati ritenuti non graditi. In Italia, il riconoscimento al diritto all'oblio si deve alla pronuncia della Corte di Cassazione, 5 aprile 2012, n. 5525, in un caso nel quale una personaggio pubblico si era rivolto dapprima al Garante e poi all'autorità giudiziaria per ottenere che un editore (RCS) provvedesse ad aggiornare un vecchio articolo presente nell'archivio *online* relativo al suo arresto, senza che fosse successivamente riportata la notizia del proscioglimento da ogni accusa. La Corte definisce il diritto all'oblio come diritto alla tutela della propria attuale identità personale e morale nella sua proiezione sociale. Inoltre, il diritto all'oblio è tra i dieci principi contenuti nella *Carta dei diritti e doveri di Internet*, elaborata dalla Commissione per i diritti e doveri di Internet e attualmente sottoposta a consultazione pubblica. Testo disponibile sul sito della camera dei deputati: www.camera.it.

[80] Ad esempio, attraverso i *cookies* che sono semplici dati inviati dal sito che si è visitato e vengono registrati, in modo tale che in una seconda navigazione all'interno di questo sito, il nostro terminale sia identificato e riconosciuto. Si pone un problema di conflitto con la riservatezza, perché, pur non essendo *virus* ma dati, i *cookies* permettono al sito che l'ha inviato di unificare tutti gli accessi compiuti con lo stesso computer e ricostruire la storia di tutte le attività compiute con esso, in modo da creare un profilo piuttosto definito dell'utente.

[81] Con il Provvedimento generale del 3 giugno 2014 adottato al termine di una consultazione pubblica, il garante della privacy ha stabilito che l'installazione dei *cookies* per finalità di profilazione e *marketing* da parte dei gestori di siti potrà avvenire solo se l'utente sarà espressamente informato ed avrà prestato il consenso. Sicchè il semplice utilizzo del servizio non potrà più essere considerato come

Il monitoraggio si estrinseca attraverso molteplici modalità esecutive, addirittura legalizzate sotto la veste di un vero e proprio obbligo giuridico[82]. E' questo il caso della *data retention*, ossia della disciplina europea (direttiva 2006/24/CE) che pone a carico dei providers delle comunicazioni l'obbligo di conservare taluni dati del traffico e, su richiesta, di fornirli, alle autorità inquirenti[83]. Si tratta di dati che non attengono al contenuto delle comunicazioni elettroniche, ma concernono le informazioni relative a: mittente e numero chiamato, indirizzi IP, localizzazione del chiamante ed apparecchiature utilizzate. Ad ogni modo, queste informazioni consentono la definizione di profili abbastanza definiti delle persone e delle loro abitudini[84].

La Corte di Giustizia si è posta il problema della giustificazione della deroga sancita dalla direttiva 2006/24/CE sull'obbligo di conservazione di questi dati, alla luce del regime di tutela del diritto al rispetto della vita privata e alla integrità dei dati personali così come articolato dalle direttive n. 1995/46/CE e 2002/58/CE. Ad avviso della Corte, dietro tale previsione si cela un elevato rischio di utilizzazione dei dati, senza che di ciò l'abbonato o l'utente riceva comunicazione o abbia consapevolezza. Tale prescrizione può ingenerare la sensazione che la vita privata sia oggetto di costante sorveglianza[85]. Ad ogni modo, non è ravvisabile alcun pregiudizio al diritto di cui all'art. 7 Carta di Nizza, nel senso di apprensione di informazioni personali relative a fatti della vita dell'utente, dal momento che gli ISP vengono in possesso di informazioni che esulano dal contenuto delle comunicazioni[86]. D'altra parte, non si mette in dubbio che la conservazione dei dati per esigenze connesse all'investigazione e prevenzione dei reati sia un obiettivo di interesse generale (§ 44). Tuttavia, proprio come anni prima aveva statuito la Corte costituzionale tedesca (BverfG, 2008) sopra citata, i giudici di Lussemburgo ritengono che sia stato violato il principio di proporzionalità: l'interferenza nella sfera dei diritti fondamentali del rispetto della vita privata e della protezione dei dati personali non è stata attuata nei limiti dello 'stretto necessario' a garantire la sicurezza collettiva. Il principio di proporzionalità quale canone di ragionevolezza delle scelte operate dal legislatore dell'Unione, è calato dalla Corte nella dimensione operativa-concreta, attraverso la puntuale elencazione dei profili di criticità riscontrabili nella direttiva: la vaghezza dei criteri elaborati per indicare quali crimini giustifichino la conservazione dei dati; la carenza di procedure e di rimedi per scongiurare il rischio che dalla raccolta di tali dati si perpetrino abusi di varia natura, poiché la raccolta non deve essere motivata dalla richiesta dell'autorità giudiziaria; l'assenza di un elenco di casi eccezionali che escludono l'obbligo di conservazione; la

---

accettazione incondizionata di regole che finiscono per espropriare il titolare dal potere di decidere della sorte dei propri dati personali.

[82] N. K. KATYAL, *Digital Architecture as Crime Control*, su: http://architectures.danlockton.co.uk/2007/10/18/review-architecture-as-crime-control-by-neal-katyal/

[83] Corte di Giustizia, Grande Camera, 8 aprile 2014, C- 293/12 e C-594/12. R. FLOR, *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?*, su: www.penalecontemporaneo.it

[84] La Commissione di studio per la redazione di principi e linee guida in tema di garanzie, diritti e doveri per l'uso di internet, ha pubblicato il 25 luglio 2014, un documento che costituisce la base giuridica della carta dei diritti e doveri in internet, dal quale emerge che l'Unione europea, nelle recenti proposte di regolamento COM(2012)11 e proposta di direttiva COM(2012)10, in materia di *privacy* delle persone fisiche prevede, tra le altre cose, il divieto di *profiling*. Su: www.documenti.camera.it/Leg17/Dossier/pdf/GI0250.pdf

[85] Corte di Giustizia, Grande Camera, sentenza 8 aprile 2014, C- 293/12 e C-594/12, § 37.

[86] Corte di Giustizia, Grande Camera, sentenza 8 aprile 2014, C- 293/12 e C-594/12, § 39.

mancata predisposizione di norme che prevedano modalità sicure delle fasi di raccolta, conservazione e distruzione. In sostanza, la disciplina sulla *data retention* è troppo vaga e generica per consentire deroghe ai diritti fondamentali sanciti negli artt. 7 e 8 della Carta di Nizza.

10. Conclusioni

La teoria dei beni comuni condivide la medesima matrice assiologica insita nell'esaltazione dei diritti fondamentali di cui è custode la Corte europea dei diritti dell'uomo e che trovano consacrazione anche nel nuovo Trattato sull'Unione europea (art. 6). La centralità della dimensione valoriale, della categoria dell' 'essere' sull' 'avere' si esprime anche attraverso lo sviluppo di momenti di condivisione: tra questi l'elaborazione di strutture di governo partecipato della Rete, ispirato a principi di democraticità nell'accesso costituisce una meta alla quale tendere per conferire la massima espansione a quegli stessi diritti fondamentali e per l'adempimento di doveri di solidarietà nei confronti della comunità[87].

La creazione di uno spazio virtuale, accessibile a tutti e sicuro, dove la personalità possa manifestarsi liberamente, rappresenta una sfida e al tempo stesso un metro con il quale misurare il sentimento di coesione sociale che attraversa la comunità. Insomma, un programma cui tendere come arricchimento spirituale dell'uomo, nel relativismo e pluralismo dei valori dominanti[88].

E' necessario, tuttavia, rifuggire da un'eccessiva idealizzazione che conduca ad ignorare le recenti acquisizioni sociologiche, secondo le quali la società attuale, figlia del sistema capitalistico e, a dispetto delle occasioni che offre la tecnologia, presenta deboli impulsi alla coesione sociale ed è caratterizzata da una partecipazione passiva sia a livello individuale sia nelle stesse associazioni[89].

Nell'ottica dell'*extrema ratio*, la teoria dei *Commons* può apportare un duplice contributo al sistema penale: in chiave di educazione positiva al rispetto dei beni utili alla comunità e sul versante della ricerca di soluzioni sanzionatorie alternative [90]. Dal primo punto di vista, essa può tradursi, grazie alla sua filosofia propositiva che spinge all'azione e alla condivisione, in un incentivo all'adozione spontanea di modelli comportamentali virtuosi. Sotto l'altro punto di vista, condotte poco rispettose potrebbero generare, da parte della stessa comunità, meccanismi di esclusione o emarginazione o stigmatizzazione che si atteggiano a risposte sanzionatorie 'informali'. Esse saranno tanto più efficaci quanto più inserite in una comunità estesa e coesa

[87] U. MATTEI, *Beni comuni*, cit., 62-63.

[88] Il Comitato dei Ministri del Consiglio d'Europa in occasione della riunione dei Delegati dei Ministri del 16 aprile 2014 ha adottato la Raccomandazione CM/Rec(2014)6 relativa a una "*Guida dei diritti umani per gli utenti di Internet*".

[89] R. SENNET, *Together. The rituals, Pleasure and Politics of Cooperation*, Yale University Press, 2012; trad., A. BOTTINI, *Insieme. Rituali, piaceri, politiche della collaborazione*, Milano, 2012, 149 ss.

[90] G. P. DE MURO, *Ultima ratio: alla ricerca dei limiti all'espansione del diritto*, in *Riv. It. dir. pen. proc.*, 2013, 1654 ss.

attorno ad un nucleo forte di valori (diritti umani, giustizia sociale), in modo tale da rendere effettivamente residuale la necessità dell'intervento del diritto penale[91].

[91] Si pensi alla pubblicazione *online* della *Carta dei diritti e doveri della navigazione in internet*, redatta dalla Commissione per i diritti e doveri di internet già citata (v. nt. 79): essa mira a creare una sorta di coscienza 'civica' condivisa tra gli utenti che dovrebbe costituire la base per la *governance* della Rete, attraverso l'enucleazione di dieci principi radicati nelle norme internazionali sui diritti umani.

LA POLITICA CRIMINALE AL TEMPO DI INTERNET[*]

Mario Caterini

Sommario: 1. La ridondante enfatizzazione mediatica dei rischi e la strumentale creazione elitaria di paure collettive. – 2. La dimostrazione empirica dell'artificiosità della rappresentazione mediatica del rischio criminale. – 3. L'influenza della rappresentazione mediatica sulle scelte di politica criminale. – 4. La 'democrazia liquida' mediante internet: i pericoli per una politica criminale legittima. - 5. Un'auspicabile *Bildung* politico-criminale e il ruolo della cultura giuspenalistica.

1. La ridondante enfatizzazione mediatica dei rischi e la strumentale creazione elitaria di paure collettive

Nella società odierna – è stato affermato autorevolmente – la sicurezza è solo una finzione sociale e, di conseguenza, pure il superamento del rischio è meramente simbolico[1]. In tale direzione, invero, milita in maniera sempre più determinante il ruolo svolto dai mass media, oggi in particolare da internet, che riesce progressivamente ad influenzare la percezione di un certo fenomeno[2]. Tali considerazioni valgono anche per i rischi relativi alle vicende criminali e per le collegate pretese di sicurezza[3]. In quest'ottica il rischio è un derivato socio-culturale, sia nella sua costruzione oggettiva che nella sua percezione soggettiva[4]. In tali casi il rischio criminale spesso appare

[*] Lo scritto propone la relazione svolta, con alcuni adattamenti, l'aggiunta delle note e di talune riflessioni alla luce del dibattito sviluppatosi in occasione del Convegno.

[1] Si veda S. MOCCIA, *L'odierna funzione di 'controllo' e "orientamento" della dottrina*, in *Criminalia*, 2013, 410, secondo cui «la sicurezza, dunque, non è più la conseguenza di un ordine sociale teso alla giustizia, ma è l'esito di scelte politiche, approssimative, orientate nel migliore dei casi alla 'riduzione del danno'; esse, in ogni caso, come l'esperienza di questi anni sta dimostrando, sono condannate al fallimento, anche perché la persona, la sua individualità, più o meno dolorosa, non si lascia facilmente sostituire da insiemi matematici o *clusters* statistici. In questi termini la sicurezza è solo una finzione sociale: dunque il superamento del rischio è destinato ad essere solo simbolico. E la media attuariale delle emozioni private, disinvoltamente scambiata per opinione pubblica, viene sovente assecondata da un legislatore poco attento, poco informato e, forse, in mala fede».

[2] In generale sull'influenza dei mezzi di comunicazione nella percezione sociale della realtà, si veda U. ECO, *Costruire il nemico e altri scritti occasionali*, Milano, 2012; in particolare sul condizionamento ad opera dei *new media* si rinvia a J. MEYROWITZ, *Oltre il senso del luogo. Come i media elettronici influenzano il comportamento sociale*, trad. it. N. Gabi, Bologna, 2002.

[3] Il diritto alla sicurezza è stato oggetto di numerose e autorevoli ricerche nella letteratura penalistica; tra i tanti, in tempi più recenti, si rinvia a D. PULITANÒ, *Sicurezza e diritto penale*, in *Riv. it. dir. proc. pen.*, 2009, 547 ss.; M. DONINI, *Sicurezza e diritto penale*, in *Cass. pen.*, 2008, 3558 ss.; W. HASSEMER, *Sicurezza mediante il diritto penale*, in *Crit. dir.*, 2008, 15 ss.; W. HASSEMER, *Sicurezza mediante il diritto penale*, in *Crit. dir.*, 2008, 15 ss.; A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti*, in *Dem. dir.*, 2000, 19 ss.; da ultimo, A. CAVALIERE, *Può la 'sicurezza' costituire un bene giuridico o una funzione del diritto penale?*, in W. HASSEMER, E. KEMPF, S. MOCCIA (a cura), *In dubio pro libertate. Festschrift für Klaus Volk zum 65. Geburtstag*, München 2009, 111 ss.

[4] Sulla percezione dei rischi si vedano L. SAVADORI, R. RUMINATI, *Nuovi rischi, vecchie paure*, Bologna, 2005, spec. 44 ss.; P. SLOVIC, *The Perception of Risk*, London, 2000, *passim*. Sulla c.d. 'società del rischio' e l'alterazione profonda della struttura del sistema penale in contraddizione con i sui principi fondamentali, si veda F. STELLA, *Giustizia e modernità. La protezione dell'innocente e la tutela delle*

socialmente costruito mediante la creazione di 'nemici' fittizi[5].

La percezione del rischio non avviene secondo un percorso lineare (ossia partendo dai fatti, passando attraverso i mass media, per finire ai consociati), bensì mediante un processo di natura circolare tra fonti che si alimentano reciprocamente[6]. Avvalendosi dell'esperienza collettiva e del senso comune, infatti, i mezzi di comunicazione percepiscono e intercettano i presunti rischi che attraggono i consociati e, mediante l'artificiosità propria della figurazione mediatica, sono capaci di influenzarne ed enfatizzarne una determinata percezione collettiva. Tale percezione, poi, viene ulteriormente rafforzata dagli stessi media che attingono nuovamente a quel senso comune, a questo punto però enfatizzato in precedenza dai media stessi, secondo un meccanismo di crescente amplificazione, equiparabile ad una specie di riproduzione per autopoiesi, ossia una viziata spirale vorticosa non sempre contenibile[7].

Da tale circolo vizioso, inoltre, spesso scaturisce una 'domanda di sicurezza' proveniente dai media e dalla c.d. opinione pubblica condizionata mediaticamente, a cui di frequente fa da *pendant* la c.d. 'risposta pubblica' che, in relazione al fenomeno criminale, o è di carattere politico, con l'emanazione di nuove norme volte [spesso solo simbolicamente] a fronteggiare il rischio percepito; oppure è di matrice giudiziale, con iniziative della magistratura che sempre più frequentemente sfociano nel c.d. 'diritto vivente', ove si assiste a 'forzature' della lettera delle norme per soddisfare supposte richieste di sicurezza provenienti dall'opinione pubblica[8]. Il circolo vizioso può

---

vittime, Milano, 2001, *passim*, spec. 387 ss., 415 ss. Per un'analisi del rischio nella prospettiva penalistica, sia endo che eso-sistemica, più recentemente si rinvia a C. PERINI, *Il concetto di rischio nel diritto penale moderno*, Milano, 2010, *passim*, spec. 4 ss., 168 ss.

[5] Sul fenomeno generale della spettacolarizzazione del crimine, recentemente si vedano E.R. ZAFFARONI, M. BAILONE, *Delito y espectáculo. La criminología de los medios de comunicación*, in E.R. ZAFFARONI, M. CATERINI (a cura), *La sovranità mediatica. Una riflessione tra etica, diritto ed economia*, Padova, 2014, 125 ss. L'argomento dell'enfatizzazione mediatica del pericolo criminale è trattato, tra i tanti, anche da J.L. FUENTES OSORIO, *Los medios de comunicación y el derecho penal*, in *Revista electrónica de ciencia penal y criminología*, 2005, n. 07-16, 16:1 ss.; F. VIANELLO, D. PADOVAN, *Criminalità e paura: la costruzione sociale dell'insicurezza*, in *Dei delitti e delle pene*, 1999, n. 1-2, 247 ss. Sull'influenza dei mezzi di comunicazione nella percezione sociale del 'nemico', si veda A. DINO, *I media e i «nemici» della democrazia*, in *Quest. giust.*, 2006, 824 ss. In genere, sulla costruzione sociale del rischio si rinvia a U. BECK, *La società del rischio. Verso una seconda modernità*, Roma, 2000, 35 ss., spec. 337; G. AMENDOLA, *Qualità della vita, bene comune, rischio accettabile: i topoi retorici e/o le strettoie concettuali della valutazione d'impatto ambientale*, in F. BEATO (a cura di), *La valutazione dell'impatto ambientale. Un approccio integrato*, Milano, 1995, 20 ss.

[6] G. PRIULLA, *Raccontar guai. Che cosa ci minaccia. Che cosa ci preoccupa*, Soveria Mannelli, 2005, 63.

[7] Con particolare riferimento al fenomeno criminale e alla capacità dei media di fornire modelli interpretativi deformanti, si veda R.V. ERICKSON, *Mass Media, Crime, Law, and Justice. An Institutional Approach*, in *The British Journal of Criminology*, vol. 31, 1991, 219 ss., secondo cui i mezzi d'informazione non sono in grado di far nascere dal nulla opinioni o convinzioni, ma sollecitano e sviluppano le attitudini dei cittadini, secondo un modello interrelazionale in cui i media offrono un'interpretazione della realtà che si combina con quella del cittadino.

[8] È molto plausibile, infatti, che il sistema mediatico possa influenzare anche i magistrati nell'assunzione delle decisioni, orientando non solo l'accertamento del fatto, ma anche l'interpretazione delle norme, verso un risultato piuttosto che un altro, in ragione delle aspettative della c.d. opinione pubblica. M. ROMANO, *Legislazione penale e consenso sociale*, in *Jus*, 1985, 413 ss., oltre che di un consenso sociale riferibile alla creazione delle norme, parla anche di un consenso sociale «con riferimento alla struttura dialogico-comunicativa del processo […] il cui esito ultimo – la decisione di condanna o di proscioglimento – condiziona la comprensione sociale dell'attività giudiziaria e ne è verosimilmente a sua volta condizionata».

proseguire con gli effetti socio-politici generati dalla c.d. 'risposta pubblica', effetti che a loro volta attraggono altre reazioni mediatiche, che suscitano a loro volta altra percezione sociale, che a sua volta spesso richiede una nuova 'risposta pubblica'. La percezione del rischio si fonda perciò su un sistema di reciproci impulsi e interferenze, che, in fin dei conti, si sostanzia in uno scontro per imporre una data interpretazione della realtà[9].

In questo [corto]circuito incalzante e interminabile, il compito di selezionare le notizie costituisce la principale forza dei mass media, anche nel *web*[10]. Assodato che deve pur avvenire un vaglio preventivo delle notizie suscettibili di diffusione, la questione si incentra soprattutto sui criteri adottati[11]. I mezzi di comunicazione improntano le loro scelte al discrimine tra ciò che costituisce informazione rispetto a ciò che non è tale, nel senso che non suscita interesse nel pubblico[12]. Nelle economie di mercato, infatti, la logica è quella commerciale, ovvero divulgare solo le notizie più vendibili, più appetibili, che per lo più corrispondono a quei fatti che eccitano le emozioni, come alcune vicende criminali[13]. Questo spesso avviene a detrimento delle informazioni su fenomeni privi di fascino mediatico, che però sarebbero ben più rilevanti, per esempio, in una seria discussione politico-criminale. La selezione 'commerciale' delle notizie suscettibili di divulgazione e, dunque, dei temi del dibattito pubblico, è capace di produrre anche una squilibrata distribuzione delle risorse, in quanto le scelte politiche, legislative e finanziarie, se condizionate da spinte populiste, non saranno tanto sensibili ai rischi più reali e gravi, ma a quelli più apparenti[14].

Più ricerche, soprattutto nei sistemi di *common law*, hanno sottoposto a verifica empirica le influenze dei mass media sul processo decisionale dei giudici professionali e dei giurati, più in particolare con riferimento alla prova del fatto; si vedano E. COSTANTINI, J. KING, *The Partial Juror: Correlates and Causes of Prejudgement*, in *Law & Society Review*, vol. 15, 1981, 36 ss.; C.A. STUDEBAKER, S.D. PENROD, *Pretrial publicity: The media, the law, and common sense*, in *Psychology, Public Policy, and Law*, vol. 3, 1997, 428 ss.; T.R. TYLER, *Viewing CSI and the Threshold of Guilt:Managing Truth and Justice in Reality and Fiction*, in *The Yale Law Journal*, 2006, 1050 ss.; in Italia, per i profili psicologici, si vedano le relazioni all'incontro "Magistrati e Mass Media", organizzato dal CSM, Roma, 2004, in particolare L. ARCURI, *Ruolo dei mezzi di comunicazione di massa nell'organizzazione delle rappresentazioni sociali e del giudizio delle persone (analisi dei processi attraverso cui i prodotti mediatici possono influenzare la decisione)*, e R. RUMIATI, *L'influenza mediatica sulla decisione*.

[9] R. ERICSON, P. BARANEK, J. CHAN, *Negotiating Control. A Study of News Sources*, Toronto, 1989.

[10] In tema si rinvia a R. MARINI, *Mass media e discussione pubblica. Le teorie dell'agenda setting*, Roma - Bari, 2011; si veda anche S. BENTIVEGNA (a cura di), *Mediare la realtà. Mass media, sistema politico e opinione pubblica*, Milano, 2002, in particolare la prima parte con gli scritti di M. MC COMBS, D. SHAW, *La funzione di agenda-setting dei mass media*; di M. BENTON, P.J. FRAZIER, *La funzione di agenda-setting dei mass media ai tre livelli di "complessità" dell'informazione*; e di S. IYENGAR, D. KINDER, *L'effetto di agenda-setting*.

[11] Si è sostenuto che la più forte influenza dei media sulla politica e sugli elettori non avviene attraverso una sorta di imposizione di contenuti ideologici, ma proprio in ragione dei processi selettivi delle informazioni ispirati a logiche interne al sistema mediatico; cfr. E. CANIGLIA, *Berlusconi, Perot e Collor come political outsider. Media, marketing e sondaggi nella costruzione del consenso politico*, Soveria Mannelli, 2000, 180.

[12] Mentre il diritto si conforma al discrimine lecito/illecito, i mezzi di comunicazione al diverso codice: informazione/non informazione; cfr. N. LUHMANN, *La differenziazione del diritto. Contributi alla sociologia e alla teoria del diritto*, trad. it. di R. De Giorgi, M. Silbernagl, Bologna, 1990, 62; ID., *Die Realität der Massenmedien*, Opladen, 1995, 17.

[13] D. GARLAND, *La cultura del controllo. Crimine e ordine sociale nel mondo contemporaneo*, Milano, 2004, 174.

[14] G. PRIULLA, *Raccontar guai*, cit., 67 ss. Per il dibattito sul c.d. populismo penale, recentemente si

La ridondante enfatizzazione mediatica dei rischi più 'commercializzabili' può indurre verso istintivi allarmi sociali, una sorta di ansia collettiva che spesso non ha vera giustificazione: si tratta del c.d. paradosso della paura, in cui l'emozione esaspera la realtà[15]. La teorizzazione della paura come strumento di controllo sociale ha origini remote e molto autorevoli[16]. Oggi, tuttavia, i mass media e segnatamente internet, in cui l'emotività assurge a parametro delle scelte, possono offrire formidabili strumenti di persuasione attraverso la paura, sempre più al centro della scena politica, al punto che i fenomeni generanti timore sociale, mediaticamente enfatizzati, frequentemente condizionano iniziative legislative di contrasto [simbolico], volte ad attrarre il favore degli elettori[17]. A questo punto è chiaro che la paura può essere catalizzata, manipolata, strumentalizzata, fino ad essere del tutto creata e, quando ciò si verifica, i fautori ne sono le *élites* politiche, economiche e mediatiche[18]. Il ruolo della comunicazione di massa – nella quale internet sta assumendo un peso sempre più determinante – diviene così indispensabile per generare sentimenti diffusi di paura attraverso la percezione collettiva dei rischi[19].

---

vedano G. FIANDACA, *Populismo politico e populismo giudiziario*, in *Criminalia*, 2013, 95 ss.; D. PULITANÒ, *Populismi e penale. Sulla attuale situazione spirituale della giustizia penale*, *ivi*, 123 ss.

[15] La letteratura in tema di paura della criminalità è molto vasta; tra i tanti si rinvia a J. SIMON, *Il governo della paura. Guerra alla criminalità e democrazia in America*, Milano, 2008, *passim*; R. CORNELLI, *Paura e ordine nella modernità*, Milano, 2008, *passim*; I. MERZAGORA BETSOS, G.V. TRAVAINI, *Criminalità e paura: una relazione complessa*, in *Difesa sociale*, 2003, 51 ss.; G.V. TRAVAINI, *Paura e criminalità. Dalla conoscenza all'intervento*, Milano, 2002, *passim*, spec. 19 ss.; per un recente tentativo di superamento della paura attraverso politiche di sicurezza orientate in senso democratico, si vedano A. CERETTI, R. CORNELLI, *Oltre la paura. Cinque riflessioni su criminalità, società e politica*, Milano, 2013.

[16] Per l'uso politico della paura nel pensiero di Hobbes, Montesquieu e Tocqueville, si rinvia a C. ROBIN, *Paura. La politica del dominio*, Milano, 2005, 41 ss., 81 ss., 91 ss.

[17] In tal senso risultano particolarmente significative le incisive parole di E.R. ZAFFARONI, *En busca de las penas perdidas. Delegitimacion y dogmatica juridico-penal*, Bueons Aires, 1989, trad. it. di G. Seminara, revisione a cura di A. Cavaliere, *Alla ricerca delle pene perdute. Delegittimazione e dommatica giuridico-penale*, Napoli, 1994, 139 ss., secondo cui «i *mass-media* – e specialmente la televisione – sono oggi elementi indispensabili per l'esercizio di potere di tutto il sistema penale. Se non esistessero […] non si potrebbero indurre sentimenti di paura nella direzione voluta […] i mezzi di comunicazione di massa sono i grandi artefici dell'illusione relativa ai sistemi penali […] si occupano della precoce introiezione del modello penale quale preteso modello di soluzione dei conflitti […] sono incaricati di generare l'illusione dell'efficienza del sistema».

[18] N. CHOMSKY, E. S. HERMAN, *La fabbrica del consenso. La politica e i mass media* (1998), trad. it. S. Rini, Milano, 2014, *passim*, spec. 363, hanno dimostrato il meccanismo elitario attraverso cui il mondo dell'informazione mobilita l'opinione pubblica per sostenere e difendere gli interessi particolari dominanti nella società: «la finalità sociale dei media è piuttosto di inculcare e difendere i progetti economici, sociali e politici dei gruppi privilegiati che dominano la società e lo stato. I media servono al conseguimento di questo scopo in molti modi: selezionando i temi, distribuendoli secondo una scala di priorità e di importanza, inquadrando le questioni, filtrando le informazioni, scegliendo enfasi e toni, e mantenendo il dibattito entro i confini di premesse accettabili». C. ROBIN, *Paura*, cit., 199, ha affermato che «le élites […] in quanto protettori ufficiali della sicurezza della comunità, decidono quali minacce siano più rilevanti […], definiscono la natura della minaccia, da dove proviene e come deve essere combattuta, mobilitando la popolazione contro di essa». Nella prospettiva politico-criminale si parla delle campagne di *law & order* per recuperare o rafforzare il consenso; cfr. C.A. PALIERO, *La maschera e il volto. Percezione sociale del crimine ed 'effetti penali' dei media*, in *Riv. it. dir. proc. pen.*, 2006, 523 ss.; più in generale sul ruolo del consenso nel diritto penale, ID., *Consenso sociale e diritto penale*, in *Riv. it. dir. proc. pen.*, 1992, 849 ss.

[19] Se poi il potere politico riesce a controllare i mass media – attraverso imposizioni o concentrazioni di proprietà –, l'alterazione del sistema democratico è ulteriore in quanto le forze politiche potrebbero riuscire a farsi sollecitare dall'opinione pubblica le riforme che esse stesse desiderano; in tema F. PALAZZO, *Mezzi di*

2. La dimostrazione empirica dell'artificiosità della rappresentazione mediatica del rischio criminale

Al fine di convalidare quanto si è sostenuto sinora, con particolare riferimento ai rischi e agli allarmi collegati alle vicende delittuose, è utile attingere alla ricerca empirico-criminologica per capire quali fatti suscettibili di rilevanza penale vengono divulgati mediaticamente, e in che modo[20]. L'inclinazione è ad esaltare il rischio percepito dalla collettività in quanto gli episodi criminali, soprattutto alcune tipologie delittuose, vengono rappresentati dai mass media come fenomeno molto più diffuso di quello che è in realtà, dilatandone la consistenza rispetto a quella riscontrabile ufficialmente nei dati statistici validati[21].

Buona parte delle notizie relative ai fatti criminosi viene scartata a favore di un novero ristretto di episodi presentati con una forte carica di disvalore. L'*agenda setting* relativa alle tipologie criminose è ferrea e restrittiva, approdando al grande pubblico quasi esclusivamente le notizie relative ad alcuni tradizionali delitti violenti (ad es. omicidio, terrorismo, ecc.), mentre altri episodi non captano alcuna attenzione mediatica o questa è molto limitata, ad eccezione di alcune categorie di avvenimenti (ad es. crimini sessuali o contro l'infanzia) che, sebbene solitamente trascurati nella loro portata generale, arrivano alla ribalta della cronaca spesso in riferimento a specifici episodi enfatizzati sul piano della gravità. Avviene inoltre che i reati statisticamente più frequenti, come quelli contro il patrimonio, se in alcuni casi per numero di notizie (soprattutto sui giornali) hanno una buona frequenza, ricevono però una scarsa divulgazione mediatica complessiva, sia per gli spazi che per i tempi dedicati[22]. I mezzi

---

comunicazione e giustizia penale, in *Pol. dir.*, 2009, 202-203; G. GIOSTRA, *Processo penale e mass media*, in *Criminalia*, 2007, 66

[20] In via generale si rinvia a G. FORTI, M. BERTOLINO (a cura di), *La televisione del crimine*, Milano, 2005, *passim*; più recentemente si veda pure R. BIANCHETTI, *Mass media, insicurezza sociale e recenti orientamenti di politica penale*, Milano, 2012, *passim*, spec. 154 ss.; meno recentemente R. GRANDI, M. PAVARINI, M. SIMONDI (a cura di), *I segni di Caino. L'immagine della devianza nella comunicazione di massa*, Napoli, 1985, *passim*.

[21] G. FORTI, R. REDAELLI, *La rappresentazione televisiva del crimine: la ricerca criminologica*, in G. FORTI, M. BERTOLINO (a cura di), *La televisione del crimine*, cit., *passim*, spec. 12 ss., 18 ss., 179; R.J. GEBOTYS, J.V. ROBERTS, B. DASGUPTA, *News Media Use and Public Perceptions of Crime Seriousness*, in *Canadian Journal of Criminology and Criminal Justice*, 30, 1988, 3 ss. Per altre discrasie numeriche e sovra-rappresentazioni sostanziali (per omissione), in particolare tra cronaca criminale riguardante cittadini italiani e stranieri, si veda E. CALVANESE, *Media e immigrazione tra stereotipi e pregiudizi. La rappresentazione dello straniero nel racconto giornalistico*, Milano, 2011, 115 ss. Il tema è trattato anche da C.A. PALIERO, *La maschera e il volto*, cit., 493 ss. Per l'analisi della notevole crescita delle notizie criminali nella stampa inglese, si vedano R. ROBERT, S. LIVINGSTONE, J. ALLEN, *Casino culture: media and crime in a winner-loser society*, in K. STENSON, R. SULLIVAN (a cura di), *Crime, risk and justice. The politics of crime control in liberal democracies*, Cullompton, 2001, 174 ss. Per alcune sintetiche osservazioni problematiche sulla differenza tra la criminalità 'effettiva' e quella 'percepita', si veda T. PADOVANI, *Informazione e giustizia penale: dolenti note*, in *Dir. pen. proc.*, 2008, 690, il quale evidenzia che la presunta disinformazione operata dai media, andrebbe confrontata, per saggiarne l'effettiva consistenza, con la possibile ignoranza statistica dei fenomeni criminali, con eventuali diverse dislocazioni territoriali e gravità dei fatti criminali, e con la 'cifra oscura' dei reati non denunciati.

[22] G. FORTI, R. REDAELLI, *La rappresentazione*, cit., 92 ss. Sulla selezione distorsiva delle notizie in tema di criminalità, si veda pure R. SURETTE, *Media, Crime, and Criminal Justice. Images, Realities, and Policies*, Belmont, 2007, *passim*. La tendenza trova riscontri anche in altre esperienze, per esempio quella irlandese, per la quale si rinvia a M. O'CONNELL, *Is Irish Public Opinion towards Crime Distorted by Media Bias?*, in *European Journal of Communication*, 1999, vol. 14, 191 ss., che ha analizzato oltre 2000

di informazione, inoltre, tendono a sopravvalutare la gravità di alcuni reati rispetto al disvalore 'ufficiale' assegnato dall'ordinamento attraverso la 'comminatoria edittale'[23].

Emerge così che la comunicazione di massa tende a divulgare maggiormente gli episodi criminali più rari, ma considerati gravi ed emotivamente eccitanti, e indiscutibilmente meno i crimini molto più diffusi, ma reputati in sé poco rilevanti perché non suscitanti l'interesse del pubblico. La comunicazione di massa, perciò, è incline a invertire l'ordine delle statistiche reali, trascurando il crimine come fenomeno sociale di larga scala e concentrando l'attenzione su singoli fatti in grado di attrarre *audience* e profitto[24].

I dati empirici che emergono dalla ricerca criminologica consentono di validare l'artificiosità della percezione del rischio criminale così come figurato dal sistema mediatico, e permettono anche di spiegare – secondo i meccanismi che meglio si descriveranno di seguito – molte scelte politico-criminali populiste e 'onnivore', che negli ultimi decenni hanno concorso alla formazione della c.d. legislazione penale dell'emergenza[25]. Infatti, se si formano mediaticamente irrazionali istanze sociali di repressione penale, la politica tende ad apprestare risposte penali solitamente simboliche, destinate alla rassicurazione sociale e ad attrarre consenso, ma ineffettive o inutili, inidonee ad orientare i consociati[26].

---

articoli e le distorsioni operate dai media ricondotte, tra l'altro, alla propensione a divulgare notizie di crimini gravi anche se infrequenti. Per l'esperienza scozzese si vedano J. DITTON, J. DUFFY, *Bias in the Newspaper Reporting of Crime News*, in *The British Journal of Criminology*, vol. 23, 1983, 159 ss. Per quella austrica, J. GUNZ, *Kriminalberichterstattung in unseren Tageszeitungen Vergeltung oder Vorbeugung? Eine inhaltsanalytische Dokumentation*, Linz, 1980, 3 ss.; per quella tedesca, H. KURY, *Mass media e criminalità: l'esperienza tedesca*, in G. FORTI, M. BERTOLINO (a cura di), *La televisione del crimine*, cit., 319 ss.

[23] Cfr. G. FORTI, R. REDAELLI, *La rappresentazione*, cit., 140 ss., 158 ss.

[24] Sull'inversione dell'ordine delle statistiche reali, si vedano sempre G. FORTI, R. REDAELLI, *La rappresentazione*, cit., 140 ss., 182, i quali, nell'operare il raffronto tra i dati di presenza mediatica delle tipologie di reati con le cifre esposte nelle statistiche giudiziarie penali, hanno tenuto in considerazione i dati Istat relativi all'anno 2000. Si veda, inoltre, C.E. PALIERO, *La maschera e il volto*, cit., 494. Ancora, R. SURETTE, *Media, Crime*, cit., 63; H.J. SCHNEIDER, *La criminalité et sa représentation par les mass media*, in *Revue internationale de criminologie et de police technique*, 48, 1995, 148 ss.

[25] In generale, sulle problematiche connesse alla legislazione dell'emergenza, si veda il fondamentale e ormai classico lavoro di S. MOCCIA, *La perenne emergenza. Tendenze autoritarie nel sistema penale*, Napoli, 1997, *passim*. Più recentemente, sempre S. MOCCIA, *L'odierna funzione di 'controllo' e "orientamento" della dottrina*, cit., 414, ha parlato di un «globalizzante, 'onnivoro' diritto penale» che manifesta la crisi in cui versa attualmente la legalità penale, formale e dei contenuti. «Le leggi penali sono ormai, troppo spesso, divenute semplicemente delle 'regole scritte', dal contenuto casuale: esse sono, però, collegate, o comunque è possibile che lo siano, anche ad una severa punizione, senza che, tuttavia, dal contenuto del divieto emerga una legittimazione del trattamento sanzionatorio». Secondo M. DONINI, *Il volto attuale dell'illecito penale*, Milano, 2004, 55, negli ultimi decenni, in Italia, il 'diritto penale del nemico' è stato chiamato 'diritto penale dell'emergenza'.

[26] In tema si veda pure M. DONINI, *Il diritto penale di fronte al "nemico"*, in *Cass. pen.*, 2006, 735 ss., che a proposito dell'impossibilità di controllo sull'uso distorto dei mass media, parla di una costruzione giornalistica e/o politica di "mostri", come strumentalizzazione della persona che dà vita a quello che definisce il secondo significato del diritto penale del 'nemico', ossia l'uso strumentale del diritto penale del fatto in funzione simbolico-espressiva e di "lotta" contro il "male" commesso da un tipo normale d'autore. Più recentemente si veda F. SCHIAFFO, *La creazione della insicurezza in Italia e negli USA: gli esiti istituzionali tra effetti simbolici e disastri reali*, in *Critica dir.*, 2012, 52 ss., in particolare a proposito del "disastro annunciato" della privatizzazione nella gestione della sicurezza pubblica nella legislazione italiana negli anni del boom mediatico della criminalità.

3. L'influenza della rappresentazione mediatica sulle scelte di politica criminale

L'artificiosità della rappresentazione mediatica del rischio criminale, così come empiricamente dimostrata dalle indagini criminologiche, è utile per vagliare anche come questa può incidere sulle scelte legislative, sempre più condizionate dagli attuali metodi di fare politica, soprattutto in seguito al declino dei più netti conflitti ideologici di un tempo[27]. Infatti, essendosi di molto affievolito il c.d. 'voto di appartenenza', le forze politiche hanno la necessità di distinguersi dalle altre e così attrarre un consenso non puramente ideologico. Perciò, i sistemi volti ad attrarre il favore degli elettori – sul modello del c.d. 'partito pigliatutto' – si basano molto sulle analisi del 'mercato' elettorale, orientandosi sempre più verso tecniche paragonabili al *marketing*[28]. L'archetipo è mutuato da una razionalità tipicamente commerciale, nel senso che le organizzazioni politiche vengono equiparate alle imprese: come queste ultime raggiungono meglio i loro obiettivi ponendo i bisogni dei consumatori all'inizio e non alla conclusione del processo produttivo, così i partiti politici, per attrarre consensi, devono porre i bisogni degli elettori come punto di partenza della formazione dei loro programmi. Il progetto politico di un partito, secondo tale modello, non dovrebbe essere un prodotto ideologicamente preconfezionato, ma un frutto maturato alla luce di indagini sul 'mercato' elettorale.

Il *marketing* politico sembrerebbe ispirarsi ad un più alto senso di democrazia, perché il legislatore non potrebbe imporre pedagogicamente una sua ideologia, bensì dovrebbe limitarsi a raccogliere le preferenze dei cittadini[29]. La validità di tale conclusione è però subordinata alla correttezza, trasparenza e democraticità dei processi che fanno nascere e sviluppare le idee, le aspettative e le ansie dei cittadini. Si può allora affermare che la democraticità di un tale modello è in buona parte legata inscindibilmente all'obiettività e alla democraticità della comunicazione massiva[30].

Ed invero, posto che il sistema mediatico riesce ad influenzare l'agenda politica, ciò implica che le stesse opzioni politiche saranno assoggettate alla filosofia sottesa al funzionamento della comunicazione di massa[31]. Se tali logiche sono guidate prevalentemente dagli interessi economici, dal profitto, anche i modelli e le idee trasfuse nei programmi politici e nella legislazione penale, saranno improntate indirettamente a ragioni meno democratiche e più economiche[32].

---

[27] In merito all'influenza dei mezzi di comunicazione sull'agenda politica e, in particolare, in riferimento all'indicazione mediatica del fenomeno criminale quale questione permanente della stessa agenda, si veda J.L. FUENTES OSORIO, *Los medios de comunicación y el derecho penal*, cit., 16:23 ss.

[28] La teoria dei partiti 'pigliatutto' risale a O. KIRCHHEIMER, *The Transformation of the Western European Party System*, in J. LA PALOMBARA, M. WEINER (a cura di), *Political Parties and Political Development*, Princeton, 1966, 177 ss., ora in G. SIVINI (a cura di), *Sociologia dei partiti politici*, Bologna, 1971, 177 ss., in particolare 192.

[29] M. HARROP, *Political marketing*, in *Parliamentary Affairs*, 1990, 277 ss.; M. SCAMMELL, *Designer Politics. How Elections are Won*, Londra, 1995, 298; A. CATTANEO, P. ZANETTO, *(E)lezioni di successo*, Milano, 2001, 13.

[30] Per alcune critiche al *marketing* politico ispirate a modelli democratici, si vedano B. FRANKLIN, *Packaging Politics. Political Communications in Britain's Media Democracy*, Londra, 2004; K.H. JAMIESON, *Dirty politics. Deception, distraction, and democracy*, New York - Oxford, 1992.

[31] Secondo T.H. QUALTER, *Opinion Control in the Democracies*, Londra, 1985, 138, il *marketing* riduce la politica a immagini commercializzabili.

[32] Nella letteratura italiana, per il rapporto tra democrazia e *marketing* politico, si veda L. MORI, *Il marketing politico e il consenso in democrazia*, in *Iride*, 2011, 563 ss.; ID., *Procedure democratiche*,

La metodologia del *marketing*, per conformarsi alla comunicazione massmediatica, si fonda inoltre su una semplificazione massima dei temi e dei dibattiti. La complessità delle questioni e delle relative argomentazioni viene rimossa per lasciare il posto a *slogan*, ad asserzioni brevi e facilmente comprensibili, in grado di procurare il favore degli elettori[33]. Anche in questo caso potrebbe apparire che le strategie del *marketing* politico siano più democratiche perché – seguendo una filosofia inclusiva – segnano una comunicazione politica adatta al linguaggio comune dei cittadini[34]. Pure in questo caso, però, il valore di tale conclusione è da verificare alla luce dei rischi connessi ad un semplicismo deleterio, inadeguato a trattare questioni complesse come la politica criminale, destinata a pesare gravemente sulle libertà fondamentali dell'uomo. In quest'ottica, dunque, il *marketing* politico non sembra di per sé una strategia più democratica, perché – quasi come se la problematicità fosse incompatibile con la democraticità – spinge verso una banalizzazione delle questioni, verso temi di respiro asfittico, sol perché popolari, agevolmente comprensibili e oggetto delle ansie degli elettori mediaticamente condizionate[35]. Un modello maturo di democrazia, invece, non può tollerare l'oscuramento mediatico e l'oblio politico di questioni e argomentazioni di maggiore complessità e serietà[36].

La simbolicità che ha caratterizzato la politica criminale degli ultimi decenni, allora, sembra essere uno dei riflessi del più generale concetto di 'governo simbolico', ove lo scopo del potere è divenuto l'esercizio del potere stesso[37], effetto altresì della difficoltà di circolazione massiva delle più autorevoli e serie idee ispirate ai fondamentali valori di uno Stato sociale di diritto.

Per riepilogare, se, da un lato, la maggiore democraticità del sistema non è di per sé assicurata dal *marketing* politico, dall'altro, lo stesso *marketing* sta comunque orientando la c.d. 'risposta pubblica' – pure la legislazione penale – sempre più verso le tendenze 'commerciali' e semplicistiche emergenti dal sistema mediatico[38]. I timori che

---

legittimazione e consenso nell'età del marketing politico: considerazioni filosofico-politiche, in *Dir. e quest. pubbl.*, 2012, 711 ss. F. PALAZZO, *Mezzi di comunicazione*, cit., 203, a proposito delle leggi del mercato che regolano ferreamente la rappresentazione del fenomeno criminale, parla di «una deriva *metodologicamente* antidemocratica».

[33] Si tratta di scorciatoie informative «che fungono da sostituti di "seconda scelta" di altri tipi di dati, più inaccessibili» cfr. S. POPKIN, M. DIMOCK, *La conoscenza dei cittadini, le scorciatoie informative ed il ragionamento politico*, in S. BENTIVEGNA (a cura di), *Comunicare politica nel sistema dei media*, Genova, 1996, 182.

[34] M. HARROP, *Political marketing*, cit.; M. SCAMMELL, *Designer Politics*, cit.

[35] Sulle forti perplessità relative all'eccessiva semplificazione del linguaggio politico e dell'informazione, con ovvie ricadute sulla correttezza delle scelte elettorali, si veda E. CANIGLIA, *Berlusoni*, cit., 191 ss.

[36] G. SMITH, J. SAUNDERS, *The application of marketing to British politics*, in *Journal of Marketing Management*, 1990, V, 295 ss.

[37] Cfr. N. O'SHAUGHNESSY, *Il marketing del marketing politico: un ossimoro?*, in A. MELLONE, B.I. NEWMAN (a cura di), *L'apparenza e l'appartenenza. Teorie del marketing politico*, Soveria Mannelli, 2004, 232.

[38] Se la scienza sociale non è concorde sulla natura e l'ampiezza del potere dei mass media, non essendo facile distinguere la loro influenza da quella dell'educazione, della religione, ecc., tutti però concordano sull'influenza che i mass media hanno sull'agenda politica; cfr. P. BUTLER, N. COLLINS, *Il marketing politico tra prodotto e processo*, in A. MELLONE, B.I. NEWMAN (a cura di), *L'apparenza*, cit., 98 ss. Per le intime implicazioni tra *marketing* politico e mass media, distinti in *free* e *paid media*, si rinvia a M. SCAMMEL, *Cosa insegna il marketing alla scienza politica*, ivi, 39; D. WRING, *Le teorie del marketing politico*, ivi, 121 ss.; N. O'SHAUGHNESSY, *Il marketing del marketing politico: un ossimoro?*, ivi, 228 ss.

derivano in generale dall'incidenza del *marketing* sulla politica [39], ossia della mercificazione e banalizzazione delle idee, sono ancor più gravi con specifico riferimento alla politica criminale, che incide sui beni fondamentali dell'individuo, come la sua libertà e dignità [40]. 'Marketizzare' le idee di politica criminale, in conclusione, può equivalere a strumentalizzare, semplicizzare, mercificare, 'vendere' i tratti più intimi dell'uomo[41].

4. La 'democrazia liquida' mediante internet: i pericoli per una politica criminale legittima

La comunicazione basata sulle nuove tecnologie sta favorendo le speranze di superamento della c.d. democrazia rappresentativa a favore di quella diretta[42]. Si parla di "democrazia liquida" per significare un sistema in cui, mediante *software* liberi, ogni cittadino ha il potere di scegliere se esercitare i propri diritti politici consistenti nel formulare proposte e nel votarle, oppure se delegarli, anche se in maniera sempre revocabile, così da rendere inutile un meccanismo unitario e periodico di elezione di rappresentanti[43].

I *new media* stanno perciò incoraggiando la convinzione che il miglior governante sarebbe da individuare nell'opinione pubblica. Attraverso la sua struttura dialogica, internet consentirebbe una controrivoluzione in grado di cambiare i meccanismi democratici, permettendo il superamento della crisi di rappresentatività della politica mediante il potere conferito ad ogni cittadino di manifestare frequentemente le proprie preferenze grazie a una sorta di metodo referendario permanente [44]. Il tema è di particolare attualità soprattutto in seguito alle affermazioni, e anche alle iniziative politico-criminali, di organizzazioni che hanno fondato su internet la propria filosofia volta ad una partecipazione diretta degli elettori alle decisioni, eliminando la mediazione degli eletti[45].

---

[39] Restringimento dell'agenda pubblica, impegno di messaggi mediatici anziché di argomentazioni, esaurimento del 'coraggio' politico, ecc. Cfr. M. SCAMMEL, *Cosa insegna*, cit., 57; P. BUTLER, N. COLLINS, *Il marketing politico*, cit., 85 ss.

[40] Per alcune considerazioni sull'alterazione del circuito democratico derivante dalle rappresentazioni mediatiche distorte, in particolare delle vicende processuali, si veda G. GIOSTRA, *Processo penale*, cit., 66. Sulla spettacolarizzazione del processo si veda R. CANESTRARI, *Reazioni psicologiche differenziali e spettacolarizzazione del processo*, in F. GALGANO (a cura), *Quaderni dell'avvocatura*, Padova, 1995, 52 ss.

[41] Si veda a S. MOCCIA, *L'odierna funzione di 'controllo' e "orientamento" della dottrina*, cit., 411, secondo il quale «l'orientamento attuale ai flussi emotivi dei consociati o di *lobbies*, anche per demagogiche finalità elettorali, spinge il legislatore – o chi per esso – ad esaudire i desideri di criminalizzazione, al di là di parametri di effettiva meritevolezza di pena di talune condotte».

[42] Sul tema recentemente si vedano R. DE ROSA, *Cittadini digitali. L'agire politico al tempo dei social media*, Santarcangelo di Romagna, 2014, *passim*; A. PUTINI, *Al di là di Internet: fra recupero e dissoluzione della democrazia*, in *Sociologia*, 2013, 42 ss.

[43] Per una più esaustiva definizione di 'democrazia liquida' si rinvia a M. BERNABÈ, S. MARCOLINI, A. ROSTELLO, *Democrazia nunciativa. Un sistema solido per società liquide*, Roma, 2013, 13 ss. Gli Autori, in relazione ai programmi informatici liberi che potrebbero consentire l'esercizio del voto delegato, fanno l'esempio di quello attualmente più conosciuto: "LiquidFeedback", piattaforma utilizzata dal c.d. Partito pirata. Sulla "democrazia liquida" e il Partito pirata, si rinvia pure a R. DE ROSA, *Cittadini digitali*, cit., 105 ss.

[44] A.L. SHAPIRO, *The Control Revolution. How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York, 1999, *passim*.

[45] Il riferimento è in primo luogo all'affermazione elettorale che in Italia ha avuto il Movimento 5 Stelle. In

L'idea è quella antica dell'agorà, che oggi, però, sarebbe realizzabile virtualmente mediante le tecnologie interattive, in grado di rendere i cittadini sempre ben informati e capaci di orientare le scelte pubbliche senza la mediazione di politici di professione. A differenza dei media tradizionali, la dialogicità di internet – ossia la sua natura bidirezionale che consente lo scambio di informazioni – è considerata il principale presupposto della sua vocazione spiccatamente democratica. Tale caratteristica tecnologica, in effetti, costituisce una grande novità rispetto alla stampa, alla radio o alla televisione, che non consentono agli utenti di 'dialogare' direttamente. Questa pur fondamentale qualità di internet, d'altronde, di per sé non sembra sufficiente ad assicurare la democraticità di un sistema politico, e una conclusione opposta verosimilmente si rivela un mito. Infatti, le nuove tecnologie, da un lato, possono anche prestarsi ad un uso distorto come, a titolo esemplificativo, quello di legittimare volontà autoritarie mediante la ratifica di decisioni dispotiche; dall'altro, internet non può da solo sostituire del tutto i tradizionali processi democratici tipici del conflitto socio-politico, ma semmai può arricchirli, costituendo, con le dovute garanzie, un valido ausilio in grado di migliorare il grado di democraticità di un sistema[46].

I problemi che pongono i *new media*, per un verso, sono analoghi a quelli della comunicazione massiva tradizionale, collegati alla logica del tornaconto economico e alle vecchie o nuove *lobbies* che ne condizionano le strategie[47]. Per un altro verso i nuovi mezzi di comunicazione massiva presentano problematiche ulteriori, derivanti dall'enormità e dalla frequente scarsa qualità delle informazioni pubblicate nel *web*. Anche e proprio a causa di tale mole esorbitante e del caos divulgativo che ne deriva, i *new media* difficilmente riescono ad infondere nei cittadini una migliore conoscenza delle

---

tema, recentemente, si veda A. FLORIDIA, R. VIGNATI, *Deliberativa, diretta o partecipativa: quale democrazia per il Movimento 5 stelle?*, relazione presentata al Convegno annuale della Società italiana di scienza politica, tenutosi a Firenze dal 12 al 14 settembre 2013. Secondo gli Autori, nelle idee del Movimento si mescolano, generando più di una contraddizione, tre diverse sfide alla democrazia rappresentativa: una riformatrice (attraverso strumenti di democrazia diretta, come referendum e petizioni, in un quadro che conserva la centralità del Parlamento); una utopica (superamento della democrazia rappresentativa a mezzo degli strumenti informatici); e una sfida plebiscitaria (uso del web e delle piazze). In senso critico pure M. BERNABÈ, S. MARCOLINI, A. ROSTELLO, *Democrazia nunciativa*, cit., 17 ss., secondo cui il «"Movimento 5 Stelle" è la prosecuzione del vecchio con nuove forme». In argomento si veda ancora F. FORNARO, *Un non-partito: il Movimento 5 stelle*, in *il Mulino*, 2012, 253 ss. I parlamentari del M5S hanno presentato numerosi disegni di legge di politica-ciminale: in tema di scambio elettorale politico-mafioso, di prevenzione e contrasto della corruzione, di riciclaggio, auto-riciclaggio e detenzione di attività finanziarie all'estero, di reati societari, tributari e fallimentari, di divieto dello svolgimento di propaganda elettorale a carico delle persone appartenenti ad associazioni mafiose e sottoposte alla misura di prevenzione della sorveglianza speciale di pubblica sicurezza. La c.d. 'emergenza democratica', del resto, e la montante protesta che reclama nuove forme di democrazia diretta, riguardano anche il resto dell'Europa e dell'Occidente, come dimostra il successo, almeno comunicativo, di movimenti come quelli degli *Indignados*, di *Occupy* e del c.d. Partito pirata.

[46] Il tema dei rapporti tra democrazia e nuove tecnologie comunicative è oggetto di vasta letteratura. In questa sede si limita il rinvio ad alcuni lavori principali: S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997; P. LÉVY, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it. di D. Feroldi, M. Colò, Milnao, 2002; ID., *Cyberdemocrazia. Saggio di filosofia politica*, a cura di G. BIANCO, Milano, 2008; D. DE KERCKHOVE, A. TURSI (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti*, Milano, 2006; D. PITTÈRI, *Democrazia elettronica*, Roma, 2007. Più recentemente L. CORCHIA, *La democrazia nell'era di internet. Per una politica dell'intelligenza collettiva*, Firenze, 2011.

[47] S. LOMBARDINI, *Accelerare non è fare*, in J. ACOBELLI (a cura di), *Politica e internet*, Soveria Mannell, 2001, 62; G.O. LONGO, *Un rapporto problematico*, ivi, 70, che parla di una rete fortemente identificata col mercato, di cui esalta la dimensione antidemocratica del denaro.

questioni socio-politiche[48].

La rivoluzione annunciata della 'democrazia liquida' interattiva, ancora una volta, sembra prevalentemente simbolica. Almeno al momento, infatti, non può condividersi l'opinione, a mo' di *slogan*, secondo cui i problemi della democrazia potrebbero essere risolti *d'emblée* con l'uso di internet. Ciò per varie ragioni: in primo luogo, ancora non tutti accedono alle nuove tecnologie e anche chi vi ha accesso non sempre riesce in un uso pienamente efficace, che invece richiede una dimestichezza informatica posseduta solo da una minoranza. Inoltre, ad oggi la prevalenza dei contenuti del *web* è gestita da un novero ristretto di 'emittenti', pur sempre secondo logiche di mercato, con le note implicazioni antidemocratiche. Infine, il caos informativo derivante dalla vastità dei contenuti pubblicati, nella sostanza, equivale a disinformazione[49].

Recentemente, anche tra i promotori dell'uso di internet quale indispensabile strumento migliorativo della democraticità di un sistema, si sono sviluppate critiche alle forme della c.d. 'democrazia liquida', in ragione dell'inopportunità di conferire ai cittadini la possibilità di votare direttamente proposte di legge, in quanto ciò presupporrebbe un bagaglio enorme di conoscenze, che i cittadini non hanno. È stato così proposto un diverso modello di democrazia, detta 'nunciativa', pur sempre basato sull'utilizzo dei nuovi mezzi di comunicazione tecnologica. Questa idea, ferma restando la necessità delle istituzioni parlamentari, implica sempre l'abbandono della democrazia rappresentativa classicamente intesa (ossia senza il vincolo del mandato), ma a favore di un sistema in cui gli eletti abbiano esclusivamente il compito di tradurre in legge, nella maniera più fedele, la volontà dei rappresentati. L'eletto, considerato una sorta di semplice *nuncius*, dovrebbe perciò essere un rappresentante perfetto, ogni volta capace di esprimere il volere della maggioranza dei suoi elettori. Ciò, d'altronde, presuppone la possibilità da parte dell'eletto di conoscere con chiarezza questa volontà, condizione che oggi potrebbe essere realizzata mediante l'impiego delle nuove tecnologie, in particolare di una piattaforma informatica in grado di garantire ampia partecipazione popolare alle scelte politiche e, più specificamente, un rapporto diretto e un controllo dell'elettore sull'eletto[50].

Questo modello abbandona l'idea utopica della 'democrazia liquida' fondata sul potere diretto dei cittadini di fare le leggi, per muoversi verso un vincolo di mandato parlamentare nel quale gli elettori dovrebbero avere il potere, da esercitare mediante la tecnologia informatica, di imporre ai propri rappresentanti gli "obiettivi di massima" da perseguire, nonché di stimolare e controllare la realizzazione di tali obiettivi. A prescindere dalle classiche riserve sull'idea rousseauiana del mandato imperativo[51], il

[48] U. ECO, *Costruire il nemico e altri scritti occasionali*, cit., nel capitolo *Veline e silenzio* afferma: «Internet, naturalmente, rappresenta, senza intento di censura, il massimo del rumore mediante il quale non si riceve nessuna informazione. Ovvero: primo, se si riceve qualche informazione non si sa se è attendibile; secondo, provate a cercare una informazione su Internet: solo noi, uomini di studio, lavorandoci dieci minuti, cominciamo a filtrare e trovare il dato che ci interessa. Tutti gli altri utenti sono fissati su un blog, su un porno specifico ecc., ma mica navigano poi troppo, perché navigare non permette di raccogliere un'informazione attendibile». Si rinvia pure a S. LOMBARDINI, *Accelerare non è fare*, cit., 64 ss.

[49] R. DAVIS, *The Web of Politics. The Internets Impact on the American Political System*, 1999, *passim*; G. MAZZOLENI, *Una rivoluzione 'simbolica'*, in J. ACOBELLI (a cura di), *Politica e internet*, cit., 80 ss.

[50] Il modello è proposto da M. BERNABÈ, S. MARCOLINI, A. ROSTELLO, *Democrazia nunciativa*, cit., *passim*.

[51] Gli argomenti a favore dell'idea che lascia al rappresentante un consistente spazio di autonomia, infatti, tradizionalmente sono fondati sia su ragioni di principio, sia di natura tecnica. Per quanto concerne le

modello della 'democrazia nunciativa', benché costituisca un'interessante sforzo di utilizzo democratico di internet, sembra però non superare le questioni, poste prima, relative alla precondizione del 'come' i cittadini si formeranno le idee intorno agli "obiettivi di massima" da perseguire[52]. Se ciò avverrà pur sempre nella maniera descritta in precedenza, attraverso filtri massmediali in grado di mercificare, banalizzare e distorcere i messaggi, allora – rimanendo alla politica criminale – l'unico argine contro possibili spinte demagogiche, repressive, emotive e irrazionali, resta un legislatore 'illuminato', non 'marketizzato', senza vincolo di mandato.

Oggi, del resto, non è possibile ignorare gli impulsi verso un utilizzo democratico di internet e un atteggiamento fobico verso le nuove tecnologie costituirebbe il segno stantio di una miope politica retriva. Bisogna, invece, riconoscere il potenziale democratico dei *new media*, non come la panacea per tutti i difetti della democrazia, ma come un utile strumento, con le dovute garanzie, per conferire quanto più è possibile la sovranità ai cittadini. Ciò, però, non deve obliterare la consapevolezza che il fulcro della democrazia risiede non solo e non tanto nel momento del voto, ma prima di tutto nella partecipazione alla discussione che richiede una corretta informazione sulle questioni socio-politiche. Orbene, partendo da questo presupposto, le problematiche di democraticità si pongono in maniera analoga sia per i mezzi di comunicazione tradizionali, sia per quelli che utilizzano le nuove tecnologie interattive. In ambo i casi la difficoltà da superare è *in primis* sempre quella dell'equilibrata e corretta formazione e informazione dei cittadini, che, d'altronde, relativamente a internet sembra a tratti più spinosa, sia per la più marcata globalità della sua essenza, sia per la carenza di regole di garanzia, sia per il caos informativo che ne deriva.

Il principio di legalità penale e la legittimazione democratica del legislatore dovrebbero tendere a garantire rappresentatività, razionalità ed estrema prudenza nel ricorso alla sanzione punitiva[53]. Se tali caratteri del sistema penale sono stati da decenni in buona parte compromessi dalla c.d. legislazione dell'emergenza, lo potrebbero essere ancor di più mediante un impiego avventato di internet. Infatti, un uso politico della capacità dialogica di internet (come, ad esempio, i referendum istantanei, o i sondaggi di *marketing* politico, o il voto di proposte da trasferire in Parlamento), se non accompagnato da un coacervo di garanzie di reale democraticità dell'apparato mediatico, sembra allo stato poco compatibile con un sistema penale veramente

---

prime, la libertà di mandato è considerata connessa all'idea di 'bene comune' in base alla quale sono da respingere tutti quegli strumenti capaci di favorire interessi particolari nella sfera pubblica. Sul piano tecnico, invece, il vincolo di mandato troverebbe un ostacolo nell'inquadramento istituzionale del Parlamento, in quanto sarebbe un meccanismo in grado di limitarne o bloccarne il funzionamento. Sul tema in generale si vedano, tra i lavori monografici più recenti, F. GIRELLI, *Insindacabilità parlamentare e divieto di mandato imperativo*, Torino, 2007, *passim*; R. SCARCIGLIA, *Il divieto di mandato imperativo. Contributo a uno studio di diritto comparato*, Padova, 2005, *passim*. Sulle ragioni teoriche del divieto di mandato imperativo, meno recentemente, si veda l'importante, sia pur breve, scritto di E. BURKE, *No al mandato imperativo*, in D. FISICHELLA (a cura), *La rappresentanza politica*, Milano, 1983, 66 ss.; nonché il più corposo lavoro di N. ZANON, *Il libero mandato parlamentare. Saggio critico sull'articolo 67 della Costituzione*, Milano, 1991, *passim*., spec. 87 ss.

[52] Sulle libertà civili come precondizione dell'esercizio dei diritti di partecipazione, si veda A. PACE, *Problematica delle libertà costituzionali. Parte generale. Introduzione allo studio dei diritti costituzionali*, Padova, 2003, 21 ss.

[53] Per tutti, G. FIANDACA, *Legalità penale e democrazia*, in *Quaderni fiorentini*, 2007, 1251; G. DE VERO, *Corso di diritto penale*, Torino, 2012, 243.

improntato all'*extrema ratio*[54]. Gli interessi economici sottesi alla rete, il caos informativo del *web*, l'esiguità di coloro che hanno adeguate conoscenze informatiche, verosimilmente dirigeranno i cittadini verso reazioni emotive, manipolate, poco rappresentative, irrazionali, repressive. Reazioni che, secondo i descritti processi di *marketing* politico, possono concretamente influenzare alcune scelte di politica criminale[55].

L'interattività, dunque, se non accompagnata da talune garanzie, potrebbe alimentare derive plebiscitarie, secondo un modello caricaturale di democrazia diretta, ove si annulla l'argomentazione e il confronto pubblico, a favore di una decisionalità illusoria fondata sulla tirannia di una maggioranza inesistente o mediaticamente strumentalizzata[56]. Il sistema mediatico nel suo complesso, *a fortiori* considerando gli ulteriori pericoli derivanti da internet, sembra perciò insidiare le basi della legalità penale-costituzionale, sotto più profili: una democraticità solo apparente delle scelte mediatiche che influenzano pesantemente e delegittimano la politica criminale[57]; una conseguente legislazione che sovente di fatto mercifica la persona, sacrificandola agli interessi del sistema mediatico secondo logiche di 'esclusione' delle 'classi pericolose' contrarie alle fondamentali garanzie di uno Stato sociale di diritto[58]; una legislazione, ancora, che nel tentativo di rincorrere l'opinione pubblica mediatizzata, affastella norme in un sistema sempre più irrazionale, sproporzionato, caotico e, dunque, in contrasto con le esigenze di *extrema ratio* del diritto penale.

5. Un'auspicabile *Bildung* politico-criminale e il ruolo della cultura giuspenalistica

Se, da un lato, è indubbio che in un modello democratico il controllo delle istituzioni non possa essere prerogativa di un'*élite* illuminata a prescindere dalla sua rappresentatività popolare, ma vada esteso in qualche modo – sia pur indirettamente – a tutti i cittadini; dall'altro lato, è altrettanto evidente che i cittadini, affinché le istituzioni abbiano maggiori *chance* di operare correttamente, dovrebbero possedere una competenza politica, intesa come consapevolezza del 'bene pubblico' e delle questioni *lato sensu* politiche[59]. Tale consapevolezza, è noto, si consegue attraverso le agenzie

[54] Secondo P. CERI, *Promesse e realtà della teledemocrazia*, in P. FANTOZZI (a cura di), *Politica, istituzioni e sviluppo*, Soveria Mannelli, 2001, 98, più che di trasferimento di potere ai cittadini, si tratta di occultamento dello stesso, in quanto – anche escludendo l'uso di collaudate tecniche distorsive, psicologiche o statistiche –, il trasferimento è illusorio perché la partecipazione è soggetta a manipolazioni e a deresponsabilizzazione, e le risposte, quando non sono meri effetti di 'trascinamento', in genere sono reazioni a vicende emotive del giorno.

[55] M. ARTUSI, A. MAURIZZI, *Le nuove frontiere del marketing politico. Internet come strumento di costruzione e gestione del consenso*, in *Mercati e competitività*, 2010, 75 ss., pensano ad internet come strumento di coinvolgimento di persone attorno ad un movimento o idea politica attraverso le tecniche del *marketing*.

[56] N. RANGERI, *Il rischio della democrazia diretta*, in J. ACOBELLI (a cura di), *Politica e internet*, cit., 116; D. PITTÈRI, *Democrazia elettronica*, cit.; P. CERI, *Promesse e realtà della teledemocrazia*, cit., 98,

[57] Sulle implicazioni della democraticità del sistema mediatico su quella del sistema penale, si vedano le fondamentali osservazioni di F. PALAZZO, *Mezzi di comunicazione*, cit., 200 ss.

[58] C.E. PALIERO, *La maschera e il volto*, cit., 536-537.

[59] Su questi temi si veda R.A. DAHL, *The Problem of Civic Competence*, in *Journal of Democracy*, 1992, 45 ss., ora in ID., *Politica e virtù. La teoria democratica nel nuovo secolo*, a cura di S. FABBRINI, Roma - Bari, 2001, 134 ss., il quale definisce anche il concetto di bene pubblico, secondo una visione classica (bene generale) e una più attuale e coerente con l'individualismo moderno (aggregazione degli interessi

formative, tra le quali un ruolo determinante è svolto dai mezzi di comunicazione e oggi in particolare da internet[60].

È difficilmente discutibile, dunque, che i processi democratici operano più adeguatamente solo se buona parte degli elettori gode di alcuni livelli minimi di conoscenza. Tali standard – sempre più faticosi da raggiungere man mano che aumenta il livello delle difficoltà delle questioni pubbliche – non sono tanto quantitativi, ma anzitutto qualitativi. Una maggiore competenza dei cittadini, perciò, non è legata di per sé ad una maggiore informazione. Anzi, come accade per i *new media*, l'eccesso di informazioni, di fatto, impedisce la formazione di un'adeguata conoscenza dei fenomeni. L'affastellamento di innumerevoli notizie, a prescindere dallo loro possibile manipolazione, rende la collettività satura di informazione, ma povera di conoscenza, assuefatta, distratta, incapace all'esercizio di vero senso critico[61].

La constatazione delle lacune e perversioni del sistema penal-mediatico, non esime dal propugnare la necessità di uno sforzo verso la maturazione di tale sistema e dal suggerirne possibili modalità. Si potrebbe auspicare una sorta di *Bildung* o *paideia* politico-criminale adeguata alle esigenze democratiche e massmediali postmoderne, nel tentativo, molto ambizioso, di tracciare il contenuto ontologico dei livelli minimi di conoscenza dei cittadini, come interiorizzazione di quei valori fondamentali costituenti l'*ethos* della società civile. Tale conoscenza potrebbe essere veicolata, nei limiti della compatibilità, anche avvalendosi della comunicazione massiva[62]. Naturalmente non nel senso di 'pedagogia di Stato' attraverso strumenti coattivi di controllo dei mass media, ma nel senso di *Bildung* come 'contatto con la cultura', come 'formazione umana', estrinsecazione di libertà, attraverso un processo continuo che impegna l'uomo a realizzare se stesso in quanto soggetto autonomo nella dimensione della vita associata, in cui l'individuo afferma la propria natura, essenzialmente sociale e politica. Dunque, una formazione continua dell'uomo che si avvicina progressivamente alla cultura e, di fronte ad essa, non ha un atteggiamento passivo, bensì volto a porre problemi, sviluppando l'intelligenza attraverso il dubbio[63].

L'esigenza di questa sorta di *Bildung* politico-criminale è tanto più avvertita quanto più si constata che, attualmente, la generalità dei consociati non entra affatto in contatto con la cultura giuspenalistica e criminologica, ma, attraverso i mass media, esclusivamente con le descritte visioni semplicistiche e 'mercificate' del fenomeno criminale. Il modello a cui ispirarsi in questa *paideia* politico-criminale dovrebbe essere conforme ai principi di una legittima politica criminale di uno Stato sociale di diritto, orientato verso una logica 'inclusiva' che privilegia garanzie e diritti, e non 'esclusiva' che invece attualmente sembra qualificare la rappresentazione mediatica del fenomeno criminale[64]. Un modello, insomma, di una 'società aperta' in cui «la libertà degli individui, la non-violenza, la protezione delle minoranze, la difesa dei deboli sono valori

---

individuali).

[60] «L'educazione consiste principalmente nella trasmissione per mezzo della comunicazione», cfr. J. DEWEY, *Democrazia e educazione* (1916), Firenze, 2000, 12.

[61] G. GIOSTRA, *Processo penale*, cit., 64.

[62] Sulla dimensione educativa dei media, recentemente si veda P. AROLDI, *La responsabilità difficile. Media e discernimento*, Soveria Mannelli, 2012, 101 ss..

[63] Per un'esauriente analisi del concetto di *Bildung* e delle sue rielaborazioni, si veda F. CAMBI, *I grandi modelli della formazione*, in F. CAMBI, E. FRAUENFELDER (a cura), *La formazione. Studi di pedagogia critica*, Milano, 1994, 63 ss.

[64] C.A. PALIERO, *La maschera e il volto*, cit., 536-537.

importanti»[65].

Non essendo possibile immaginare cittadini onniscienti, questa *Bildung* chiaramente non potrebbe spingersi verso i concetti più complicati e raffinati, ma al più dovrebbe mantenersi, attraverso metodi comunicativi semplificati, sul piano valoriale dei principi di una legittima politica criminale che costituiscono la struttura portante dei moderni sistemi penali occidentali. La finalità, insomma, dovrebbe essere quella di trasmettere ai cittadini gli strumenti culturali minimi per consentire una lettura consapevole del fenomeno criminale, per conoscere i presupposti essenziali di legittimità delle scelte legislative di penalizzazione, per consentire una basilare analisi critica delle tendenze giudiziarie. Tale processo necessiterebbe di molto tempo, quello occorrente affinché tali principi e valori siano maturati, 'digeriti', interiorizzati dalla collettività al punto da ridurre le spinte più emotive, irrazionali e repressive che attualmente caratterizzano il sistema penal-mediatico.

L'idea probabilmente può apparire ingenuamente utopica, irrealizzabile se paragonata alla concretezza della realtà. Ma tale conclusione forse trascura la capacità, l'intelligenza collettiva se posta a 'contatto con la cultura', cosa che attualmente non ha luogo. Del resto, fino a quando i principi di una legittima politica democratica non verranno interiorizzati nell'*ethos* della società, di fatto i meccanismi democratici non potranno funzionare del tutto correttamente e permarranno sempre conflitti più o meno latenti tra opinione pubblica, mass media, politica, magistratura, scienza.

L'acquisizione di questo *ethos* politico-criminale, peraltro, è evidente che incontra degli ostacoli difficili da superare. *In primis* nel sistema mediatico, in quanto è evidente che una *Bildung* rivolta ai principi e valori non ha la capacità seduttiva di quelle informazioni che sollecitano più direttamente le corde emotive del pubblico. Ciò implica che i mass media dovrebbero abbandonare, almeno in parte, l'*agenda setting* incentrata esclusivamente sulla commerciabilità delle informazioni, per aprirsi, mediante operatori dell'informazione dotati di un'attrezzatura culturale adeguata, ad una lettura del fenomeno criminale più critica e meno sensazionalistica.

Gli ostacoli che si incontrano nel sistema politico, invece, sono legati alla 'marketizzazione' delle scelte. L'esercizio della politica, infatti, dovrebbe estrinsecarsi in un effettivo e alto confronto culturale e nell'adottare delle decisioni, a volte a primo acchito impopolari, ma ispirate a opzioni ideologiche/valoriali di fondo in grado anch'esse di svolgere un ruolo pedagogico. In ciò, il mondo politico dovrebbe aprirsi maggiormente alla cultura penalistica e criminologica, accettandone almeno quei risultati consolidati da decenni di univoche ricerche[66]. Tra i compiti del giurista, infatti, accanto a

[65] K. POPPER, *Il futuro è aperto*, Milano, 1989, 176.

[66] Sul rapporto tra scienza penalistica e politica, la letteratura è vasta. Tra i tanti, si vedano, in vario senso, C. ROXIN, *Kriminalpolitik und Strafrechtssystem*, Berlino, 1970, trad. it. *Politica criminale e sistema del diritto penale*, a cura di S. Moccia, Napoli, 1998; G. VASSALLI, *Politica criminale e sistema penale*, ne *Il Tommaso Natale*, 1978, *Scritti in memoria di Girolamo Bellavista*, vol. II, 999 ss.; S. MOCCIA, *Politica criminale e riforma del sistema penale. L'Alternativ-Entwurf e l'esempio della Repubblica federale tedesca*, Napoli, 1984; F. BRICOLA, *Rapporti tra dogmatica e politica criminale*, in *Riv. it. dir. proc. pen.*, 1988, 3 ss.; F. PALAZZO, *Scienza penale e produzione legislativa: paradossi e contraddizioni di un rapporto problematico*, in *Riv. it. dir. proc. pen.*, 1997, 693 ss.; M. DONINI, *Metodo democratico e metodo scientifico nel rapporto fra diritto penale e politica*, in *Riv. it. dir. proc. pen.*, 2001, 27 ss.; più recentemente, ID., *Democrazia e scienza penale nell'Italia di oggi: un rapporto possibile?*, in *Riv. it. dir. proc. pen.*, 2010, 1067 ss.; F. PALAZZO, *"Requiem" per il codice penale? (Scienza penale e politica dinanzi alla ricodificazione)*, in *Cass. pen.*, 2011, 4064 ss.

quelli più tradizionali dell'interpretazione delle norme, dell'astrazione dommatica e della sistematizzazione, vi sono anche quelli relativi alla politica criminale e alla riforma legislativa[67]. In ragione di ciò, coerentemente con la libertà di ricerca e di opinione, è compito della «scienza giuridica far sentire la propria voce, già nella fase progettuale delle norme, per orientare le scelte del legislatore in conformità ai principi di una legittima politica criminale ed ai principi di una corretta attività di normazione […] La scienza può pretendere attenzione unicamente attraverso la sua autorevolezza, connessa ad una forte capacità di comunicazione»[68].

È indispensabile, dunque, una comunicazione razionale tra scienza e legislatore, ma anche qualora si raggiungesse questo fondamentale obiettivo, alla luce dei descritti meccanismi 'marketizzati' che condizionano le odierne scelte politiche di criminalizzazione, è verosimile che l'auspicabile autorevolezza della dottrina risulti comunque pressoché impotente a fronte di opzioni legislative che si esauriscono in ciò che sembra volere l'elettorato mediaticamente condizionato, a prescindere dai principi di una legittima politica criminale, attualmente quasi ignoti al 'grande pubblico'[69]. La scienza, allora, oltre all'essenziale canale di comunicazione con il legislatore, potrebbe aprirne uno meno indiretto anche con i cittadini, con quello strato della società che forma la c.d. opinione pubblica, comunicazione un tempo pressoché impensabile e che oggi, invece, potrebbe essere facilitata proprio attraverso le nuove tecnologie come internet.

La scienza giuspenalistica, a partire da quella più giovane, dovrebbe allora occuparsi più di politica criminale, mostrandosi anche maggiormente aperta alle esigenze e speranze della collettività. La dottrina dovrebbe dunque scendere dalla 'torre eburnea', dovrebbe abbandonare l'atteggiamento più 'aristocratico' che in parte conserva, distaccato, scarsamente interessato alle implicazioni più 'popolari' della politica criminale, impegnandosi invece in un ruolo attivo in questa sorta di *Bildung* politico-criminale, pure attraverso i media[70]. D'altronde, la possibilità di svolgere concretamente questo ruolo di

[67] Si veda S. MOCCIA, *L'odierna funzione di 'controllo' e "orientamento" della dottrina*, cit., 415, il quale, tra l'altro, ha evidenziato la necessità di una robusta interazione tra politica criminale e dommatica, in maniera tale che la funzione della scienza penalistica si rivolga legittimamente anche, appunto, alla politica criminale e alla legislazione. Il dogmatismo meramente tecnicistico, secondo lo stesso Autore, finisce invece per assecondare scelte illiberali, allorché dà la stura a giustificazioni teoriche volte ad escludere le problematiche di politica criminale dalla teoria del sistema penale. Per l'esigenza della costruzione di un sistema penale che assuma come principi di riferimento i valori politico criminali di derivazione liberal-solidaristica, sovente normativizzati nelle Costituzioni orientate ai principi dello stato sociale di diritto, si rinvia al fondamentale lavoro di C. ROXIN, *Kriminalpolitik und Strafrechtssystem*, cit., 37 ss.

[68] Cfr. sempre S. MOCCIA, *L'odierna funzione di 'controllo' e "orientamento" della dottrina*, cit., 417, 419 .

[69] Emblematiche, in merito, le parole del recente *Discorso del Santo Padre Francesco alla delegazione dell'Associazione internazionale di diritto penale*, in *Bollettino Sala stampa della Santa Sede n. B0787*, tenuto nella Sala dei Papi il 23 ottobre 2014: «C'è il rischio di non conservare neppure la proporzionalità delle pene, che storicamente riflette la scala di valori tutelati dallo Stato. Si è affievolita la concezione del diritto penale come *ultima ratio*, come ultimo ricorso alla sanzione, limitato ai fatti più gravi contro gli interessi individuali e collettivi più degni di protezione. Si è anche affievolito il dibattito sulla sostituzione del carcere con altre sanzioni penali alternative. In questo contesto, la missione dei giuristi non può essere altra che quella di limitare e di contenere tali tendenze. È un compito difficile, in tempi nei quali molti giudici e operatori del sistema penale devono svolgere la loro mansione sotto la pressione dei mezzi di comunicazione di massa, di alcuni politici senza scrupoli e delle pulsioni di vendetta che serpeggiano nella società».

[70] Sul tema si veda M. DONINI, *Il diritto penale di fronte al "nemico"*, cit., che parla di un compito permanente della scienza penale di controllo critico sugli eccessi irrazionali della "democrazia penale", che

guida nel percorso collettivo di 'contatto con la cultura' giuspenalistica, è legato ad uno sforzo di maggiore unitarietà della dottrina, almeno sulle questioni cardinali, ossia sui principi di una legittima politica criminale. In mancanza di un messaggio scientifico armonico, da un lato si fornirebbe il pretesto alla politica per sviare le riforme; dall'altro, il messaggio discorde sarebbe fuorviante e incapace di consolidare quell'*ethos* collettivo cui tendere.

La pur immaginabile velletarietà della ipotizzata *Bildung* politico-ciminale potrebbe però essere dimostrata solo dopo averne constatato seriamente il pratico insuccesso. Prima di allora, prima di aver adottato concrete e durature azioni in tal senso, pur con tutte le difficoltà implicate, sembra rimanere uno strumento cui anelare se si vuole tentare di ridurre la natura simbolica ed emergenziale che attualmente presenta il sistema penale. Gli sforzi volti all'interiorizzazione sociale dei principi a fondamento di una legittima politica criminale, verosimilmente non risolverebbero l'interezza delle criticità del sistema penale, ma di certo non le aggraverebbero. Ogni 'contatto con la cultura', anche mediatico, non mercificato, non semplicistico, semmai potrà portare benefici al consorzio civile, altrimenti bisognerebbe diffidare completamente delle capacità di discernimento della collettività, ossia negare le basi stesse di ogni modello democratico.

---

dovrebbe svolgersi, in forma divulgativa, anche sui mass media, perché ad altri livelli il discorso rimane specialistico, senza nessuna possibilità di influenza sull'opinione pubblica. Recentemente, sul dibattito generale intorno al ruolo della dottrina nella formazione e legittimazione del diritto penale, si vedano J.L. GONZÁLEZ CUSSAC, *Gli orizzonti, vecchi e nuovi, della dogmatica*, in *Criminalia*, 2013, 363 ss.; A. MANNA, *La dottrina tra legislazione e giurisprudenza nel sistema penale*, ivi, 389 ss.; S. MOCCIA, *L'odierna funzione di 'controllo' e "orientamento" della dottrina*, cit., 409 ss.

UNO STATUTO PENALE PER *INTERNET*
VERSO UN DIRITTO PENALE DELLA PERSUASIONE

Pasquale Troncone

Sommario: 1. La progressiva rilevanza giuridica della "società della Rete", le fonti europee e la Costituzione italiana 2. La Rete come interesse primario da proteggere. Il diritto penale come Agenzia di controllo transnazionale 3. Il consenso come cardine del nuovo "ambiente giuridico". L'inglobamento in Rete del complesso delle relazioni private e istituzionali 4. Un nuovo ruolo del diritto penale: verso la palinodìa o la negazione degli assetti tradizionali? 5. I problemi di certificazione di attendibilità delle informazioni nella Rete 6. Le linee sistematiche di una proposta cautelare e sanzionatoria per gli illeciti commessi in Rete. La responsabilità penale da ambiente informatico

1. La progressiva rilevanza giuridica della "società della Rete", le fonti europee e la Costituzione italiana.

Siamo giunti al punto in cui la storia dell'uomo deve fare i conti con la pervasività della tecnologia che ha traghettato, tutti inconsapevoli della notevole ridondanza dei suoi effetti, la comunità globale in un mondo intriso di realtà artificiale [1]. Una rivoluzione industriale post-moderna, in cui lo scopo non è costituito da un modo diverso di produrre ricchezza ma dove diversa diventa la persona stessa, con un fine che non muta: l'economia condiziona i rapporti sociali con mezzi nuovi, coinvolgendo le persone che da soggetti si trasformano in operatori, consumatori e utenti. La stessa economia muta i suoi connotati di valore e da economia fondata su beni e finanza si trasforma in "*economia informazionale*" dove il valore intrinseco che il mercato gli riconosce viene individuato nella rilevanza della informazione [2]. In questo modo l'economia informazionale genera un nuovo assetto dei rapporti economici senza confini e con essa un nuovo ordine sociale dove la realtà senza alcun supporto materiale incrocia il mondo corporeo.

Il punto da cui origina questa nuova vicenda umana è quello in cui si opera la divaricazione tra *corpo fisico* e *corpo elettronico* della persona, approdata ormai alla duplice sponda dove il reale si dissocia in realtà concreta e realtà immateriale o artificiale (spesso si trova in uso quest'ultima definizione che in realtà suona inappropriata, come "pura invenzione", mentre così non è), generando una nuova endiadi "*mondo fisico*" - "*mondo elettronico*"[3].

[1] S. COTTA, *La sfida tecnologica*, Il Mulino, Bologna, 1968.

[2] Sul punto è interessante l'analisi di internet come fattore economico e come fattore di sviluppo che entra a far parte del calcolo del PIL nazionale, in BOSTON CONSULTING GROUP (BCG), *Fattore Internet: come Internet sta trasformando l'economia italiana*, in *www.fattoreinternet.it.*

[3] Sulla base del pensiero di Michel Foucault, che ha curato J. BENTHAM, *Panopticon ovvero la casa d'ispezione*, Marsilio, Venezia, 1983, il corpo dissociato viene discusso in S. RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Il Mulino, Bologna, 2006, 73. D. LYON, *La società sorvegliata*, Feltrinelli, Milano, 2003, 96 e ss. S. RODOTÀ, *Trasformazioni del corpo*, in *Pol. del dir.*, n. 1, 2006, 3. G. RESTA, *Identità personale e identità digitale*, in *Dir. Informatica*, fasc. 3, 2007, 511.

Il concetto con cui si intende definire la realtà artificiale che veniva qualificata come "realtà virtuale" cioè "dematerializzata", distinguendola dalla realtà naturale, vale a dire il complesso delle informazioni aggiunte o sottratte elettronicamente al punto che le persone si trovano immerse in una situazione nella quale le percezioni naturali di molti dei cinque sensi non sembrano neppure essere più presenti, appare oggi a rischio e surrogato da un altro progressivo concetto definito di "realtà aumentata", in cui vi è un arricchimento della percezione sensoriale umana mediante informazioni, -in genere manipolate- e convogliate elettronicamente, che non sarebbero neppure percepibili con i cinque sensi.

Queste sono le ragioni per cui è necessario prendere atto di una nuova dimensione dei rapporti umani e del rapporto tra "individuo" e "persona" -come formanti di un medesimo "soggetto"- che progressivamente invoca un sempre maggiore intervento del diritto per governare rapporti giuridici e tutelare posizioni soggettive con forme regolative nuove e, forse, inconsuete per la tradizione.

Il mondo immateriale la cui matrice genetica è costituita dai flussi dei dati informatici è tale da rivelarsi agli occhi dell'osservatore comune come un immenso contenitore di informazioni, vicende personali e sociali che coinvolgono persone non sempre adeguatamente tutelate e protette da condotte offensive la cui rapidità e la cui distanza non sempre sono facilmente controllabili ed evitabili[4].

Tuttavia spetta agli strumenti normativi stendere un velo di protezione contro le iniziative lesive la cui molteplicità di forme e di obiettivi è direttamente proporzionale alla enorme vastità della rete informatica[5]. Le stesse definizioni del mondo immateriale della rete provano la oggettiva difficoltà di affrontare adeguatamente il tema delle tutele, si pensi alla incontenibile definizione del *web* (letteralmente ragnatela) che viene utilizzata per compendiare l'insieme dei siti *Internet.*

La crescita degli utenti in *Internet* ha portato alla strutturazione di una vera e propria "*società in rete*" [6] e come tutti gli aggregati umani, oltre alla vita di relazione interpersonale -collettiva e confidenziale-, nasce l'esigenza di regolamentare un vero e proprio ordinamento giuridico che affonda le sue ragioni nelle regole del corretto (o controllato) funzionamento di un sistema sociale che, questa volta, scivola attraverso la strumentalità di operazioni informatiche[7]. Occorre, quindi, progettare una disciplina per un ordine sociale non materiale e che non può essere governato dalle regole e dalle sanzioni del mondo corporeo, semplicemente perché al centro del sistema delle relazioni si trova l'"informazione"[8], destinata a diventare la nuova base operativa per lo

[4] G. ALPA, *Privacy e statuto dell'informazione*, in *Riv.dir.civ.*, 1979.

[5] Sulla questione V. ZENO ZENCHOVIC, *Informatica ed evoluzione del diritto,* in *Dir.informaz. e informatica*, 2003, pag. 89: "*Se sulla scena compaiono in maniera così pervasiva gli elaboratori, i programmi, le reti che interconnettono i primi, l'utilizzo dei secondi in praticamente qualsiasi bene dotato di una certa complessità, è ovvio che ci vorranno regole giuridiche che si occupino di questi fenomeni, li classifichino, ne stabiliscano i rapporti con quanto già esistente*".

[6] Secondo la felice intuizione di M. CASTELLS, *La nascita della società in rete*, Egea, Milano, 2014, 27.

[7] SANTI ROMANO, *L'ordinamento giuridico*, Firenze, 1951.

[8] Effettivamente in termini giuridici, ma ancor più importante suona in termini penalistici, il significato di informazione come un autonomo bene giuridico, come sostenuto da P. PERLINGIERI, *L'informazione come bene giuridico*, in *Rass. di dir. civ.*, 1990. G. PASCUZZI, *Il diritto dell'era digitale*, Il Mulino, Bologna, 2002.

sviluppo ordinato di un ordine sociale di nuova generazione e una nuova struttura sociale che riconosca a ciascun utente la "cittadinanza digitale"[9].

Un cambio di prospettiva s'impone quindi in questo spazio tecnologico, entrato sì a far parte del sistema delle leggi, ma ancora privo di uno statuto coerente e sistematico che offra garanzie alla stessa Rete e ai diritti di coloro che vi entrano in contatto. E' giunto, infatti, il momento in cui occorre stabilire la griglia dei principi fondamentali per l'impiego di *Internet* sulla base della centralità degli interessi e dei diritti della persona umana, tenuto conto che attraverso la Rete si legano ormai tutti i rapporti tra singoli e tra individuo e Istituzioni[10].

Sul terreno normativo non mancano riferimenti di valore importanti che possono diventare fondativi per il diritto della Rete, ma soprattutto possono stabilire i margini dell'intervento di tutela secondo una concezione di tipo teleologico. In primo luogo la centralità della persona si coglie nella individuazione della titolarità ed esclusività dei dati personali e identificativi come riportata nella Carta dei diritti fondamentali dell'Unione Europea che stabilisce all'art. 8 "*Protezione dei dati di carattere personale*": "1. *Ogni persona ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*".

Altra fonte di sicura rilevanza è la Convenzione Europe dei Diritti dell'Uomo che all'art. 8 "*Diritto al rispetto della vita privata e familiare*", prescrive che "*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*".

Entrambe le norme fondano una precisa e autonoma area di tutela ma non ancora viene perimetrato l'ambito operativo dove si può esprimere appieno la protezione dei diritti così enucleati.

La questione della fondazione costitutiva di *Internet* nasce su questa prospettiva normativa, e non può essere considerata soltanto come l'esigenza di stabilire le procedure operative da seguire nell'uso della Rete e la correttezza delle modalità di svolgimento delle procedure standardizzate, ma si deve concretizzare una piattaforma giuridica finalizzata a tutelare la stessa Rete da abusi e illeciti da parte degli utenti.

Il tema intercetta oggi i lavori della Commissione parlamentare presieduta dal Prof. Stefano Rodotà chiamata a elaborare un testo normativo per l'esercizio dei diritti in Rete e la tutela di coloro che vi navigano[11]. Il testo, ancora provvisorio e aperto al contributo di tutti i cittadini, è stato presentato il 13 ottobre 2014 e, oltre a riportare la

[9] G. GRANIERI, *La società digitale*, Laterza, Roma-Bari, 2006. S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Laterza, Roma-Bari, 2014, 13.

[10] Un "*Internet Bill of Rights"* secondo S. RODOTÀ, *Il mondo nella rete cit.*, 61.

[11] S. RODOTÀ, *Una costituzione per internet?*, in *Pol. del dir.*, 2010, 337.

disciplina ripartita in 14 paragrafi, si apre con un Preambolo -tipico delle Carte costituzionali moderne- intitolato "*Dichiarazione dei diritti in internet*"[12]. A cominciare dal Preambolo risulta in maniera estremamente chiara che la Rete non può più essere considerata soltanto come l'ambiente immateriale in cui reperire notizie e informazioni secondo un profilo semplicemente dichiarativo degli atti giuridici, ma si è trasformata in un vero e proprio settore dove le dinamiche di relazione sociale assumono connotati di tipo costitutivo che vengono conferiti a tutte le operazioni e le informazioni che in quello spazio sono sottoposte a trattamento e diffuse.

La vera rivoluzione culturale che si coglie nei principi regolatori è l'aver stabilito un collegamento funzionale tra i diritti fondamentali della persona umana, che passano in particolare attraverso l'eguaglianza e la "*diversità*" -principio quest'ultimo ancora sconosciuto al mondo giuridico- e la vita delle Istituzioni, nel senso che il funzionamento democratico delle Istituzioni dipende unicamente dal rispetto dei principi della persona umana e in questo modo respingere ogni tentativo dei poteri pubblici o privati di creare una società sorvegliata per il controllo e la selezione sociale[13].

Ma in realtà la Rete ha con il tempo guadagnato uno spazio autonomo al punto da diventare essa stessa centro di diritti, assumendo a fondamento il più generale diritto di libertà nell'ambito del quale *Internet* si ritaglia uno spazio di autonomia, il cui referente di valore viene tradizionalmente rintracciato nell'art. 15 della Carta fondamentale del 1948 ma che si ridefinisce come un vero e proprio diritto di libertà fondamentale della società umana e transazionale, secondo la previsione di orientamento dell'art. 2 della Costituzione italiana.

In questo progressivo accrescimento del rilievo sostanziale, *Internet* acquisisce lo *status* di bene giuridico con individuale e autonoma rilevanza, semplicemente considerando le sue naturali coordinate identificative che gli conferiscono sempre crescente importanza: la dimensione spaziale, il numero di utilizzatori, la frequenza di uso, l'utilità delle informazioni reperite, la libertà di comunicare in tempo reale con chiunque, la forma gratuita, il valore probatorio delle informazioni reperite in Rete, la pluralità e l'importanza dei soggetti istituzionali coinvolti nella Rete, la funzione di mezzo esclusivo per il rapporto cittadini-pubbliche istituzioni, il nuovo sistema delle transazioni commerciali (l'*e-commerce*), l'incidenza sul PIL nazionale.

2. La Rete come interesse primario da proteggere. Il diritto penale come Agenzia di controllo transnazionale

Il complesso e composito mondo che integra il *network* alimentato da *Internet*, avendo acquisito, e si è visto, una dimensione materiale e giuridica del tutto autonoma e singolare, emerge come un universo operativo che progressivamente ha maturato una sua indipendente operatività, fino raggiungere una individualità che pone al giurista una specifica istanza di protezione. Una richiesta di tutela che non ha confini geografici e normativi ma che per sua natura è di tipo transnazionale, al punto da intersecare in

[12] Reperibile in *www.parlamento.it*.

[13] D. LYON, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Feltrinelli, Milano, 1997. RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973. Z. BAUMAN, *Dentro la globalizzazione. Le conseguenze sulle persone*, Laterza, Roma-Bari, 2006, 56 e ss. M. CASTELLS, *Galassia internet*, Feltrinelli, Milano, 2013, 163.

maniera trasversale molteplici ordinamenti giuridici e con essi molteplici assetti legislativi.

Il primo presidio di protezione appare dunque quello della uniformità di regolazione dei rapporti individuali, ma allo stesso tempo collettivi, tra chi usa *Internet* e tra il singolo utente e gli ordinamenti coinvolti. Questo nuovo moderno spaccato giuridico presenta una particolare singolarità strutturale ove l'operatività strumentale condiziona i diritti e le posizioni giuridiche dei singoli, nel senso che la tutela del singolo utente deve necessariamente derivare dalla garanzia della regolare funzionalità del sistema informatico che costituisce la base operativa della Rete.

Questa è la ragione per cui l'indagine sui requisiti dei presidi di protezione deve necessariamente partire dall'assunto che occorre assicurare una tutela primaria a *Internet* per aprire un nuovo orizzonte in cui le istanze di salvaguardia non siano rivolte soltanto ai singoli utenti, proprio perché la Rete appare destinata ad acquisire in maniera sempre più definita la natura di espediente attuativo delle democrazie moderne[14]. Il diritto penale dunque come strumento di giustiziabilità dei diritti è chiamato a svolgere un ruolo di protezione, in modo che, in una prospettiva teleologica tradizionale, il primo interesse da tutelare sia proprio *Internet*.

In questo modo sembra però messo alle corde il sistema penale dell'offensività costituzionale, come sfondo di protezione del bene giuridico di riferimento, che, allo stesso tempo, rappresenterà l'oggetto di tutela e il limite di applicazione di una norma penale, soprattutto quando un bene strumentale, come la Rete, sopravanza in valore la categoria dei diritti fondamentali della persona[15]. Ma in realtà il vero punto di svolta si coglie in questa solo apparente strozzatura del sistema dei valori, poiché la chiave interpretativa della rilevanza degli interessi vuole *Internet* come una componente costitutiva del sistema democratico moderno ed esso stesso la migliore garanzia dei diritti fondamentali della persona. In altri termini, un nuovo diritto primario la cui tutela è determinante perché l'unico in grado di garantire appieno il complesso assetto dei diritti fondamentali della persona umana, proprio nel rispetto della scala dei valori costituzionali. Dunque, conferma del fondamento teleologico del sistema penale e allo stesso tempo rispetto della Carta costituzionale nazionale, di quella europea e della Convenzione Europea dei diritti dell'Uomo[16].

---

[14] S. RODOTÀ, *Il mondo della rete*, Laterza, Torino, 2014.

[15] F. MANTOVANI, *Il principio di offensività nella Costituzione,* in *Aspetti e tendenze del diritto costituzionale. Scritti in onore di Costantino Mortati,* Giuffrè, Milano, 1977, vol. IV, *Le garanzie giurisdizionali e non giurisdizionali del diritto obiettivo,* 447. G. MARINUCCI - E. DOLCINI, *Costituzione e politica dei beni giuridici,* in *Riv.it.dir. e proc.pen.,* 1994, 333. F. PALAZZO, *Meriti e limiti dell'offensività come principio di ricodificazione,* in *Prospettive di riforma del codice penale e valori costituzionali,* Giuffrè, Milano, 1996, 73. S. MOCCIA, *Il diritto penale tra essere e valore,* Esi, Napoli, 1992, 32. MOCCIA S., *Sui principi normativi di riferimento per un sistema penale teleologicamente orientato,* in *Riv.it.dir. e proc.pen.,* 1989, 1006. M. DONINI, voce *Teoria del reato,* in *Dig. disc. pen.,* vol. XIV, 1999, 226. G. FIANDACA, *La giustizia penale in Bicamerale,* in *Foro it.,* 1997, parte V, coll. 167. G. FIANDACA, *Legalità penale e democrazia,* in *Quad. fior.,* 2007, pag. 1247. V. MANES, *Il principio di offensività nel diritto penale,* Giappichelli, Torino, 2005. D. PULITANÒ, *Obblighi costituzionali di tutela penale?,* in *Riv.it.dir. e proc.pen.,* 1983, 498.

[16] Le dinamiche di sviluppo del costituzionalismo moderno rispetto al diritto penale (e processuale) classico, che a sua volta evolve dall'ambito meramente sanzionatorio e punitivo a quello aperto alla propedeutica tutela dei diritti e dei valori, sono senza alcun dubbio la base di discussione per un assetto giuridico che guadagna nuove coordinate operative, tipiche del mondo immateriale della Rete

In previsione dei nuovi assetti che dovrebbero orientare un diritto penale continentale fondato sulla molteplicità generativa delle fonti internazionali e soprattutto per il ruolo chiamato a svolgere circa gli obblighi di tutela di "nuova generazione", si pone in termini problematici un'altra categoria concettuale che rappresenta il punto estremo degli impegni di protezione normativa, quella del "*divieto di depenalizzazione*" che acquista spazio sulla base delle scelte della giurisprudenza sovranazionale[17]. Una legittimazione che non origina non dall'esistenza di un obbligo specifico ma dalla necessità di riconoscere rilevanza ordinamentale a un valore nuovo che non merita di degradare a fatto indifferente per il diritto penale.

La nuova dimensione spaziale del diritto penale, nella sua funzione di controllo dei comportamenti e delle iniziative di conformazione, ne qualifica la veste ordinamentale costituendolo come una nuova Agenzia di controllo su tutto il mondo delle relazioni che s'intrecciano all'interno della Rete. Un'Agenzia che, come per gli ordinamenti coinvolti, attraversa trasversalmente tutti i nodi della Rete e i *provider* che operano a livello planetario, nel tentativo di uniformarne i comportamenti e prevenire condotte illecite e comunque utilizzare questa capacità di condizionamento per imporre ai singoli utenti atteggiamenti rispettosi di una convivenza civile che non passa per la materialità dei contatti personali.

A ben vedere può essere interessante il ruolo del diritto penale in questo ambito, occupato, per la gran parte da soggetti sufficientemente alfabetizzati, in parte perché "nativi digitali", in altra parte per avere acquisito successivamente le capacità operative, un ruolo che non può essere confinato alla punizione o alla deterrenza ma che si apre a propositivi di comportamenti virtuosi (si vedrà più avanti il senso). In realtà l'Agenzia di controllo deve servire a svolgere un controllo sociale non sugli utenti ma sulla Rete, un controllo sociale a difesa della Rete e, solo in questa dimensione, a difesa del singolo utente. Anche se va precisato che, se è pur vero che la Rete va salvaguardata come un bene primario, la persona umana non perde la sua centralità rimanendo il naturale destinatario delle scelte politico-legislative.

In questa chiave fondativa il diritto penale può ricoprire il ruolo decisivo di controllo, non di controllo sociale, ma di una forma di vigilanza che assicuri un libero e incondizionato uso della Rete da parte di ciascuno senza alcuna limitazione, come nello spirito della democrazia.

Particolarmente interessanti e precise sono le riflessioni di S. STAIANO, *Per orbite ellittiche. Modello garantista, valore della certezza, diritto penale*, in *www.associazionedeicostituzionalisti.it*, 2011.

[17] S. MANACORDA, *"Dovere di punire"? Gli obblighi di tutela penale nell'era della internazionalizzazione del diritto*, in *Il lato oscuro dei diritti umani. Esigenze emancipatorie e logiche di dominio nella tutela giuridica dell'individuo*, a cura di Meccarelli M., Palchetti P., Sotis C., Universidad Carlos III de Madrid, 2014, 307. Sulla questione degli obblighi di depenalizzazione a pag. 310: "*Il divieto di depenalizzazione (in senso lato) afferisce ugualmente alla categoria degli obblighi di natura sostanziale ma si realizza mediante un procedimento inverso, che può dar luogo ad una serie di ingiunzioni emanate dal giudice internazionale: astenersi dall'introdurre o estendere le disposizioni che istituiscono cause di esclusione della responsabilità (quali cause di giustificazione e scusanti) o altre norme favorevoli al reo (come nel caso del riconoscimento di effetti retroattivi a norme modificative che determinano una depenalizzazione parziale)*". D. PULITANÒ, *Obblighi costituzionali di tutela penale cit.*, 484. C. PAONESSA, *Gli obblighi di tutela penale. La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari*, Pisa, ETS, 2009. C. SOTIS, *Obblighi comunitari di tutela e opzione penale: una dialettica perpetua?*, in *Riv.it.dir. e proc.pen.*, 2002, 173. V. VIGANÒ, *Obblighi convenzionali di tutela penale?*, in *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, a cura di Manes V. e Zagrebelsky V., Milano, Giuffrè, 2011, 243.

3. Il consenso come cardine del nuovo "ambiente giuridico". L'inglobamento in Rete del complesso delle relazioni private e istituzionali

Una prima puntualizzazione nei rapporti tra utente e Rete discende direttamente dalle opzioni di tutela individuate dalla Commissione Rodotà. Occorre preliminarmente stabilire una distinzione tra autonome sfere di tutela nella vita operativa di *Internet*: a) la tutela della struttura che garantisce la funzionalità dei *network*; b) la tutela dei diritti delle persone che assumono la qualifica di "utenti" per l'impiego che fanno della Rete e dei supporti informatici, indispensabili per gestire le informazioni in *Internet*[18].

A partire dall'art. 4 "*Tutela dei dati personali*" (non a caso si parla di materia ampiamente nota al Prof. Rodotà, ex Presidente dell'Autorità Garante del trattamento di dati personali) si pone l'accento sulla posizione giuridica soggettiva dell'utente e dei suoi dati identificativi, per poi passare con l'art. 6 "*Inviolabilità dei sistemi e domicili informatici*" a regolare le garanzie per i supporti tecnici e la intangibilità delle strutture di *software* e *hardware*.

Proprio il richiamo al Codice per il trattamento dei dati, D.lgs. n. 196/2003, pone al centro della vicenda giuridica dei diritti della Rete la manifestazione di volontà con cui un soggetto si determina a entrare in relazione con altri singoli o le Istituzioni che possono fare uso dei suoi dati personali, a patto che vi sia il consenso espresso dell'interessato[19]. Questo cardine su cui finisce per ruotare la relazione in Rete resta in realtà la migliore garanzia del fatto che il centro di interesse dell'ordinamento giuridico è e resta la persona, l'unica in grado di stabilire attraverso la liberta autodeterminazione se scambiare o acquisire informazioni in Rete. Per quanto poi concerne il consenso, in forma espressa, esso si desume dal fatto che la persona assume la qualifica di utente per essere entrato nella dinamica della Rete e in questo modo aver condiviso operatività e scambio di informazioni.

La relazione, dunque, nell'ambito della società informazionale è rappresentata dal potere di attivare e disattivare contatti, come opzione che non può tollerare condizionamenti o limitazioni, in quanto discendente dal cardine su cui ruotano i rapporti: il consenso dell'interessato. Diversamente dalla società corporea la struttura sociale di *Internet* non grava di alcun obbligo o dovere i suoi utenti, non a caso la gratuità della Rete assicura l'accesso incondizionato di chiunque secondo le regole della democrazia, salvo il caso in cui l'utente viola le regole di comportamento della compagine sociale.

Il libero consenso, essenzialmente fondato sull'incondizionata autodeterminazione a concedere l'uso dei propri dati, completa il quadro delle libertà fondamentali della persona-utente ma in modo tale che se l'assenza del consenso vale ad escluderlo, questo fatto però non è destinato a limita l'operatività di *Internet* che continua a trattare i flussi dei dati degli altri utenti, i quali, a loro volta, si siano resi disponibili al trattamento dei dati in Rete[20]. Ecco perché in un progetto organico di un quadro di tutela deve esistere la protezione differenziata della Rete rispetto a quella della persona-utente, perché si

[18] M. ATELLI, *Dal diritto ad essere lasciati soli al diritto ad essere lasciati in pace: la prospettiva del danno di petulanza*, in *Riv.crit.dir.priv.*, 1997.

[19] Ci sia consentito a tale proposito citare P. TRONCONE, *Il delitto di trattamento illecito dei dati personali*, Giappichelli, Torino, 2011.

[20] V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno e resp.*, 1998.

propone come estrinsecazione dei diritti di libertà fondamentali sanciti dalla Carta costituzionale.

La premessa di metodo e di valore crea i presupposti perché *Internet* possa incamerare tutto il complesso delle relazioni che s'instaurano tra singoli utenti o gruppi di utenti e poi tra utente e Istituzioni. In fondo l'ufficialità dell'importanza sociale della Rete nasce dal fatto che le Istituzioni abbandonano il metodo di lavoro tradizionale ed entrano in contatto con i cittadini attraverso l'operatività informatica. Questo capovolgimento sostituisce il mezzo di una relazione, quella utente-Istituzione, improntata da un lato a una prestazione di un servizio cui l'Istituzione è tenuta, dall'altro alla partecipazione democratica che il cittadino deve alle Istituzioni di appartenenza. Come si vede il discorso si sposta anche sul piano politico, poiché in fondo *Internet* sta inglobando al suo interno quelle relazioni che esprimono una scelta di indirizzo e un modo diverso di partecipare alla vita istituzionale e politica di un Paese.

Il problema della tutela dei dati, dunque, è il tema centrale nell'odierno dibattito che non può non riguardare l'uso e le molteplici forme di trattamento in Rete.

La prima delle questioni in materia di dati, infatti, riguarda la Direttiva del Parlamento europeo n. 2006/24/CE che consentiva la conservazione dei dati da parte degli operatori per finalità di giustizia e di repressione dei reati. La Corte di Giustizia dell'Unione europea di Lussemburgo in data 8 aprile 2014 ha invalidato la predetta Direttiva in considerazione della lesione del principio di proporzionalità, in quanto la conservazione dei dati, seppure destinata a ragioni di giustizia, non può essere tale da prevaricare il diritto alla vita privata e alla protezione dei dati personali[21].

La seconda questione, invece, ha avuto a oggetto il c.d. "diritto all'oblio", ossia la possibilità di procedere alla rimozione dei dati in Rete da parte degli operatori informatici, in particolare Google, quando sia trascorso un tempo sufficiente a garantire l'interesse pubblico alla notizia. La Corte di Giustizia in data 13 maggio 2014 ha stabilito che chiunque può obbligare il motore di ricerca che ha indicizzato quella informazione alla rimozione della notizia motivandone però il venir meno dell'interesse pubblico[22].

4. Un nuovo ruolo del diritto penale: verso la palinodìa o la negazione degli assetti tradizionali?

La piattaforma della Rete che s'intende proteggere come avamposto di tutela della persona umana appare oggi sostanzialmente caratterizzata come un nuovo diritto che emerge sempre più in maniera netta e autonoma, quello della libertà della Rete che, secondo alcuni studiosi, rappresenta la frontiera di un nuovo diritto di libertà costituzionale che addirittura si rende garante del principio di democrazia negli Stati moderni come un "diritto umano"[23].

[21] La decisione è della Corte di Giustizia dell'Unione Europea, 8 aprile 2014, (C-293/12, C-594/15), Digital Rights Ireland Ltd., par. 42-46, con nota di R. FLOR, *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 *www.penalecontemporano.it*, 28 aprile 2014.

[22] Corte di Giustizia UE, Sez. grande, sentenza 13 maggio 2014 n. C-131/12, in *www.altalex.it*.

[23] La designazione di libertà dell'accesso a Internet come appartenente alla categoria dei diritti umani è stata convincentemente sostenuta dal: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, in *Assemblea Generale dell'ONU*, redatto dal Frank La Rue (Commissario Speciale delle Nazioni Unite) e presentato al Consesso il 16 maggio

Ripetutamente è stato invocato -anche dall'ONU- un intervento a livello di legge fondamentale degli Stati, dove sia prevista e sancita l'importanza di *Internet* come un bene comune di assoluta rilevanza ordinamentale, che abilita all'esercizio degli altri diritti fondamentali[24].

Appare dunque chiaro che la centralità assunta dal sistema della Rete possa naturalmente elevarla a rango di bene giuridico di riferimento, cui il diritto penale, come per gli altri beni giuridici fondamentali, è chiamato a predisporre un adeguato e rigoroso sistema di tutele.

Non bisogna tuttavia trascurare che vi sono dei tratti genetici della Rete di comunicazione, su cui è costruita la realtà immateriale del *web*, che potrebbero mettere in crisi l'elaborazione di uno statuto penale di *Internet*, proprio perché la divaricazione dei settori operativi da tutelare, da un lato la struttura tecnologica e dall'altro i contenuti in Rete, determina la divaricazione dei modelli di tutela, distinti in oggetti fisici, informazioni e dati[25].

Il diritto penale classico legato al tema irrinunciabile del principio di legalità di delitti e pene e al sistema delle garanzie individuali può trovare adeguato spazio e un'azione efficace e non simbolica solo se non arretra rispetto all'esigenza di porre corrette condizioni a base del suo intervento. Occorre, dunque, una rifondazione del diritto penale per un nuovo campo che si propongono obiettivi divergenti da quelli statutari, dove l'impegno di criminalizzazione potrebbe entrare in tensione con il principio di legalità penale per effetto dei differenti e incoerenti interventi normativi, nazionali e sovranazionali.

Un nuovo sistema assiologico se vuole conservare indenne il complesso dei meccanismi di tutela fondato sulla rilevanza degli interessi da proteggere, secondo gli obblighi della teoria del bene giuridico, deve innanzitutto anteporre alla generalità degli interessi singolari quella della primaria tutela della Rete. Infatti, nella società contemporanea questo enorme spazio immateriale che si riempie di liberi contenuti deve essere prima di ogni altra cosa salvaguardato come un bene a sé stante, oltre che autonomamente rilevante.

La posta in gioco non è dunque l'importanza di ciascuno dei molteplici interessi coinvolti nella funzionalità del *web* ma è in primo luogo il *web* stesso a diventare il primitivo bene giuridico da sottoporre a rigorosa tutela.

Si potrebbe facilmente obiettare che questo modo di procedere in realtà è la manifestazione di una inaspettata *palinodìa* del diritto penale, qualcosa di già visto che viene considerato poco adattabile rispetto agli scopi che la tutela penale della Rete si propone. Un tentativo di rinunciare ai corollari della legalità penale che hanno caratterizzato la storia prima della dematerializzazione determinata dall'avvento di *Internet*.

2011. Del resto anche il progetto Rodotà all'art. 2 stabilisce, in perfetta simmetria concettuale, il diritto alla libera fruizione che si concretizza anche nella necessità che vengano rimossi gli ostacoli "di ordine economico sociale" che ne impediscono l'accesso.

[24] T.E. FROSINI, *Il diritto di accesso a Internet*, in *www.confronticostituzionali.eu*, 18 novembre 2013. G. DE MINICO, *Diritti Regole Internet*, in *www.costituzionalismo.it*, n. 2, 8 novembre 2011.

[25] Si veda a tale proposito il progressivo impianto di penalizzazione differenziata che riguarda la struttura tecnica e i contenuti della Rete a seguito della ratifica della *Convenzione di Budapest* del 23 novembre 2001, in AA.VV., *Le nuove leggi penali. Sistema penale e criminalità informatica*, a cura di Luparia L., Giuffrè, Milano, 2009.

Resta tuttavia fermo il fatto che il sistema normativo-prescrittivo attuale non viene distolto dall'assetto un diritto penale teleologicamente orientato dai principi espressi dalle Carte nazionali e ribaditi dalle Convenzioni continentali, basti pensare agli artt. 6 e 7 della CEDU. La materia punitiva resta comunque rigidamente ancorata al rispetto dei presidi di garanzia del singolo ordinamento giuridico e anche di quello relativo alla Rete globale, oggi in fase di progettazione, anzi quest'ultimo finisce per sovrapporsi anche se non aderisce appieno a quello tradizionale costituito da corporeità sociale e materialità delle condotte.

5. I problemi di certificazione di attendibilità delle informazioni nella Rete

Il mondo immateriale reca con sé un pregiudizio connaturato, secondo il quale, non esistendo un supporto materiale ma soltanto la creazione di una informazione immateriale, tutto può essere modificato e tutto può essere alterato anche per fini illeciti[26].

In questo modo l'universo di *Internet* rischia di vivere il permanente sospetto della formale inattendibilità delle informazioni che fluiscono in Rete. Si tratta di un pregiudizio di carattere culturale, ma quello da cui partire per capovolgere la prospettiva e riconoscere certezza alle informazioni e alle relazioni nella ragnatela di *Internet*[27].

Un ordinamento giuridico che voglia conferire legittimità istituzionale all'ambiente dei *network*, sotto il profilo pedagogico-educativo, deve formare gli utenti a convincersi della certezza e dell'attendibilità delle fonti e del fatto che la loro alterazione rende per loro stessi instabile la genuinità delle informazioni che normalmente recepiscono e utilizzano. Scoprire che l'autore di falsificazioni, per la fisiologia stessa della costituzione strutturale di *Internet*, è destinato a diventare automaticamente vittima di informazioni inattendibili, vuol dire introdurre elementi di discussione utili a destabilizzare possibili disegni alterativi.

Una sicura soluzione che ponga un limite ad abusi e che conferma il carattere consensuale della vita in Rete può essere individuata nella firma digitale e nella certificazione dell'identità con cui gli utenti escono dall'anonimato e partecipano, come soggetti liberamente autenticati, riconoscibili, tracciabili e rintracciabili, alla vita del mondo di *Internet*[28]. La identificabilità del soggetto fisico nel mondo dematerializzato stabilisce i contorni della *identità digitale* e rafforza il ruolo della *cittadinanza digitale*, una vera e propria qualificazione sociale dell'utente. Solo in questo modo l'integrità della realtà immateriale può essere difesa da una realtà artificiale -artatamente falsificata- nella quale possono essere introdotti fatti e atti non genuini[29].

---

[26] AA.VV., *Computer e diritto. L'informatica giuridica nella società dell'informazione e della conoscenza*, a cura di Florindi E., Giuffrè, Milano, 2012. G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, Utet, 1999.

[27] L. PICOTTI, *Problemi penalistici in tema di falsificazione di dati informatici*, in *Dir.informaz. e informatica*, 1985, 958. E ancora L. PICOTTI, *Problemi penalistici in tema di falsificazione di dati informatici*, in *Riflessioni ed esperienze sui profili oggettivi e soggettivi delle falsità documentali*, a cura di Ugo Dinacci-Angelo R. Latagliata-Marcello Mazza, Padova, Cedam, 1986, 91 e ss.

[28] Sul tema particolarmente interessante è la decisione di Cass. pen., Sez. V, 8 novembre 2007, n. 46674, in *Dir. informatica*, fasc. 4-5, 2008, 526, con nota di C. FLICK, *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona.*

[29] G. MARINI, *Condotte di alterazione del reale aventi ad oggetto nastri ed altri supporti magnetici e diritto penale,* in *Riv.it.dir. e proc.pen.*, 1986, 382.

La recente introduzione nel corpo del codice penale di una speciale aggravante all'art. 640-*ter* c.p. "*Frode informatica*" denominata indebito utilizzo d'identità digitale continua ad arricchire il quadro delle incriminazioni in materia senza però alcuna cautela di coerenza sistematica: "*la pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*"[30]. E che manchi una strategia unitaria è provata dalla scissione della condotta di utilizzo da quella di furto di identità[31].

6. Le linee sistematiche di una proposta cautelare e sanzionatoria per gli illeciti commessi in Rete. La responsabilità penale da ambiente informatico

La stessa Rete, come fatto connaturato al suo modo di essere, stabilisce i criteri selettivi dei possibili reati punibili, poichè vi sono categorie di reati, ad esempio contro la vita o l'incolumità individuale, che non possono trovare alcuna compatibilità con il mezzo informatico[32].

La Rete, in buona sostanza, qualifica *ab origine* le modalità della condotta che tipicizza il fatto, dove anche la violenza, la induzione o la minaccia acquistano tratti identificativi nuovi perchè di tipo immateriale.

Vi sono, infatti, categorie di reato che trovano in *Internet* la più congeniale forma di consumazione e tra questi i reati di opinione, quelli contro la reputazione e la dignità personale, i reati contro la libertà sessuale e contro i minori[33], i reati contro il patrimonio e soprattutto i reati di falso[34]. La categoria dei delitti contro la fede pubblica rappresenta, non a caso, quella più caratteristica e tipica perchè si nutre di quello scollamento esistente tra realtà concreta e realtà immateriale. I documenti informatici alterati attraverso condotte di falsificazione ne ricevono in questo modo, paradossalmente, una imprevista attendibilità, poichè un'ampia -ma falsa- cornice informativa della realtà immateriale conferisce loro una sicura ma solo apparente genuinità. Si tratta in questo modo di fatti da punire in maniera particolarmente severa e del resto l'art. 491-*bis* c.p. "*Falso documento informatico*" è orientato in questo senso e per la prima volta costruisce una fattispecie in perfetta aderenza con i caratteri della Rete[35]. Il problema è costituito dall'interrogativo se possa o meno esistere un "*diritto penale dell'informatica*" come sub-sistema normativo autonomo[36]. L'interrogativo resta

[30] G. MALGIERI, *La nuova fattispecie di 'indebito utilizzo d'identità digitale'*, in *www.penalecontemporaneo.it*, 22 ottobre 2014.

[31] G. ZICCARDI, voce *Furto d'identità*, in *Dig.disc.pen.*, a cura di A. GAITO, Torino, 2011, 253.

[32] C. SARZANA DI S. IPPOLITO, *Criminalità e tecnologia: il caso dei computer-crimes*, in *Rass. penit. e crimin.*, 1979, 53 e ss. A. ALESSANDRI, *Riflessi penalistici dell'innovazione tecnologica*, Giuffrè, Milano, 1984. L. PICOTTI, *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova, 2004.

[33] R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, in *www.penalecontemporano.it*, 20 settembre 2012.

[34] A. MANNA, *Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronico*, in *Dir.informaz. e informatica*, 2002, 955.

[35] Ci sia consentito citare P. TRONCONE, *La tutela penale del documento dematerializzato tra vicende novative e nuove aspirazioni sistematiche*, in *Riv.pen.*, 2008, 1277. Sul tema del documento informatico come fonte di prova processuale, si veda G. VERDE, *Per chiarezza di idee in tema di documentazione informatica*, in *Riv.dir.process.civ.*, 1990, 715.

[36] K. TIEDEMANN, *Criminalità da computer*, in *Pol. del dir.*, 1984, pag. 613 e da pag. 629 e ss. viene riportato un ampio corredo normativo costituito delle numerose fattispecie incriminatici esistenti nel sistema penale tedesco.

senza risposta ma la soluzione va trovata nel progetto di un nuovo ordinamento sociale e giuridico.

Il tema dello spazio fisico globale rimane centrale al tema, parcellizzato in Stati sovrani e ordinamenti autonomi in cui scorre la struttura fisica di comunicazione, cui si sovrappone in modo uniforme e compatto lo spazio immateriale costituito da *Internet*, un immenso mondo in cui la regolazione dei comportamenti è assolutamente libera e sciolta da vincoli che tuttavia deve fare i conti con la moltitudine di leggi sovrane vigenti negli spazi fisici che impongono, nella più ampia diversità, soluzioni, divieti, obblighi e differenziati strumenti regolativi dei conflitti[37].

Il vero problema è la ricerca del tipo della fonte normativa ossia una cornice prescrittiva di ordine generale che possa essere stabilita da una Convenzione o un Trattato internazionale, orientato a compiere una scelta di tipo strategico sul piano della regolazione giuridica della immensa Rete. Occorre sancire se a livello dei singoli Stati sovrani sia opportuno o meno stabilire una sincronia tra lo spazio di *Internet* e quello fisico e quali norme sostanziali e quali strumenti processuali possano essere adottati a livello locale; oppure sia necessaria una regolamentazione uniforme e coerente in tutta la Rete con norme di valore giuridico trans-nazionale.

Se il tema al centro del dibattito guarda a *Internet* come a una di quelle componenti appartenenti alla categoria dei "*beni comuni*" dell'umanità, indispensabili perchè fondativi e funzionali alla vita e al benessere della persona, ebbene occorre elaborare uno statuto giuridico e nell'ambito di questo uno statuto penale per predisporre strumenti di protezione e di tutela giudiziaria. Ipotesi di incriminazione particolarmente precise e coerenti nella puntualizzazione degli elementi di tipicità raccolti intorno a un interesse giuridico e strumenti di intervento repressivo che possano cogliere con immediatezza l'infrazione e dove si stabilisca in maniera chiara che le frontiere fisiche nazionali non garantiscono alcuna immunità. In realtà, perché *Internet* possa essere definito un bene comune e ricevere autonoma tutela, occorre che siano protette anche la struttura tecnica e la tecnologia che tengono in vita la Rete. L'assenza di supporti tecnologici oppure, in maniera equivalente, il danno cagionato alle strutture fisiche, rende irrimediabilmente vulnerabile il mondo immateriale dei *network*. A tale proposito occorre rilevare che il legislatore italiano, ma in realtà anche i sistemi legislativi degli altri paesi, hanno messo in campo norme penali dedicate precipuamente allo scopo, tra queste il danneggiamento informatico e l'accesso abusivo a un sistema informatico[38].

D'altra parte, sul fronte della prevenzione, occorre lasciare libera l'attività di indagine informatica senza filtri preventivi e con poteri di intervento di natura inibitoria e cautelare reale che possa consentire alla polizia giudiziaria di effettuare scambi di informazioni e richieste di intervento di tipo planetario, all'interno di tutta la Rete e per

[37] Una soluzione di tipo fondativo potrebbe essere costituita sulla base dell'art. 83 della Costituzione europea, in F. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *www.penalecontemporaneo.it*, 2014, 5: "*L'importanza di strumenti d'indagine quali le online searches è avvertita anche a livello di Unione Europea, sia ai fini della cooperazione giudiziaria, sia nel contesto delle nuove competenze penali ad essa attribuite col Trattato di Lisbona, tra cui rientra la criminalità informatica (art. 83 TFUE)*".

[38] Si veda Cass. pen., sez. V, ord. 11.2.2011 (dep. 23.3.2011), n. 11714, Pres. Calabrese, Est. Scalera, ric. Casani, con nota di A. SCIRÈ, *Abuso del titolo di legittimazione all'accesso ad un sistema informatico: alle SS.UU. la questione della configurabilità del delitto di cui all'art. 615 ter c.p.*, in *www.penalecontemporaneo.it*, 21 settembre 2011.

ciascun ramo di essa[39]. Uno degli interventi possibili potrebbe essere non solo il blocco del sistema informatico ma anche l'individuazione della stazione informatica da cui è partita l'attività illecita che potrebbe essere inibita anche in remoto.

Le buone pratiche (o buone prassi, *best practices)* possono essere uno dei veicoli per concepire una più adeguata tutela penale di *Internet* che non si fondino però su vincoli di carattere etico ma che propongano un'efficacia pressione sugli utenti, dissuasiva e tale da compromettere la loro futura reputazione in Rete. Una buona pratica potrebbe essere richiedere da parte del sito *Internet* il consenso preventivo all'uso di informazioni, precisandone la destinazione e le forme di trattamento, ma allo stesso tempo diffidare da comportamenti che potrebbero analiticamente essere elencati. Si potrebbe, ad esempio, richiedere uno specifico impegno all'impiego della Rete da un determinato domicilio informatico e utilizzare strumenti di inibizione informatica nel caso di violazione dell'impegno.

E' pur vero che la mancata identificabilità dell'utente o la creazione di elementi identificativi non veri potrebbe consentire una deroga alle restrizioni, ma resta il fatto che il principio di libertà della Rete e del *web* come bene giuridico primario non consente di andare oltre e invoca il principio di autoresponsabilità[40]. Occorre giungere al punto che lo stesso utente avverta il peso dell'esclusione dalla Rete e che, dunque, non consideri conveniente assumere comportamenti lesivi se vuole rimanere in navigazione. Questo sforzo implica che siano istituiti fin dalle scuole dell'obbligo dei corsi di alfabetizzazione e di educazione all'uso della Rete, alla corretta gestione di immagini e informazioni, calibrando il peso dell'importanza di accedere e fruire di *Internet* con le conseguenze sanzionatorie che ne limitino l'accesso, formulando in questo modo un modello educativo profilato appunto sul principio dell'autoresponsabilità[41].

Sul piano sanzionatorio occorrerebbe ipotizzare, infatti, misure punitive tipiche e specifiche per l'ambiente immateriale dei *network*, dove il ruolo che il diritto penale può giocare è quello di tipo persuasivo-pedagogico, piuttosto che punitivo ed estraniativo. La "reclusione informatica" o l'"ergastolo informatico", seppure forme punitive cui fare ricorso, non garantirebbero la comunità di *Internet* da successive incursioni. Molto più efficace, invece, potrebbero essere quelle iniziative repressive messe in campo dalla stessa comunità digitale degli utenti che respingono il dialogo e lo scambio di dati con il dichiarato responsabile di precedenti illeciti. Ad esempio, la categoria dei "*troll*", molestatori informatici che in Gran Bretagna sono puniti con una sanzione detentiva fino a sei mesi e che il Governo inglese propone di aumentare fino a due anni di reclusione sono il tipico esempio di punizione fondata sulla sicura individuazione del responsabile[42].

---

[39] Sulle perquisizioni *on-line* si veda S. MARCOLINI, *Le cosiddette perquisizioni online (o perquisizioni elettroniche)*, in *Cass.pen.*, 2010, 2855; e ancora F. IOVENE, *Le c.d. perquisizioni online cit.*, 1.

[40] H. JONAS, *Il principio responsabilità. Un'etica per la civiltà tecnologica*, Einaudi, Torino, 2006, 210 e ss.

[41] Molto interessante è l'esperienza sul campo riportata in AA.VV., *Educare alla cittadinanza digitale. Per un utilizzo attivo dei media, a scuola e nel territorio*, a cura di A. Membretti, Ibis, Pavia, 2010. L. CAMERON-CURRY - M. POZZI - S. TROIA, *Educare alla cittadinanza digitale. Un viaggio dall'analogico al digitale e ritorno*, Tangram Edizioni Scientifiche, Trento, 2014.

[42] Notizia apparsa sul *Corriere della sera* del giorno 19 ottobre 2014.

Il diritto penale della persuasione potrebbe giocare un ruolo importante in questo caso, un ruolo di tipo preventivo-pedagogico quando gli utenti allontanano il soggetto che molesta e di tipo repressivo-rieducativo quando esista la possibilità di individuare attraverso i nodi della Rete e il singolo *provider* il punto di trasmissione dei flussi di dati molesti.

Ormai la tecnologia può mettere in campo risorse importanti al servizio delle investigazioni informatiche e formare la piattaforma probatoria degli strumenti processuali per intervenire alla consumazione di reati commessi con la Rete. La tecnica di individuazione attraverso i "*cookies*", ad esempio, può rivelarsi determinante in quanto i *cookies* sono marcatori digitali che si ritrovano dell'*hard disk* dei *computer* da cui partono i dati[43]. Una volta individuato con certezza il mezzo potrà scattare una misura cautelare di tipo probatorio per accertare la responsabilità penale dell'utente.

Altro punto molto importante riguarda la tenuta dei principi di garanzia fondamentali della materia punitiva e in particolare il principio di colpevolezza per il fatto illecito consumato in ambiente informatico.

In questo senso molta attenzione dovrebbe essere dedicata, proprio in chiave pedagogica, prima di tutto allo *standard* di alfabetizzazione dell'utente sospetto, perché si abbia la prova della piena consapevolezza dell'illecito commesso. Un ruolo importante potrebbe giocarlo la tecnica di elaborazione delle singole figure di reato, allestite secondo modalità di condotta facilmente riconoscibili nella descrizione astratta dei comportamenti vietati, evitando di ricorrere a ipotesi generali e indeterminate o a formulazioni di tipo casistico. E anche a questo punto si pone il problema del formante normativo da cui genera la disciplina penale.

Una possibile ipotesi potrebbe essere l'elaborazione di una coerente e completa codificazione che avvenga con un Testo Unico così com'è accaduto per il trattamento dei dati. Un corpo unico fondato sulla interrelazione normativa, calibrata ed esauriente, che conferisca coerenza sistematica alla materia e che tragga l'orientamento dai principi generali e costitutivi sanciti da una Carta fondamentale o da un Trattato internazionale.

[43] M. CASTELLS, *Galassia internet cit.*, 164.

LA GIUSTIZIA PENALE NELLA RETE? TUTELA DELLA RISERVATEZZA *VERSUS* INTERESSE ALL'ACCERTAMENTO E ALLA PREVENZIONE DEI REATI NELLA RECENTE GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

Roberto Flor

1. Introduzione

Il *cyberspace* viene oggi descritto come un "*wild west*" della globalizzazione del crimine [1]. Ad esso vengono legate diverse espressioni metaforiche, non tutte immediatamente comprensibili, quali: "tecnologia veloce dei flussi informativi globali" e delle "traslazioni" "uomo-macchina" attraverso la rete; "sfera di iper-mobilità che riflette la pace globale della iper-modernità"; tecnologia "*open-ended*", decentralizzata e non gerarchica; "connessione con la realtà virtuale"; "topografia" virtuale creata dalla rete quale sistema di interattività e multimedialità. Esse evocano, però, il superamento della concezione meramente "tecnica" di Internet e del *cyberspace* - ossia quali reti o spazi globali di interconnessione di *computers* - per abbracciare una dimensione sociologica, basata sulla loro forza riconfigurativa della società e delle esperienze personali degli utenti, influenzate in modo determinante dai nuovi modi di comunicazione dinamica, transnazionale ed interattiva[2].

Oggi il *cyberspace* costituisce uno spazio virtuale in continua evoluzione che consente non solo la delocalizzazione delle risorse, anche grazie alle nuova dimensione

[1] Vedi B. SANDYWELL, *On the globalisation of crime: the Internet and new criminality*, in Y. JEWKES, M. YAR, *Handbook of Internet Crime*, Willan Publishing, 2010, 38 e ss. Cfr., inoltre, R. FLOR, *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 L. CAMALDO (cur.), *La circolazione e il contrabbando di prodotti contraffatti o pericolosi. La tutela degli interessi finanziari dell'Unione Europea e la protezione dei consumatori* , Torino , G. Giappichelli - Torino , 2013 , 118 - 178

[2] Cfr. T. JORDAN, *Cyberpower: A Sociology and Politics of Cyberspace and the Internet*, Londra, 1998; D. Lyon, *The Electronic Eye: The Rise of Surveillance Society*, Cambridge, 1994; B. SANDYWELL, *Monsters in Cyberspace: Cyberphobia and Cultural Panic in the Information Age*, in *Inf. Com. Soc*., 9, 1, 39-61. Alcuni Autori parlano di effettivo impatto sociale del *cyberspace*: vedi D.S. WALL, *Cybercrimes: New Wine, no Bottles*?, ora in D. S. WALL, *Cyberspace Crime*, Ashgate Publishing, 2003, 3 e ss. Sugli elementi specializzanti del *cyberspace* rispetto al mondo fisico vedi C. REED, *Making Laws for Cyberspace*, Oxford, 2012, 25 e ss.

del *cloud*[3] e della "struttura" del *web*, ma altresì la detemporalizzazione delle attività, che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente, che fanno venire meno l'esigenza di un "collegamento" o "contatto" fisico fra persona e sistema informatico.

"Smaterializzazione" e "velocizzazione" coinvolgono, dunque, anche le condotte concrete, che prescindono o si distanziano dalla fisicità dei comportamenti o dei fatti esteriori capaci di "incorporare" l'accadimento materiale (il danno o il pericolo concreto)[4].

L'innovazione-rivoluzione tecnologica offre però anche nuovi strumenti e mezzi per la ricerca delle prove, e consente di perseguire altresì fini "preventivi". La concreta esigenza di misure efficaci di contrasto a gravi forme di criminalità vale anche rispetto a reati "tradizionali", che trovano nelle nuove tecnologie un essenziale ausilio per la loro realizzazione. Si pensi solo alle attività preparatorie di attentati terroristici, che possono trovare in Internet un formidabile mezzo di comunicazione e di pianificazione degli attacchi, oppure alla lotta contro la diffusione di materiale pedopornografico *online*.

In questo contesto la sentenza del 13 maggio 2014 della Corte di Giustizia sul c.d. caso Google/Spagna è immediatamente passata alle cronache come la decisione che ha riconosciuto il c.d. "diritto all'oblio"[5].

In verità la controversia, sul piano sociale prima ancora che su quello del diritto penale sostanziale, e rilevante per tutto il sistema di giustizia penale, risulta essere più complessa, in quanto coinvolge questioni attinenti non solo ai possibili profili di responsabilità del fornitore di un servizio nella società dell'informazione e di Internet, ai limiti degli "ordini" delle "autorità competenti" di rimozione di dati e informazioni per la tutela della riservatezza in rapporto al bilanciamento con gli altri diritti fondamentali coinvolti ed il perseguimento di interessi di rilevanza collettiva, ma anche ai profili distopici che talvolta si vogliono attribuire a Internet, proprio quale *"wild west*" della globalizzazione del crimine, portato a estremi apocalittici.

Non è certo la prima volta che la Corte di Giustizia ha dovuto affrontare problematiche riguardanti proprio il bilanciamento fra le diverse esigenze, da un lato, di tutela dei diritti fondamentali e, dall'altro, di accertamento e prevenzione di attività illecite e di reati[6]. Pur trattandosi, in questi ultimi casi, di questioni pregiudiziali sull'interpretazione delle direttive 2000/31/CE sul commercio elettronico, 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, 2004/48/CE sul rispetto dei diritti di proprietà intellettuale,

[3] La nozione di *cloud computing* allude ad un insieme di tecnologie che permettono di memorizzare, archiviare e/o elaborare dati grazie all'utilizzo di risorse hardware/software delocalizzate in rete. Cfr., per una spiegazione tecnica, B. FURHT, A. ESCALANTE, *Handbook of Cloud Computing*, Lexis Nexis, 2010.

[4] Cfr. quanto già evidenziato da L. PICOTTI, *Sicurezza, informatica e diritto penale*, in M. DONINI, M. PAVARINI (cur.), *Sicurezza e diritto penale*, Bologna, 2011, 217 e ss., 223-224.

[5] Corte di Giustizia dell'Unione europea, sent. 13 maggio 2014 (C-131/12). Per i primi commenti si rinvia a B. VAN ALSENOY, A. KUCZERAWY AND J. AUSLOOS, *Search engines after Google Spain: internet@liberty or privacy@peril?*, in ICRI, 15/2013, 1-74; G. FINOCCHIARO, *Editoriale*, in *Giustizia civile.com*, 2014, 3 e ss.; A. PALMIERI, R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro Italiano*, 1, 2014, 1-16.

[6] Vedi, ad esempio, Corte di Giustizia dell'Unione europea, sent. 24 novembre 2011 (C-70/10) e 16 febbraio 2012 (C -360/10), nonché, in termini parzialmente diversi, Corte di Giustizia dell'Unione europea, sent. 27 marzo 2014 (C-314/12). Cfr. ampiamente R. FLOR, *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*?, in *Dir. inf*., 2014, 775 – 803.

95/46/CE sul trattamento dei dati personali e 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, esse hanno, di fatto, posto in discussione l'uso di taluni mezzi tecnologici "invasivi" rispetto alla tutela dei diritti fondamentali, ferma restando la validità degli atti europei.

Con la sentenza del 13 maggio 2014 (c.d. caso Google/Spagna), invece, la Corte di Giustizia ha affermato la prevalenza dei diritti tutelati dagli artt. 7 e 8 della Carta, in determinate condizioni, rispetto alla libertà di espressione e agli interessi economici dei *providers,* rafforzando in questo modo la posizione giuridica della persona interessata da un trattamento di dati personali, benchè non sia pacifico poter ricavare dalle norme della direttiva 95/46, intepretate alla luce delle disposizioni dalla Carta, un diritto "generalizzato" all'oblio.[7]

Questa sentenza giunge dopo un'altra importante decisione (c.d. caso *data retention*) [8], in cui i Giudici di Lussemburgo hanno affrontato per la prima volta la delicata questione concernente il bilanciamento fra le esigenze di repressione ed accertamento dei reati e la tutela dei diritti fondamentali dell'individuo, che possono essere fortemente limitati dagli obblighi di conservazione dei dati di traffico telefonico e telematico nella società informazione, annullando la direttiva 2006/24 perché contraria agli artt. *7,* 8 e 11 della Carta dei diritti fondamentali dell'Unione europea. In quest'ultima sentenza la Corte ha esaminato gli obblighi di conservazione dei dati nell'UE alla luce dei principi di necessità e proporzionalità, tenuto conto e nell'interesse della sicurezza nazionale, del buon funzionamento del mercato interno e del rafforzamento del rispetto della vita privata, nonché del diritto fondamentale alla protezione dei dati personali, fornendo alcune linee guida essenziali, che si inseriscono inevitabilmente nel contesto più ampio della riforma in atto, a livello europeo, di tutta la disciplina in materia di tutela della *privacy,* attraverso un *corpus* unico di norme[9].

Queste ultime due decisioni, in particolare, se da un lato rafforzano la tutela della riservatezza, dall'altro segnano uno strappo epocale nell'odierna società di Internet, ponendo dei limiti decisi all'uso delle tecnologie e della rete, che non sempre possono produrre effetti positivi rispetto alla tutela di rilevanti contro interessi di natura generale e collettiva.

2. Le principali linee argomentative della Corte di Giustizia nel caso Google/Spagna

In estrema sintesi, nel c.d. caso Google/Spagna[10] la Corte ha affermato che l'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di

[7] Vedi, in questo senso, le conclusioni dell'Avvocato Generale Niilo Jääskinen presentate il 25 giugno 2013.

[8] Vedi Corte di Giustizia dell'Unione europea, sent. 8 aprile 2014 (C-293/12 e C-594/12), con primo commento di R. FLOR, *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 http://www.penalecontemporaneo.it/upload/1398628841FLOR_2014.pdf, a cui si rinvia per gli ulteriori riferimenti bibliografici. Cfr. anche E. COLOMBO, Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE, in Cass. pen., 7/8, 2014, 2705 e ss.

[9] Si fa riferimento alle concrete iniziative europee. In questa sede basti il rinvio a: http://ec.europa.eu/justice/data-protection/index_en.htm

[10] Per una descrizione dei fatti all'origine della sentenza si veda R. FLOR, *Dalla data retention al diritto all'oblio,* cit.

applicazione degli artt. 12, lett. b), e 14, co. 1, lett. a), della direttiva 95/46, possono ordinare al gestore del servizio (Google) di cancellare, dall'elenco di risultati che appare a seguito di una ricerca, i *link* verso pagine *web* pubblicate da terzi (nel caso di specie in una testata giornalistica *online*) e contenenti informazioni relative a una persona. Il fornitore del servizio è obbligato, inoltre, a sopprimere gli stessi *link* anche nel caso in cui il nome o le informazioni non vengano previamente o simultaneamente cancellati dalle pagine *web* del quotidiano, eventualmente quando la loro pubblicazione sia altresì di per sé lecita. Sulla base dell'interpretazione di tali prescrizioni, dettate dall'art. 6, co. 1, lett. da c) a e), direttiva 95/46, un trattamento di dati inizialmente lecito potrebbe divenire, con il tempo, incompatibile con la direttiva, qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura, in particolare, nel caso in cui i dati risultino inadeguati, non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità e al medesimo tempo trascorso. E'agevole notare che, secondo la Corte, i diritti fondamentali di cui agli artt. 7 e 8 della Carta prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico degli utenti a trovare l'informazione in occasione di una ricerca *online* relativa ad una persona determinata. Ferme restando, secondo i Giudici, le eccezioni legate, ad esempio, al ruolo ricoperto da tale persona nella vita pubblica, che potrebbe giustificare la prevalenza dell'interesse degli utenti ad avere accesso all'informazione[11].

Le motivazioni della sentenza muovono, anzitutto, dalle definizioni di "trattamento" di dati e di "responsabile del trattamento" (o, meglio, "titolare del trattamento"), così come previste dalla direttiva.

La prima, ex art. 2, lett. b), è estremamente ampia e fa riferimento a qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di 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.

La Corte ha già avuto modo di affrontare la questione e ha concluso che l'operazione consistente nel far comparire su una pagina Internet dati personali deve essere considerata un «trattamento»[12].

Nel c.d. caso Google/Spagna sono presenti anche informazioni riguardanti persone fisiche identificate o identificabili, e dunque «dati personali» . Di conseguenza l'uso della rete e di un motore di ricerca comporta che il gestore di questo ultimo «raccoglie» , «estrae», «registra» e «organizza» tramite i suoi programmi di indicizzazione, «conserva» e, eventualmente, «comunica» e «mette a disposizione» dei propri utenti tali dati e informazioni, essendo indifferente che essi non vengano modificati dal motore di ricerca o vengano elaborati in modo automatizzato dai softwares o dagli applicativi.

Quanto alla questione se il gestore di un motore di ricerca debba essere considerato «responsabile del trattamento» dei dati personali appare decisivo il fatto che egli stesso a determina le finalità e gli strumenti della sua attività e, dunque, del trattamento di dati

[11] Per quanto riguarda la situazione italiana *in subiecta materia* basti il rinvio al recente provvedimento del Garante Privacy, 10 luglio 2014, n. 353.

[12] Si veda caso Lindqvist (C-101/01, EU:C:2003:596, punto 25)

personali che effettua. Pertanto può essere considerato senza dubbio un «responsabile» (o, meglio, titolare - *controller*) ex art. 2, lett. d), della direttiva.

Il trattamento di dati personali effettuato nell'ambito dell'attività di un motore di ricerca, ad ogni modo, si distingue nettamente da quello effettuato dai gestori di siti o dagli editori di *web-sites* o testate giornalistiche *online*.

Il primo, infatti, scansiona e organizza le informazioni tramite procedimenti di indicizzazione, rinviando a pagine *web* o a contenuti presenti nella rete. Si tratta di un'attività che può essere oggetto di limitazioni da parte dei gestori dei siti, dei *social media* o dei *social network*s nonché, in alcuni casi, da parte degli utenti stessi, i quali possono richiedere di essere esclusi in tutto o in parte dagli indici automatici.

Rimane però fermo un dato oggettivo, ossia che le finalità e gli strumenti anche di tale trattamento sono determinati dal gestore del motore di ricerca.

In sintesi, dunque, ex art. 2, lett. b) e d) della direttiva 95/46, da un lato, l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», se tali informazioni contengano dati personali, e, dall'altro lato, il gestore del motore di ricerca deve essere considerato «responsabile» ("titolare") del trattamento.

Ne consegue logicamente che tale trattamento di dati effettuato per le esigenze del funzionamento del motore di ricerca non è sottratto agli obblighi e alle garanzie previsti dalla direttiva per la tutela delle libertà e dei diritti fondamentali delle persone fisiche, in particolare del diritto al rispetto della vita privata e dei dati personali (ex artt. 7 e 8 della Carta)[13].

Per quanto riguarda il trattamento di dati effettuato da Google, l'art. 7, lett. f), della direttiva 95/46, richiede di operare un bilanciamento di interessi fra i diritti coinvolti, consendo il trattamento dei dati se risulta essere necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del terzo o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, la quale può opporsi per motivi legittimi al trattamento dei dati che la riguardano, ex art. 14, co. 1, lett. a) della direttiva.

Tale diritto può essere esercitato direttamente nei confronti del titolare del trattamento, oppure attraverso il ricorso all'autorità di controllo o all'autorità giudiziaria (artt. 12, lett. b), e 14, co. 1, lett. a) della direttiva 95/46)

Considerata la potenziale gravità dell'ingerenza nell'area di "riservatezza" pertinente alla persona, il trattamento dei dati da parte del gestore di un motore di ricerca non può essere giustificato solo sulla base di interessi di natura economica.

E' vero, come affermano i Giudici, che la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a

[13] Questo ultimo prevede che i dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. In tal senso gli Stati membri devono garantire a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento, a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non sia conforme alle disposizioni della direttiva.

quest'ultima. E' però altresì vero che sia la direttiva, che la Carta esigono che venga effettuato un corretto bilanciamento tra tale interesse e i diritti fondamentali della persona di cui agli artt. 7 e 8 della stessa Carta.

Il trattamento dei dati effettuato dal gestore del motore di ricerca si aggiunge a quello effettuato dagli editori di siti web, distinguendosi allo stesso tempo.

Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli artt. 12, lett. b), e 14, co. 1, lett. a), della direttiva contro il gestore del motore di ricerca, ma non contro l'editore della pagina web, che potrebbe aver trattato i dati «esclusivamente a scopi giornalistici».

Sulla base di queste principali argomentazioni i Giudici hanno ritenuto che nel c.d. caso Google/Spagna non sussistessero ragioni per affermare come preponderante l'interesse del pubblico ad avere accesso, nel contesto di una ricerca *online*, alle informazioni personali, ritenendo prevalenti i diritti di cui agli artt. 7 e 8 della Carta, anche rispetto all'interesse economico del gestore del motore di ricerca, purchè vi sia una verifica inerente al diritto dell'interessato, che potrebbe essere sacrificato nel caso in cui sussitano ragioni particolari (come il ruolo ricoperto nella vita pubblica) che giustifichino l'ingerenza nei suoi diritti fondamentali per la sussistenza di un interesse preponderante del pubblico ad ottenere l'informazione.

3. La sentenza della Corte di Giustizia sulla c.d. *data retention*: un importante passo per il rafforzamento del diritto alla riservatezza. Ma con quali effetti per il sistema di giustizia penale?

In questo già articolato contesto la sentenza della Corte di Giustizia sulla c.d. *data retention* ha notevolmente complicato la situazione[14].

I Giudici, infatti, hanno invalidato la direttiva 2006/24, in quanto non compatibile con i limiti imposti dal rispetto del principio di proporzionalità, alla luce degli artt. 7, 8 e 52, par. 1, della Carta.

Tale direttiva richiedeva l'applicazione degli obblighi di conservazione a tutti i dati di traffico connessi a qualsiasi mezzo comunicativo. Questi obblighi riguardavano, dunque, l'archiviazione di dati relativi, in modo generalizzato, a tutti gli utenti e a tutti i mezzi di comunicazione elettronica, così come a tutte le modalità di traffico delle informazioni (via telefono, Internet, e-mail ecc.) senza differenziazioni, limiti o eccezioni rispetto all'obiettivo di contrastare la criminalità grave. Inoltre, tale archiviazione aveva ad oggetto dati di persone che, nemmeno indirettamente, si trovavano nella situazione di dare adito a procedimenti penali o di essere collegate, anche solo in modo remoto, a reati gravi, anche in situazioni in cui non sussistevano prove che la loro condotta potesse in qualche modo far sospettare un loro coinvolgimento. Inoltre essa non prevedeva alcuna eccezione, con la conseguenza che si trovava ad essere applicata anche alle persone le cui comunicazioni erano soggette, in base alle norme di diritto nazionale, all'obbligo del segreto professionale.

[14] Corte di Giustizia dell'Unione europea, sent. 8 aprile 2014 (C-293/12 and C-594/12), con commento di R. FLOR, *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 *Dir. pen. cont*., 28 aprile 2014, 1-16, a cui si rinvia per l'approfondimento delle argomentazioni della Corte. Cfr., con riferimento agli effetti sia a livello europeo che nel sistema tedesco, S. NELLES, *Quo vadis Vorratsdatenspeicherung*?, Göttingen, 2014.

La direttiva non prevedeva nemmeno alcun rapporto tra i dati oggetto dell'obbligo di conservazione e una minaccia per la sicurezza pubblica. In particolare, tale obbligo non era limitato a: a) dati relativi a un determinato periodo di tempo e/o una particolare zona geografica e/o ad un cerchio di persone che potevano essere coinvolte, in un modo o nell'altro, in un crimine grave; b) a persone che potevano, per altri motivi, contribuire, grazie alla conservazione dei loro dati, alla prevenzione, accertamento e perseguimento di reati gravi.

La direttiva non prevedeva nemmeno alcun limite oggettivo, sostanziale o procedurale[15], per l'accesso ai dati da parte delle competenti autorità nazionali e per il successivo utilizzo a fini di prevenzione, accertamento [o nell'ambito di procedimenti penali] riguardanti reati che, in considerazione della portata e della invasività della interferenza con i diritti fondamentali di cui agli artt. 7 e 8 della Carta, fossero di una gravità tale da giustificare una limitazione a questi diritti. Al contrario, la direttiva faceva riferimento in modo generale, ex art. 1, par. 1, a «reati gravi» come «definiti dagli Stati membri», e non prevedeva che l'accesso ai dati avvenisse dopo l'esame di un giudice o di una autorità amministrativa indipendente, la cui decisione potesse, a seguito di una richiesta motivata presentata nel quadro delle procedure di prevenzione o accertamento di gravi reati, o nell'ambito di procedimenti penali, limitare l'accesso ai dati e il loro utilizzo a quanto fosse strettamente necessario ai fini del raggiungimento dell'obiettivo perseguito.

Per quanto riguarda il periodo di archiviazione dei dati, la direttiva faceva riferimento ad un lasso di tempo minimo (6 mesi) e massimo (24 mesi) senza distinguere le categorie di dati e la loro possibile utilità per il raggiungimento degli obiettivi perseguiti, ovvero in accordo con le persone coinvolte. Inoltre, il "periodo finestra" non era basato su criteri oggettivi al fine di assicurare che fosse limitato alla stretta necessità. Ne consegue che l'interferenza con i diritti fondamentali in esame avveniva senza limiti o regole precise.

Con riferimento alla sicurezza ed alla protezione dei dati oggetto dell'obbligo di archiviazione, la direttiva non prevedeva misure di garanzia sufficienti – come richieste, invece, dagli artt. 7 e 8 della Carta – in specie contro il rischio di abusi, accesso illegale o uso non autorizzato, nonchè in relazione alla molteplicità e diversità di dati che dovevano essere archiviati, alla natura dei medesimi ed ai rischi connessi alla loro integrità, confidenzialità e genuinità. La direttiva, inoltre, non prevedeva l'obbligo per gli Stati membri di disciplinare elevati standard di sicurezza, permettendo in tal modo ai *providers* di poter seguire criteri di mera economicità per assicurare la protezione delle informazioni[16]. Infine, la direttiva non richiedeva che i dati in questione dovessero essere conservati all'interno dell'Unione europea, con la conseguenza che non era possibile ritenere che il controllo, espressamente richiesto dall'art. 8, par. 3 della Carta,

[15] L'art. 4 della direttiva, infatti, lascia agli Stati membri il compito di definire le regole procedurali da seguire e i requisiti sostanziali per garantire l'accesso e la comunicazione dei dati.

[16] Il c.d. "criterio di economicità" era già stato evidenziato, in senso critico, dalla Corte costituzionale tedesca nella citata sentenza del 2 marzo 2010 sulla *data retention* (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), *on-line* in http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html Per un primo commento in italiano si consenta il rinvio a R. FLOR, *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*, 11, 2 , 2010 , 359-392. Nella letteratura tedesca vedi S. NELLES, *Quo vadis Vorratsdatenspeicherung*?, cit., 265 e ss.

da parte di un'autorità indipendente in conformità con le esigenze di tutela e sicurezza dei dati, fosse pienamente garantito.

Leggendo a contrario questa sentenza è possibile ricavare alcune linee guida per una riforma della normativa sulla c.d. *data retention*.

Ferme le delicate questioni sui limiti temporali della conservazione dei dati e sulle procedure di accesso e di acquisizione delle informazioni, le criticità principali riguardano, *in primis*, l'individuazione dei "gravi" reati "presupposto", nonché la definizione dei presupposti oggettivi che possano giustificare la *data retention.* In secondo luogo, la valutazione sull'esistenza di un *fumus commissi delicti* dovrebbe essere lasciata ad un organismo indipendente (giudice) attraverso la previsione di una procedura snella e "tempestiva", che consenta comunque un accertamento concreto sulla sussistenza del reato "presupposto", basato su elementi indiziari (provvedimento motivato dell'autorità giudiziaria su richiesta del pubblico ministero, anche su istanza del difensore dell'imputato), che può pervenire *ex post*, in un lasso di tempo comunqe breve, esclusivamente in ipotesi di urgenza (ad esempio quando sussistono elementi oggettivi e concordanti relativi alla preparazione di attentati terroristici), purchè vi sia una definizione: a) di un elevato livello delle "misure di sicurezza" da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento; b) di apposite sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito o in caso di mancato rispetto del "principio di necessità" nel trattamento dei dati (ad esempio quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato o le persone a lui collegate solo in caso di indispensabilità).

Nel caso in cui le norme interne dei singoli Stati, come nel caso italiano, non rispettino gli standard ricavabili dalla sentenza della Corte, esse dovrebbero essere disapplicate per contrasto con il diritto europeo.

La soluzione più immediata, ma purtroppo ad effetto "locale", vede come protagonista il legislatore nazionale, il quale dovrebbe intervenire ed adattare l'attuale disciplina agli standards elaborati dalla Corte di Giustizia.

Sarebbe però maggiormente auspicabile un intervento del legislatore europeo, nell'ambito di una più ampia politica criminale dell'Unione. La stessa individuazione dei fenomeni criminali gravi e di natura transnazionale, nonché la conseguente definizione dei "reati presupposto", potrebbe trovare una base legale nell'art. 83, par. 1, del Trattato sul funzionamento dell'Unione europea (TFUE).

Il *valore aggiunto* riguarda, da un lato, l'efficacia, per la forza vincolante delle fonti per gli Stati membri; dall'altro lato le *garanzie,* che devono circondare la produzione di norme penali (legittimazione democratica e trasparenza del procedimento legislativo, controllabilita` politica, da parte dei Parlamenti nazionali durante la fase « ascendente » dei fondamentali principi di sussidiarieta` europea e di proporzionalita`, ex art. 5 TUE e Protocollo applicativo n. 2 allegato al TFUE, piena controllabilita` giudiziaria di tali presupposti da parte della Corte di Giustizia ed, indirettamente, delle giurisdizioni nazionali nella fase applicativa).

L'epocale sentenza della Corte di Giustizia, di cui si condivide l'iter argomentativo e motivazionale, che fonda le proprie basi nel percorso già intrapreso da numerose Corti

costituzionali europee [17] , si scontra con la complessità dell'attuale società dell'informazione, governata dalla inarrestabile rivoluzione informatica e dalla esasperata velocità evolutiva delle tecnologie, che hanno trasformato i dati e le informazioni in "beni immateriali" di inestimabile valore.

Nell'attuale assetto sociale ed economico il ricorso a strumenti investigativi a "contenuto tecnologico" e alla *data retention* risulta indispensabile, per prevenire e per accertare gravi reati lesivi di importanti beni giuridici[18].

Nella delicata operazione di bilanciamento fre le contrapposte esigenze di tutela, il c.d. "diritto all'oblio", afferente alle prerogative della sfera di riservatezza della peronsa, deve essere considerato proprio rispetto all'interesse generale dell'accertamento e prevenzione di gravi reati.

I principi espressi dalle sentenze della Corte di Giustizia sui casi c.d. data retention e Google/Spagna, devono essere letti congiuntamente per tentare di elaborare una griglia di standards minimi per consentire tale giudizio di bilanciamento e per definire i contorni dei possibili limiti al diritto del soggetto interessato di ottenere la cancellazione dei dati e delle informazioni che lo riguardano anche da motori di ricerca.

4. Verso una definizione del "diritto all'oblio"

4.1. Il diritto all'oblio nelle conclusioni dell'Avvocato Generale

La ricostruzione del "diritto all'oblio" effettuata dalla Corte di Giustizia nella sentenza Google/Spagna in parte contrasta con le conclusioni dell'avvocato generale, il quale ha affermato, sulla base di specifiche argomentazioni, che non possa ritenersi pacifico poter ricavare dalle norme della direttiva 95/46 (direttiva), intepretate alla luce delle disposizioni dalla Carta, un diritto "generalizzato" all'oblio.[19]

Secondo l'avvocato generale, infatti, *i diritti alla rettifica, alla cancellazione, al congelamento e all'opposizione previsti nella direttiva non corrispondano al «diritto all'oblio» della persona interessata*

In particolare la direttiva non prevederebbe un diritto generale di questo che possa permettere al soggetto interessato di limitare o di impedire la diffusione di dati personali che egli consideri compromettenti o contrari ai propri interessi.

I criteri da applicare dovrebbero invece essere individuati nello scopo del trattamento e negli interessi da questo tutelati, bilanciati con quelli della persona interessata, e non invece con le preferenze di quest'ultima. Pertanto, una preferenza soggettiva non

[17] Vedi R. FLOR, *La Corte di Giustizia*, cit., 1-16.

[18] Gli stessi Stati membri, in generale, hanno affermato che la conservazione dei dati è «quanto meno utile, e in alcuni casi indispensabile, per prevenire e contrastare la criminalità, compresa la protezione delle vittime e l'assoluzione degli imputati innocenti». La Repubblica ceca, ad esempio, ha considerato la conservazione dei dati «assolutamente indispensabile in un gran numero di casi»; la Slovenia ha indicato che l'assenza di dati conservati «paralizzerebbe l'attività delle agenzie di contrasto»; l'Ungheria ha affermato che era «indispensabile nelle attività ordinarie [delle agenzie di contrasto]»; il Regno Unito ha descritto la disponibilità di dati relativi al traffico come «assolutamente essenziale … per condurre indagini riguardanti il terrorismo e i reati gravi». Vedi in questo senso il rapporto della Commissione europea relativo alla "Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24)", COM(2011) 225 definitivo, 25, nota 105.

[19] Vedi, in questo senso, le conclusioni dell'Avvocato Generale Niilo Jääskinen presentate il 25 giugno 2013.

dovrebbe costituire un motivo preminente e legittimo ai sensi dell'articolo 14, lett. a), della direttiva 95/46.

Anche se il gestore del motore di ricerca è riconducibile alla categoria dei «responsabili del trattamento» (o, meglio, titolare/*controller*), la persona interessata non avrebbe in ogni caso un «diritto all'oblio» assoluto da far valere.

La sentenza della Corte affronta la questione del bilanciamento soprattutto rispetto alla tutela della libertà di espressione e di impresa, seguendo la linea interpretativa della Corte europea dei diritti dell'uomo, la quale ha già dichiarato, nella sentenza Aleksey Ovchinnikov[20] , che «in alcuni casi può essere giustificato limitare la riproduzione di informazioni già divenute di pubblico dominio, ad esempio al fine di impedire un'ulteriore diffusione dei dettagli della vita privata di una persona estranea a qualsiasi dibattito politico o pubblico su un argomento di importanza generale». Pertanto, in linea di principio, il diritto fondamentale alla protezione della vita privata può essere invocato anche se le informazioni di cui trattasi sono già di pubblico dominio.

Non ha torto l'Avvocato Genereale qunado sostiene che il problema della protezione dei dati si è posto, in questo caso, solo quando un utente ha inseritio nome e cognome della persona interessata nel motore di ricerca ottenendo un link verso le pagine web di un giornale in cui compaiono gli articoli contestati. L'utente ha però *esercitato attivamente il proprio diritto ad ottenere informazioni relative alla persona interessata provenienti da fonti pubbliche* per motivi che possono essere fra i più disparati. Cercare informazioni tramite motori di ricerca costituisce, nell'attuale contesto sociale, forse lo strumento più importante per esercitare tale diritto fondamentale.

Partendo da questa prospettiva, e considerando il legittimo diritto di impresa del fornitore dei servizi in Internet e del gestore del motore di ricerca, ossia quello di organizzare e indicizzare i risultati delle ricerche degli utenti, riconoscere valore predominante al diritto all'oblio vorrebbe dire sacrificare la libertà di espressione e di informazione, che potrebbero essere compromesse ulteriormente se la valutazione, caso per caso, fosse lasciata solo alla decisione degli stessi fornitori di servizi.

In tale contesto, è condivisibile l'osservazione dell'Avvocato Generale, quando avverte che le «procedure di notifica e rimozione» di cui alla direttiva 2000/31 sul commercio elettronico si riferiscono a "contenuti illeciti, mentre il presente caso verte su una richiesta di soppressione di informazioni legittime e legali entrate nella sfera pubblica".

4.2 Il diritto all'oblio nella proposta di regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)

Il c.d. diritto all'oblio è espressamente disciplinato dall'art. 17 della Proposta della Commissione per un regolamento generale sulla protezione dei dati personali[21] .

In estrema sintesi tale disposizione prevede il diritto all'oblio e alla cancellazione[22], rafforzando il diritto alla cancellazione di cui all'art. 12, lett. b) direttiva 95/46, nonché

[20] Aleksey Ovchinnikov v. Russia, n. 24061/04, 16 dicembre 2010.

[21] Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 def., 25 gennaio 2012.

l'obbligo per il responsabile (titolare) del trattamento che abbia divulgato dati personali di informare i terzi della richiesta dell'interessato di cancellare tutti i link verso tali dati, le loro copie o riproduzioni. La disposizione prevede inoltre il diritto di limitare il trattamento in determinati casi, evitando l'ambiguo termine di "blocco dei dati". In particolare, l'interessato deve avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o trattati, quando abbia ritirato il consenso o si sia opposto al trattamento o quando questo ultimo non sia conforme alle disposizioni del regolamento. Tuttavia, occorre consentire l'ulteriore conservazione dei dati qualora sia necessario per finalità storiche, statistiche e di ricerca scientifica, per motivi di interesse pubblico nel settore della sanità pubblica, per l'esercizio del diritto alla libertà di

[22] Si riporta di seguito il testo dell'art. 17. "L'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore, se sussiste uno dei motivi seguenti: a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si fonda il trattamento, di cui all'articolo 6, paragrafo 1, lettera a), oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati; c) l'interessato si oppone al trattamento di dati personali ai sensi dell'articolo 19; d) il trattamento dei dati non è conforme al presente regolamento per altri motivi. 2. Quando ha reso pubblici dati personali, il responsabile del trattamento di cui al paragrafo 1 prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione. 3. Il responsabile del trattamento provvede senza ritardo alla cancellazione, a meno che conservare i dati personali non sia necessario: (a) per l'esercizio del diritto alla libertà di espressione in conformità dell'articolo 80; (b) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 81; (c) per finalità storiche, statistiche e di ricerca scientifica in conformità dell'articolo 83; (d) per adempiere un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento; il diritto dello Stato membro deve perseguire un obiettivo di interesse pubblico, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo; (e) nei casi di cui al paragrafo 4. 4. Invece di provvedere alla cancellazione, il responsabile del trattamento limita il trattamento dei dati personali: a) quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche; b) quando, benché non ne abbia più bisogno per l'esercizio dei suoi compiti, i dati devono essere conservati a fini probatori; c) quando il trattamento è illecito e l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo; d) quando l'interessato chiede di trasmettere i dati personali a un altro sistema di trattamento automatizzato, in conformità dell'articolo 18, paragrafo 2. 5. I dati personali di cui al paragrafo 4 possono essere trattati, salvo che per la conservazione, soltanto a fini probatori o con il consenso dell'interessato oppure per tutelare i diritti di un'altra persona fisica o giuridica o per un obiettivo di pubblico interesse. 6. Quando il trattamento dei dati personali è limitato a norma del paragrafo 4, il responsabile del trattamento informa l'interessato prima di eliminare la limitazione al trattamento. 7. Il responsabile del trattamento predispone i meccanismi per assicurare il rispetto dei termini fissati per la cancellazione dei dati personali e/o per un esame periodico della necessità di conservare tali dati. 8. Quando provvede alla cancellazione, il responsabile del trattamento si astiene da altri trattamenti di tali dati personali. 9. Alla Commissione è conferito il potere di adottare atti delegati in conformità all'articolo 86 al fine di precisare: a) i criteri e i requisiti per l'applicazione del paragrafo 1 per specifici settori e situazioni di trattamento dei dati; b) le condizioni per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico, come previsto al paragrafo 2; c) i criteri e le condizioni per limitare il trattamento dei dati personali, di cui al paragrafo 4".

espressione, ove richiesto per legge o quando sia giustificata una limitazione del trattamento dei dati anziché una loro cancellazione.

Per garantire tale informazione, è necessario che il responsabile (titolare) del trattamento prenda tutte le misure ragionevoli, anche di natura tecnica, in relazione ai dati della cui pubblicazione è responsabile, anche se ha autorizzato un terzo a pubblicarli.

Anche nei casi in cui i dati personali possano essere lecitamente trattati per proteggere interessi vitali dell'interessato, oppure per motivi di pubblico interesse, nell'esercizio di pubblici poteri o per il legittimo interesse di un responsabile (titolare) del trattamento, l'interessato deve comunque avere il diritto di opporsi al trattamento dei dati che lo riguardano.

La proposta di regolamento, però, prevede specifiche limitazioni al diritto all'oblio e alla cancellazione dei dati, fornendo una base giuridica per il bilanciamento fra contrapposte esigenze, ancorata al rispetto del principio di legalità. L'art. 21, infatti, dispone che l'Unione o gli Stati membri possono limitare, mediante misure legislative, la portata di tale diritto qualora la limitazione costituisca una misura necessaria e proporzionata in una società democratica per salvaguardare: a) la pubblica sicurezza; b) le attività volte a prevenire, indagare, accertare e perseguire reati; c) altri interessi pubblici dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, e la stabilità e l'integrità del mercato; d) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; e) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lett. a), b), c), e d); f) la tutela dell'interessato o dei diritti e delle libertà altrui.

La questione più delicata riguarda l'individuazione dell'organo o del soggetto deputato al giudizio di bilanciamento fra le diverse esigenze, da un lato, di tutela della riservatezza e, dall'altro lato, di giustizia penale o per la tutela della sicurezza pubblica o, ancora, per la protezione della libertà di espressione.

L'art. 12 della proposta di regolamento fa incombere in prima battuta sul responsabile (titolare) del trattamento l'obbligo di stabilire le procedure per l'esercizio dei diritti dell'interessato, fra i quali quelli di cui all'art. 17, che devono comprendere l'informazione a tale soggetto, tempestivamente e al più tardi entro un mese – termine prorogabile in casi specifici (se più interessati esercitano i loro diritti e la loro cooperazione è necessaria in misura ragionevole per evitare un impiego di risorse inutile e sproporzionato al responsabile del trattamento dal ricevimento della richiesta) - se è stata adottata un'azione. Se il responsabile (titolare) rifiuta di ottemperare alla richiesta dell'interessato, egli deve informarlo dei motivi e delle possibilità di proporre reclamo all'autorità di controllo e anche ricorso giurisdizionale.

E' noto che nella maggior parte dei casi il fornitore di servizi è un soggetto privato che esercita la libertà di impresa. Egli dovrebbe dimostrare, in caso di rifiuto, non solo che i suoi legittimi interessi possono prevalere sull'interesse o sui diritti e sulle libertà fondamentali dell'interessato, ma anche che la richiesta, nel settore che qui interessa, non possa essere accolta per le esigenze legate alle attività volte a prevenire, indagare, accertare e perseguire reati.

La proposta di regolamento, però, non individua espressamente un nucleo di reati gravi, che possano giustificare un'invasione nella sfera di riservatezza dell'individuo o, quantomeno, la necessità di proteggere beni giuridici di predominante importanza.

Inoltre, il fornitore di servizi coinvolto attivamente in attività di indagine svolge un ruolo di carattere "pubblico", che comporta in molti casi il riserbo sulla natura del coinvolgimento o sull'attività che è "delegato" a svolgere per gli organi investigativi.

Egli sarà dunque portato a rifiutare la cancellazione dei dati o il pieno esercizio del diritto all'oblio, lasciando all'autorità di controllo o all'autorità giudiziaria giudicare su eventuali reclami.

La proposta di regolamento, però, prevede, ex art. 79, specifiche sanzioni amministrative nel caso in cui il responsabile (titolare) non rispetti il diritto all'oblio o alla cancellazione, ometta di predisporre meccanismi che garantiscano il rispetto dei termini o non prenda tutte le misure necessarie per informare i terzi della richiesta dell'interessato di cancellare tutti i link verso i dati personali, copiare tali dati o riprodurli, in violazione dell'art. 17, salve le ulteriori sanzioni, che potrebbero avere altresì natura penale, previste dagli Stati membri, ex art. 78 della stessa proposta.

A ciò si aggiungono gli obblighi generali previsti dall'art. 22 della proposta, fra cui quelli inerenti alla sicurezza dei dati, disciplinati dal successivo art. 30.

In conclusione, il diritto all'oblio definito dalla nuova proposta non è (naturalmente) di natura assoluta e omnicomprensivo dei diritti riconosciuti al soggetto interessato.

5. Verso una definizione "integrata" del diritto all'oblio e possibili linee guida per il bilanciamento con le esigenze proprie del sistema di giustizia penale

A questo punto, e ai fini del presente lavoro, non rimane che affrontare la questione relativa ai rapporti fra diritto all'oblio ed esigenze di perseguire, accertare o prevenire gravi reati, che presuppone la lettura integrata fra le sentenze della Corte di Giustizia sulla *data retention* e sul caso Google/Spagna.

In prospettiva *de jure condendo*, considerando la proposta di regolamento europeo, nella sua attuale formulazione, si potrebbe delimitare il c.d. diritto all'oblio, anche nell'ottica di una auspicabile disciplina degli obblighi di archiviazione dei dati di traffico telefonico e telematico.

Dovrebbe però essere prevista la possibilità di cancellare o rimuovere i dati personali, su richiesta del soggetto interessato, in particolare dai motori di ricerca, dopo un periodo – finestra determinato, in cui eventualmente tali informazioni dovrebbero essere rese non accessibili al pubblico o alle persone non autorizzate.

In tal caso il legislatore europeo, alla luce delle citate sentenze della Corte, dovrebbe osservare le linee guida ricavabili dalla decisione sulla c.d. *data retention* e predisporre un "sistema di obblighi integrato", che preveda: limiti temporali alla conservazione dei dati; procedure di accesso e di acquisizione delle informazioni; l'individuazione dei "gravi" reati "presupposto", nonché la definizione dei presupposti oggettivi che possano giustificare la *data retention; che* la valutazione sull'esistenza dei presupposti sia lasciata ad un organismo indipendente (giudice) attraverso la previsione di una procedura snella e "tempestiva", purchè vi sia una definizione a) di un elevato livello delle "misure di sicurezza" da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento; b) di apposite sanzioni di inutilizzabilità del materiale

probatorio acquisito in modo illecito o in caso di mancato rispetto del "principio di necessità" nel trattamento dei dati.

A questi presupposti dovrebbero aggiungersi gli obblighi di rendere inaccessibili i dati, su richiesta del soggetto interessato. In tal caso si tratterebbe di un diritto all'oblio bifasico. In una prima fase l'interessato otterrebbe l'effetto di non rendere accessibili le informazioni (ad esempio tramite motori di ricerca o i siti che le contengono), le quali però, sul piano tecnico, rimarrebbero a disposizione del fornitore del servizio – se il soggetto destinatario dell'obbligo è riconducibile a questa categoria - per un periodo limitato, utile e necessario per il perseguimento, l'accertamento o la prevenzione di gravi reati. In tal caso sarebbe possibile il coordinamento fra la proposta di regolamento europeo, in particolare dell'art. 21, con una futura e auspicabile disciplina europea in materia di *data retention*.

In una seconda fase, ossia trascorso il periodo previsto da tale ultima disciplina, il fornitore del servizio potrebbe procedere alla cancellazione del dato, salve le ulteriori esigenze di proroga della conservazione nel caso in cui il soggetto interessato sia divenuto indagato o imputato in un procedimento penale. In tale ultima situazione potrebbe trovare piena applicazione una disposizione quale quella di cui all'art. 21 della proposta di regolamento. La qualità di indagato o imputato, infatti, giustificherebbe la conservazione di dati anche con riferimento ai reati non inclusi in un'ipotetica lista di incriminazioni presupposto di una certa gravità.

Per quanto riguarda gli aspetti "procedurali", un primo modello potrebbe essere ricavato dalla direttiva e-commerce e basarsi su un procedimento ingiunzionale connotato da un atto qualificato di un organismo indipendente (un giudice, anche eventualmente su segnalazione o su richiesta della persona fisica o dell'autorità garante), in modo da consentire di effettuare il bilanciamento fra le contrapposte esigenze di tutela e di perseguimento di interessi generali collettivi, che non può essere lasciato all'apprezzamento "soggettivo" del singolo provider [23]. Tale "modello" troverebbe conferma sia nella sentenza della Corte sulla *data retention* sia in quella sul caso Google/Spagna[24].

La "gravità potenziale" dell' ingerenza nei diritti fondamentali verrebbe via via affievolita proprio in base alla rilevanza dei contro interessi e dei diritti che necessiterebbero di tutela quantomeno paritaria.

A ciò deve aggiungersi che a favore della non cancellazione possono sussistere, in primo luogo, anche ragioni statali tipiche di natura paternalistica, ossia quando i dati

[23] Si vedano i rilievi critici espressi da R. Flor, La Corte di Giustizia, cit.

[24] Vedi punto 82 della sentenza: «L'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di applicazione degli artt.12, lett. b), e 14, co. 1, lett. a), della direttiva 95/46, da effettuarsi allorché ricevono una domanda quale quella oggetto del procedimento principale, possono ordinare al suddetto gestore di 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 tale persona, senza che un'ingiunzione in tal senso presupponga che tale nome e tali informazioni siano, con il pieno consenso dell'editore o su ingiunzione di una delle autorità sopra menzionate, previamente o simultaneamente cancellati dalla pagina web sulla quale sono stati pubblicati». Ex art. 28, par. 3 e 4 della direttiva, qualsiasi persona può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali, e che tale autorità dispone di poteri investigativi e di poteri effettivi di intervento che le consentono di ordinare in particolare il congelamento, la cancellazione o la distruzione di dati, oppure di vietare a titolo provvisorio o definitivo un trattamento.

sono raccolti ed archiviati nell'interesse del medesimo individuo e/o della collettività. In tal caso, pur potendo limitare l'accesso a queste informazioni, esse non dovrebbero essere completamente eliminate ma solamente, e eventualmente, oscurate (rectius rese accessibili solo a persone determinate, autorizzate o legittimate).

In secondo luogo, possono prevalere non solo interessi collettivi o generali, che portano beneficio all'intera comunità, come nel caso delle esigenze legate alla repressione e alla prevenzione dei reati, nonché alla raccolta della prova in formato digitale, che rispondo altresì all'esigenza di proteggere la sicurezza nazionale, ma anche, come ha affermato la Corte di Giustizia, la libertà di espressione e la libertà economica[25].

Fermo restando il diritto del soggetto interessato di ottenere, tramite l'ordine di un giudicie, la cancellazione di dati o informazioni che lo riguardano, che costituiscono gli "effetti" o il "pregiudizio" di un illecito già accertato (si pensi ai classici casi di diffamazione tramite *social networks*, blog o siti indicizzati dai motori di ricerca: in questo caso l'interesse principale della "vittima" è ottenere la rimozione della notizia diffamatoria dai risultati delle ricerche *online* e/o dai siti in cui si trova [26]). Analogamente, come è ricavabile dalle motivazioni della sentenza nel caso Google/Spagna, dovrebbe rimanere fermo il diritto all'oblio dell'autore di un reato che, scontata la pena, vede associato il proprio nome a fenomeni criminosi anche a distanza di molti anni, nel rispetto degli standard e dei meccanismi procedurali descritti dalla Corte stessa, eventualmente integrati con le ulteriori safeguards sopra riportate[27].

Ad ogni modo la domanda della persona interessata pressuppone l'incompatibilità con la direttiva 95/46 del trattamento, anche se questo inizialmente era da considerarsi lecito[28].

---

[25] In questo senso vedi P. Bernal, Internet Privacy Rights, Cambridge University Press, 2014, 199 e ss. E' utile tenere distinta la figura di un motore di ricerca rispetto a quella di siti-fonte o testate giornalistiche online. Il trattamento da parte dell'editore di una pagina web, infatti, potrebbe consistere nella pubblicazione di informazioni relative a una persona fisica, effettuata «esclusivamente a scopi giornalistici» . Ex art. 9 della direttiva 95/46, egli benificerebbe delle deroghe alle prescrizioni dettate da quest'ultima, mentre non integrerebbe tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli arti. 12, lett. b), e 14, co. 1, lett. a), della direttiva contro il suddetto gestore del motore di ricerca, ma non contro l'editore della pagina web.

[26] Si veda a titolo esemplificativo, fra alcuni dei più recenti casi italiani: Trib. Milano, ord. 24 marzo 2011. Si veda altresì la recente proposta di legge "Modifiche alla legge 8 febbraio 1948, n. 47, al codice penale e al codice di procedura penale in materia di diffamazione, di diffamazione con il mezzo della stampa o con altro mezzo di diffusione, di ingiuria e di condanna del querelante" (Atto Camera 925 – Atto Senato 1119), in particolare nella versione emendata a seguito della sentenza della Corte di Giustizia sul caso Google/Spagna: *«Art. 2-bis (Misure a tutela del soggetto diffamato o del soggetto leso nell'onore e 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 ai siti internet e ai motori di ricerca l'eliminazione dei contenuti diffamatori o dei dati personali trattati in violazione delle disposizioni di cui alla presente 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 ai siti internet e ai motori di ricerca la rimozione delle immagini e dei dati ovvero di inibirne l'ulteriore diffusione. 3. In caso di morte dell'interessato, le facoltà e i diritti di cui al comma 2 possono essere esercitati dagli eredi o dal convivente»*.

[27] Vedi *supra*, par. 2 e 3.

[28] Con il tempo, infatti, tale trattamento potrebbe non essere più necessario in rapporto alle finalità per le quali sono stati raccolti i dati, come nei casi in cui essi risultino inadeguati, o non siano più pertinenti, in rapporto proprio al tempo trascorso.

6. Conclusioni.

Nell'attuale assetto della società dell'informazione e di Internet non è possibile pensare di affrontare le sfide poste dalle nuove tecnologie senza poter sfruttare le loro potenzialità.

Per l'accertamento e la prevenzione di reati, infatti, l'accesso a dati e informazioni personali comporta spesso un "salto nel passato", per ricostruire trame comunicative, "spostamenti" *online* e, talvolta, fisici, sulla scorta di tecniche di localizzazione.

Il "monitoraggio" della rete e, dunque, anche dei risultati della ricerca tramite *search tools* e *web search engine* può risultare in molti casi un'attività indispensabile al fine non solo di raccogliere elementi indiziari o probatori, ma anche per individuare la fonte o il luogo "virtuale" specifico in cui sono "archiviati" i dati, oltre che per prevenire attività illecite e gravi reati.

La questione da porsi riguarda i limiti entro i quali può operare il legislatore (nazionale ed europeo) nella compromissione dei diritti fondamentali e nel prevedere gli standars su cui basare il delicato giudizio di bilanciamento con altri diritti fondamentali e con le esigenze di tutelare importanti interessi generali e collettivi, nel rispetto del principio di proporzione.

Al riguardo, l'art. 52 della Carta dei diritti fondamentali dell'Unione europea, identifica proprio nel principio di proporzione il criterio guida fondamentale, sia sul piano ermeneutico che su quello delle scelte politico normative del legislatore, delimitandone l'area di discrezionalità.

Sarebbe utopistico, infatti, credere che l'utente medio del nuovo millennio non utilizzi le opportunità offerte dalla evoluzione-rivoluzione informatica. Sarebbe altrettanto utopistico credere di contrastare forme di criminalità anche grave senza ricorrere alle stesse opportunità offerte dalla evoluzione-rivoluzione informatica.

Per queste ragioni le linee guida ricavabili dalla lettura sistematica delle sentenze della Corte di Giustizia sui casi Google/Spagna e *data retention* potrebbero costituire il primo ed importante mattone delle fondamenta su cui edificare i "parametri" certi per consentire il giudizio di bilanciamento fra le contrapposte esigenze di tutela, nonché di accertamento e prevenzione dei reati.

Laboratorio Permanente di Diritto Penale
Via Fontana, 28 – 20122 Milano (Italia)
C.F. 97664840150
Web: http://labdirpen.wix.com/diplap

Di.P.La.P. è un'associazione fondata da un gruppo di studiosi italiani di diritto e procedura penale per aggregare e rispondere alle istanze di rinnovamento e democratizzazione della ricerca e del dibattito penalistici. Valori costitutivi sono l'autonomia e l'indipendenza organizzativa e scientifica, la multidisciplinarietà, l'apertura al mondo extra-accademico e professionale, la solidarietà intergenerazionale.

Il volume raccoglie gli atti del I convegno nazionale del Laboratorio Permanente di Diritto Penale, che si è tenuto a Perugia il 19 settembre 2014, sul tema "La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet".

L'incontro è stato caratterizzato da un vivace dibattito sui temi più attuali che coinvolgono le complesse implicazioni fra il sistema penale e le nuove tecnologie in una prospettiva europea ed internazionale: la società dell'informazione, infatti, ha da tempo comportato dei cambiamenti epocali in ogni settore della vita umana, implicanti non solo molteplici opportunità di sviluppo "positivo", sul piano sociale, culturale ed economico.

Su questo fertile terreno fioriscono difatti anche nuovi fenomeni, modi e tipi di comportamenti di rilievo penale, e si aprono "altri" percorsi per commettere reati "tradizionali"; d'altro canto il mondo digitale si dimostra una fondamentale frontiera per la lotta alla criminalità moderna, offrendo innovativi strumenti e mezzi per la ricerca delle prove e, in generale, per il contrasto a vasti settori di illiceità penale.

I curatori

Daniela Falcinelli è ricercatrice a tempo determinato in diritto penale nell'Università di Perugia (sede di Terni, Narni), nonchè docente di diritto penale presso le Scuole forensi di diversi Consigli dell'Ordine degli Avvocati e corsi post lauream.

Roberto Flor è ricercatore confermato in diritto penale e professore aggregato di diritto penale, diritto penale dell'informatica ed International Criminal Law nell'Università di Verona.

Stefano Marcolini è ricercatore confermato in diritto processuale penale e professore aggregato in diritto penitenziario e diritto processuale penale nell'Università dell'Insubria (sede di Como).

DIPLAP Editor

2015