ISSN 2240-7243

AIAF

RIVISTA DELL'ASSOCIAZIONE ITALIANA DEGLI AVVOCATI PER LA FAMIGLIA E PER I MINORI

2020/1

Cybercrime e Codice Rosso

G. Giappichelli Editore

Rivista trimestrale - I - 2020

www.aiafrivista.it

AIAF

RIVISTA DELL'ASSOCIAZIONE ITALIANA DEGLI
AVVOCATI PER LA FAMIGLIA E PER I MINORI

RIVISTA DELL'ASSOCIAZIONE ITALIANA DEGLI
AVVOCATI PER LA FAMIGLIA E PER I MINORI
Trimestrale – reg. Trib. Milano 24 settembre 2013, n. 288

Anno XXIV, n. 1

G. Giappichelli Editore - 10124 Torino
via Po, 21 - Tel. 011-81.53.111 - Fax 011-81.25.100
http://www.giappichelli.it

ISSN 2240-7243
EISSN 2704-6508

Redazione
Via Lentasio n. 7, 20122 Milano – tel. 02 29535945
segreterianazionale@aiaf-avvocati.it www.aiaf-avvocati.it

La pubblicazione di ogni scritto è subordinata alla valutazione positiva di *blind referees*

Stefania Bandinelli, Paola Bardi, Massimo Benoit Torsegno, Francesca Caporale, Ethel Carri, Giuliana Castelletti, Elisa Chiaretto, Federica Di Benedetto, Chiara Favilli, Federica Fuggetti, Rossana Lo Monaco, Barbara Manganelli, Stefania Mendicino, Luciano Olivero, Anna Pacciarini, Alessandra Poli, Maria Rita Salvatore, Giulia Sapi, Fausta Scia, Elisa Tosini

Stampa
Stampatre s.r.l., via Bologna 220, 10154 Torino
Finito di stampare nel mese di marzo 2020

CYBERCRIME E TUTELA PENALE DEI DIRITTI DELLA PERSONA E DELLA *PRIVACY* NEL WEB

Lorenzo Picotti
Professore di Diritto penale nell'Università di Verona

Abstract: La criminalità cibernetica richiede una risposta sempre più sofisticata ed evoluta, apparendo indispensabile la convergenza di una corretta disciplina processuale, accanto ad un'innovativa disciplina di diritto penale sostanziale, che adeguando progressivamente le formulazioni normative non idonee o introducendo nuove fattispecie specifiche – come ad esempio quella più recente di cui all'art. 612 *ter* c.p. che incrimina il *revenge porn* – renda sicura o più agevole la punizione dei nuovi fenomeni delittuosi. Osserva l'autore che è dunque compito del giurista, adeguare le proprie conoscenze non solo normative, ma anche tecniche, indispensabili per cogliere la nuova dimensione, con cui ci si deve ormai confrontare, affinché possa essere garantita effettiva tutela.

Parole chiave: *cybercrime – privacy* nel web – reati cibernetici – violenza virtuale – offesa

Abstract: *Cybercrime requires an increasingly sophisticated and evolved response, given that a convergence between appropriate procedural discipline and innovative regulation of criminal law appears indispensable. This convergence, by gradually adjusting unsuitable regulatory formulations or introducing new specific offences – such as, for example, the more recent one pursuant to art. 612* ter *of the Italian Criminal Code that makes revenge porn a crime – would make it simpler and easier to punish new criminal phenomena. The author observes that it is therefore the jurist's task to adjust not only his or her regulatory knowledge, but also the techniques indispensable for grasping the new dimension to be dealt with so that effective protection might be guaranteed.*

Keywords: *cybercryme – web privacy – cyber crimes – virtual violence – offense*

1. Introduzione: lo sviluppo del *Cyberspace* e le nuove esigenze di tutela dei diritti fondamentali

Lo sviluppo impetuoso delle tecnologie informatiche, ed in particolare delle modalità di connessione, trasmissione, automazione nella raccolta e nell'elaborazione dei dati, in quantità sempre più grandi (c.d. *big data* e TIC: "tecnologie dell'informazione e della comunicazione", in inglese ICT), che consentono altresì di collegare pressoché permanentemente – grazie ai sempre più sofisticati dispositivi mobili (*smartphone, tablet,* apparecchi portatili di ogni genere e

dimensione, ecc.), dotati di una capacità di memoria e di una velocità di elaborazione e trasmissione dei dati, che fino a pochi anni fa erano inimmaginabili anche per i più avanzati computer disponibili sul mercato – milioni di utenti e rendere così accessibili e fruibili, in ogni momento e luogo, grazie anche ai molteplici servizi *cloud*, informazioni, messaggi, video, film, eventi in diretta, file audio musicali e di qualsiasi altro genere e dimensione, ha profondamente trasformato e fatto evolvere non solo l'economia, la politica, la gestione del tempo libero e delle relazioni sociali ed individuali, ma anche le tecniche di realizzazione e le modalità di manifestazione di comportamenti illeciti e di fatti criminosi, o quantomeno dannosi, che hanno trovato nuove opportunità di espandersi e di svilupparsi nel c.d. *Cyberspace*, assumendo l'ampia denominazione, oggi corrente, di *cybercrime*, vale a dire "reati cibernetici".

Occorre subito sottolineare che, accanto all'indispensabile substrato tecnologico, appare decisiva in questa rapida trasformazione – che è stata definita a ragione "rivoluzione cibernetica", o quarta rivoluzione [1] – la parallela dimensione sociale del fenomeno, poiché in forza della diffusione ed utilizzazione in ogni ambito di tali tecnologie e dispositivi, si è sviluppata detta nuova realtà globale, il *Cyberspace*, in cui ci troviamo ormai tutti permanentemente "immersi", senza potercene distaccare.

Non si tratta di una dimensione o mondo "virtuale", come talora si afferma, quasi fosse possibile separarlo dalla società odierna, ma viceversa di un suo ambito del tutto reale, in cui si svolge una parte imprescindibile della nostra vita personale e di relazione, oltre che degli attori politici, economici e sociali, coinvolgendo tutti i diversi settori, dall'informazione al lavoro, dalla produzione al commercio, dall'istruzione alla ricerca, fino al tempo libero ed ai rapporti più intimi.

Per questo anche la tutela (non solo penale) dei diritti fondamentali della persona, a partire dalla *privacy* [2], messa strutturalmente in pericolo e per taluni addirittura ormai "morta" date le caratteristiche di tale sviluppo, che si nutre incessantemente delle informazioni e dei dati che ciascun utente, consapevolmente o meno, lascia nel web, si gioca oggi necessariamente e sempre più nella dimensione del *Cyberspace*, in cui si commettono – proprio per il descritto avvolgente sviluppo – anche le più allarmanti e gravi violazioni, che ivi acquistano potenzialità offensive ed espansive del tutto inedite.

Da tempo i giuristi più attenti – superata l'utopistica idea degli anni '90, quando Internet era stato reso accessibile al pubblico e veniva, quindi, visto soltanto come un nuovo spazio di libertà e di democrazia, potenzialmente illimitato ed aperto a chiunque, in grado di sfuggire addirittura ai vincoli ed alle restrizioni del mondo reale – hanno evidenziato come sia necessario pensare al più presto ad un'efficiente e compiuta regolamentazione giuridica, a partire dall'idea di una "Costituzione per Internet" [3]. Ad essa ha lavorato in effetti anche in Italia un qualificato gruppo di lavoro, istituito dalla Camera dei Deputati nella scorsa legislatura e guidato da Stefano Rodotà, che ha portato nel 2015 alla redazione di un importante testo – purtroppo mai divenuto valida fonte giuridica e forse troppo poco conosciuto – nel quale, in coerenza anche con altri modelli

[1] Cfr. per tutti, con ampi riferimenti anche alla letteratura internazionale, L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (2014), trad. it. Raffaello Cortina, Milano, 2017; e più di recente il capitolo introduttivo di U. PAGALLO, *Profili tecnico-informatici e filosofici*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *Cybercrime*, Utet Giuridica, Milano, 2019, p. 3 s. e la bibliografia ivi citata.

[2] Su tale nozione, da intendere quale "diritto alla protezione dei dati personali", sia consentito rinviare a L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in ID. (a cura di), *Tutela penale della persona e nuove tecnologie*, Cedam, Padova, 2013, p. 32 s., anche per la distinzione dalla confinante categoria della "riservatezza informatica" e sui reati che la offendono, su cui si veda più di recente I. SALVADORI, *I reati contro la riservatezza informatica*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 656 s. con ampi riferimenti bibliografici.

[3] Cfr. in specie S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014.

elaborati in ambito internazionale, è raccolto un essenziale catalogo di diritti fondamentali della persona, da salvaguardare prioritariamente nel *Cyberspace*, desunti da o riconducibili a quelli già riconosciuti dalle Convenzioni internazionali e dalle Costituzioni delle società democratiche, ma appositamente selezionati, riformulati, integrati con nuovi contenuti, in modo da garantire quelle libertà basilari e quei diritti dell'uomo, su cui si deve fondare la moderna società digitale, per salvaguardare i canoni di democrazia propri della tradizione del *rule of law* e dello Stato di diritto[4].
La mancata attuazione di questo e di simili ambiziosi progetti di portata globale, richiede in ogni caso, più concretamente e limitatamente, di cercare e rinvenire, nelle previsioni normative degli ordinamenti vigenti, a partire dalle fonti sovranzionali in materia, gli strumenti giuridici indispensabili per contrastare l'illegalità e soprattutto le violazioni dei diritti fondamentali della persona che si commettono nel *Cyberspace*, fornendo tutela, il più possibile efficace e dunque, ovviamente, anche penale, a coloro che individualmente o collettivamente ne sono vittime.
La dematerializzazione, l'ubiquità, la permanenza nel tempo delle violazioni e delle condotte illecite che sono oggi rese possibili anche con la copertura dell'anonimato dalle nuove tecnologie e dalla loro espansione non adeguatamente regolamentata nel *Cyberspace*, richiedono in particolare al penalista di cogliere e di confrontarsi con i limiti della disciplina positiva vigente, cercandone una corretta reinterpretazione od adattamento ed eventualmente di proporne la riforma, fino a sviluppare nuove categorie concettuali e sistematiche.

2. La nozione di "violenza" nel *Cyberspace*

Si può paradigmaticamente muovere dal concetto di "violenza" nel *Cyberspace*.
Tradizionalmente nel diritto penale si distingue fra "violenza sulle cose" e "violenza alla persona": nozioni entrambe che si è costretti a riadattare, se si manifestano o, meglio, si pensano come realizzabili attraverso sistemi di elaborazione automatica e di trasmissione o comunicazione in rete di dati, messaggi, immagini od ogni altro contenuto dannoso o pericoloso.
Si pensi, in particolare, muovendo da una sintomatica norma del nostro ordinamento positivo, alla definizione di "violenza sulle cose" contenuta nell'art. 392, 2° comma, c.p., al quale fin dal 1993 è stato aggiunto un nuovo 3° comma, per far fronte a fatti di danneggiamento di oggetti o beni informatici "immateriali" come programmi, software, informazioni, dati, raccolti da sistemi di elaborazione e trattamento automatizzati, che si manifestavano con le prime applicazioni ed utilizzazioni degli elaboratori elettronici.
Ebbene, con la nuova estensione definitoria, il legislatore ha dovuto abbandonare il presupposto della "fisicità" degli atti costituitivi della nozione tradizionale, pensati come ricadenti su oggetti materiali ("cose"), ed ha invece delineato le diverse condotte di «alterazione, modificazione o cancellazione in tutto o in parte di un programma informatico» ovvero di «impedimento o turbamento del funzionamento di un sistema informatico o telematico»[5].

[4] Si veda la "Dichiarazione dei diritti in Internet" elaborato dalla *Commissione per i diritti e i doveri relativi ad Internet* che può reperirsi, unitamente ai documenti preparatori, al sito della Camera dei Deputati *www.camera.it*.

[5] Il capoverso dell'art. 392 c.p. recita: «Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione»; mentre il 3° comma, aggiunto dall'art. 1, l. 23 dicembre 1993, n. 547, estende così tale nozione: «Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico». Sia consentito rinviare, sulle ragioni ed i limiti di tale novella, a L. PICOTTI, (voce) *Reati informatici*, in *Enc. giur. Treccani*, VIII, agg., 2000, p. 16 s.

Tali comportamenti possono essere considerati come "violenti" solo in senso traslato, rappresentando piuttosto una modalità di interferenza abusiva o non autorizzata sul corretto funzionamento di sistemi informatici o sulla disponibilità, integrità, autenticità di programmi, dati ed informazioni, da parte di soggetti non legittimati ad intervenirvi.
Ma l'equiparazione voluta dal legislatore è comunque importante, in quanto detta nozione è un elemento costitutivo essenziale di molteplici altri delitti, oltre a quello di «esercizio arbitrario delle proprie ragioni con violenza sulle cose» (art. 392, 1° comma, c.p.), da cui aveva tratto spunto la novella del 1993. Esso è ad esempio alla base dei delitti di danneggiamento informatico (artt. 635 *bis* s. c.p.), vale a dire non sulle "cose" materiali (come prevede il reato di danneggiamento comune, di cui all'art. 635 c.p.), bensì su dati, informazioni, programmi ovvero sistemi informatici e telematici; ed è elemento costitutivo anche di più gravi reati, come la «turbata libertà dell'industria o del commercio» mediante "violenza sulle cose" (art. 513 c.p., che prevede in alternativa anche l'uso di "mezzi fraudolenti"), nonché l'«illecita concorrenza con minaccia o violenza» di cui all'art. 513 *bis* c.p.[6], o l'estorsione, parimenti realizzabile mediante violenza sulle cose (art. 629 c.p.), che in effetti risulta sia commessa, in numerose ipotesi anche recenti, installando clandestinamente, ad es. mediante un *trojan* o semplici e-mail ingannevoli, programmi c.d. maligni (*malware*) nei sistemi informatici delle vittime, che ne criptano il software, i dati e gli archivi, bloccandone la disponibilità, che può essere riacquisita solo previo pagamento di un importo estorsivo, magari in *bit coin*, cui viene subordinata la consegna della chiave di decriptazione.

3. (Segue). In particolare le nuove forme di "violenza alla persona" e l'offesa dei suoi diritti fondamentali nel *Cyberspace*

Rispetto ai diritti fondamentali della persona è ancor più rilevante l'incidenza di simili forme di interferenze, manipolazioni, condotte abusive o comunque non autorizzate commesse nel *Cyberspace* nel contesto di relazioni interpersonali.
Innanzitutto vengono in rilievo forme di raccolta, trattamento e gestione non autorizzate di informazioni e dati di contenuto personale, comprese immagini, video, registrazioni anche vocali di conversazioni o quant'altro, carpite all'insaputa o contro la volontà del titolare o comunque dell'interessato cui si riferiscono, che già di per sé costituiscono violazioni della *privacy*[7], poi utilizzate o diffuse per coartare la volontà e la libertà di autodeterminazione della vittima, dun-

[6] Su tale problematica fattispecie, introdotta dalla l. 13 settembre 1982, n. 646, c.d. Rognoni-La Torre per il contrasto alla mafia, cfr. di recente Cass., Sez. II., sent. 19 giugno 2018 (dep. 5 luglio 2018), n. 30406, Pres. Davigo, Est. Recchione, in *www.penalecontemporaneo.it* (fasc. 5/2019), con ampio commento di E. MEZZA, *Illecita concorrenza con minaccia o violenza: l'affannosa ricerca di una tipicità sfuggente.*

[7] Come noto, la disciplina del trattamento e della circolazione dei "dati personali" si impernia sul principio del consenso dell'interessato (vale a dire del soggetto cui i dati si riferiscono), sia nella raccolta, sia ancor più nella comunicazione e diffusione degli stessi, salve le numerose ipotesi in cui le diverse attività di "trattamento" siano previste od imposte dalla legge o da altre disposizioni, anche contrattuali, o per fini specificamente definiti che le legittimano. In materia il nostro codice della *privacy* (d.lgs. 30 giugno 2003, n. 196) è stato profondamente modificato dal d.lgs. 10 agosto 2018, n. 101, di adeguamento al Reg. UE n. 698/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. GDPR), che ha abrogato la precedente Direttiva 95/46/CE. Esso, a differenza di quest'ultima, ha efficacia diretta nel nostro ordinamento, comprese le incisive sanzioni di natura amministrativa previste nel caso di violazioni di suoi numerosi precetti. Le sanzioni penali, invece, sono rimaste di competenza del legislatore nazionale, che ha però ampiamente riformulato la disciplina previgente, con il citato d.lgs. n. 101/2018. Per i testi normativi ed i numerosi provvedimenti connessi, si veda il sito ufficiale del Garante *www.garanteprivacy.it*; per commenti cfr. D. LABIANCA, *Il sistema delle tutele nel regolamento europeo n. 679/2016 sulla protezione dei dati personali*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 978 s.; F. RESTA, *I reati in materia di protezione dei dati personali, ivi*, p. 1019 s.

que quale strumento di ricatto o comunque di minaccia di un male ingiusto, idoneo a condizionarne le decisioni od a far tollerare ulteriori comportamenti ingiusti; sia per finalità di mera ritorsione, di svilimento, di umiliazione o anche di semplice diffamazione del soggetto che ne sia ritratto o coinvolto, producendo offese spesso irreparabili della sua immagine, identità, dignità.
L'esperienza recente dimostra come questi comportamenti, pur non potendosi qualificare giuridicamente "violenti", in mancanza, per di più, di una norma definitoria o di "equivalenza" normativa, quale quella sopra esaminata con riferimento alla nozione di "violenza sulle cose", si presentano con una forza di aggressione e di pressione morale sulla vittima, che può anche essere di fatto superiore a quella di una violenza fisica, specie considerando le caratteristiche dei comportamenti e dei loro effetti nel *Cyberspace*, su cui si tornerà ancora. Ed essi si moltiplicano in modo allarmante, specie nei *social network*, ma non solo, per la facilità di realizzazione e la mancanza di un diretto contatto personale con la vittima, che contribuisce a far venir meno i freni inibitori[8].
Spesso, purtroppo, si tratta di fatti commessi a danno di minori, e ad opera anche di altri minori, come emerge nel preoccupante fenomeno del c.d. cyberbullismo, che si presenta in molteplici forme in allarmante espansione in diversi ambiti, da quello scolastico, a quello sportivo e più genericamente di frequentazioni anche nel tempo libero, in ogni caso configurandosi in termini di "sopraffazione" e di "degradazione" della vittima, nei rapporti fra coetanei e non solo, in cui la perdita del reciproco rispetto e riconoscimento della rispettiva qualità di "persona" sembra facilitata proprio dall'intermediazione delle TIC[9].
Ma anche nel contesto di relazioni sentimentali, coniugali, interpersonali, logorate o che entrino in crisi o cessino, spesso anche a causa dell'interferenza con messaggi o rivelazioni colte nel *Cyberspace*, emergono strascichi di così forte frustrazione e reazione, anche radicale ed incontrollata, che si manifestano non più o non soltanto con espressioni dirette, comunicazioni verbali o scritte, pur anche fisico-corporali, in un confronto comunque reale fra le persone, bensì mediatamente e spesso esclusivamente nel web e nei *social network*[10]: con tutta la carica di diffusività, capillarità, incontrollabilità e permanenza delle comunicazioni, dei messaggi, delle immagini, dei video diffusi nel web, che determinano un non meno grave livello di umiliazione e degradazione della persona che ne sia bersaglio, tanto da poter essere parimenti assimilabile ad una "violenza" quantomeno morale sulla stessa. Si pensi ai comportamenti qualificabili come *revenge-pornography*, oggetto di recente specifica incriminazione penale[11], ovvero come *cyberstalking*, parimenti oggetto della specifica previsione normativa di una nuova circostanza aggravante del delitto di atti persecutori[12]; o più banalmente ai numerosissimi casi di diffamazione *on-*

[8] Per un quadro generale cfr. R. FLOR, *Le "nuove" forme di violenza contro "soggetti vulnerabili" nel contesto tecnologico: un quadro fenomenico*, in questa *Rivista*. E di recente cfr. CEDU, Sez. IV, 11 febbraio 2020, ricorso 56867/15, *Butaruga v. Romania* secondo cui nella fattispecie di "violenza domestica" contro le donne rientrano anche i casi di cyberviolenza come l'accesso ai dati sensibili della vittima e ai suoi *account* privati.

[9] In argomento, cfr. infra, G. DE STROBEL, *Il cyberbullismo: la nuova legge 29 maggio 2017, n. 71*, in questa *Rivista*, nonché nell'ampia letteratura (non solo penalistica), basti il rinvio a M. C. PARMIGGIANI, *Il cyberbullismo*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 631 s.

[10] Volendo cfr. in argomento L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* Social Network. *Aspetti penali*, in *Giur. merito*, 2012, 12, p. 2522 s.

[11] L'art. 10, l. 19 luglio 2019, n. 69 ha introdotto nel codice penale l'art. 612 *ter*, quale autonoma figura delittuosa volta a reprimere tale fenomeno. Per un commento si rinvia a F. PANIZZO, *Luci ed ombre sulla "vendetta pornografica" disciplinata dall'art. 612* ter *c.p.*, in questo fascicolo della *Rivista*.

[12] Il 2° comma dell'art. 612 *bis* c.p., che punisce il delitto di "atti persecutori", prevede un'aggravante «se il fatto è commesso attraverso strumenti informatici o telematici» a seguito della modifica portata dall'art. 1, 3° comma, lett. d), d.l. 14 agosto 2013, n. 93, conv. in l. 15 ottobre 2013, n. 119. Sul tema cfr. F. MACRÌ, *Il Cyberstalking*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 615 s.

line, in ogni forma ed in specie sui *social network*, inquadrati dalla giurisprudenza nella fattispecie aggravata di cui al 3° comma dell'art. 595 c.p.[13], giungendo però talora fino alla deformazione od al "furto" dell'identità c.d. digitale della persona offesa, che per ora il legislatore ha considerato soltanto come peculiare ipotesi aggravata della frode informatica, ma che in realtà dimostra di andare ben oltre l'ambito dei delitti contro il patrimonio, attingendo il nucleo essenziale dei diritti della persona, da tutelare in quanto tale nel *Cyberspace*, per il crescente peso che vi assume, tanto che se ne suggerisce da tempo un'autonoma apposita incriminazione[14].

Si tratta di comportamenti lesivi che richiedono certamente una specifica risposta penale, avendo una carica di offensività di beni giuridici primari, quali i diritti fondamentali della persona, non minore di quella ravvisabile in corrispondenti comportamenti che tradizionalmente si manifestano e vengono incriminati dalle comuni fattispecie concepite per condotte poste in essere nel mondo fisico esterno al web.

Non solo deve valere il principio che ciò che è illecito e meritevole di sanzione penale *off-line*, non può essere lecito o tollerato *on-line*: ancor più, un efficace intervento repressivo, laddove si dimostra inefficace od insufficiente la prevenzione (come dimostra il contrasto al cyberbullismo), appare indispensabile proprio per i peculiari connotati di diffusività, potenzialmente illimitata nello spazio globale del web, di accessibilità a chiunque, da qualunque luogo ed in ogni momento, dei dati, messaggi, immagini, video, audio e qualsiasi altro contenuto illecito o dannoso, caricato e diffuso nel *Cyberspace*, che è destinato a permanere per un tempo indeterminato, essendo assai difficile se non tecnicamente impossibile intervenirvi in modo tale da garantire una definitiva ed assoluta rimozione dalla rete. L'architettura propria di Internet e delle tecniche di trasmissione telematica, veicolate in snodi, rami, reti autonome, *router*, server di trasmissione, con cui sono riprodotti automaticamente e rinviati i pacchetti di dati, nei quali si scompongono documenti e file di ogni genere, seguendo i percorsi di connessione disponibili e sempre mutevoli, ha portato la stessa giurisprudenza europea ha dover riconoscere l'impossibilità di una compiuta e totale rimozione, tanto da limitare ad es. l'obbligo di cancellazione all'esclusione della reperibilità con i comuni browser e motori di ricerca, nelle versioni corrispondenti a tutti gli Stati membri (c.d. portata territoriale del diritto alla deindicizzazione)[15].

Di qui, la peculiare necessità di attuare, accanto a politiche di prevenzione e di responsabilizzazione, interventi diretti a garantire la possibilità d'individuare l'identità degli utenti e la sistematica e pronta collaborazione dei gestori delle reti e dei servizi nel web (i c.d. *Internet Service Providers*), specie se in quelle posizioni dominanti, ormai acquisite attraverso concentrazioni progressive di potere e controllo, come nei casi paradigmatici di Facebook o di Google, che devono essere quantomeno bilanciate da una corrispondente ascrizione di responsabilità, eventualmente anche penale, in caso di violazioni degli obblighi di prevenzione e d'impedimento dei reati o di rimozione tempestiva dei contenuti illeciti o dannosi, pur riferibili agli utenti[16].

[13] In argomento si veda P. LASALVIA, *La diffamazione via* web *nell'epoca dei* social network, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 331 s.; volendo già L. PICOTTI, *Profili penali delle comunicazioni illecite via* Internet, in *Dir. inf. inform.*, 1999, 2, p. 283 s.

[14] In argomento cfr. M. MARRAFFINO, *La sostituzione di persona mediante furto di identità digitale*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 307 s.; e già R. FLOR, Phishing, identity theft e identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, p. 899; da ultimo C. CRESCIOLI, *Una sentenza della Cassazione sulla sostituzione di persona* online, in *www.penalecontemporaneo.it* (21 giugno 2019).

[15] Cfr. Corte Giust. UE, 24 settembre 2019, causa C-507/17, *Google LLC v. CNIL*, che può leggersi anche nel sito "Osservatorio *Cybercrime*" (*http://sites.les.univr.it/cybercrime*), sub *Topic* "Privacy"; nonché Corte Giust. UE, 3 ottobre 2019, causa C-18/18, *Glawischin-Piesczek v. Facebook*, *ivi*, sub *Topic* "Internet Service Provider", circa il rispetto dell'ambito del diritto internazionale pertinente.

[16] Sull'ampio dibattito e sull'evoluzione della giurisprudenza europea in materia, cfr. volendo L. PICOTTI, *Diritto penale e*

4. Cenni alle principali classificazioni sistematiche dei *cybercrime* in specie in danno di vittime vulnerabili

La recente legislazione nazionale e convenzionale, oltre che dell'Unione europea, documenta la progressiva attenzione giuridica e penale, diretta a contrastare i nuovi fenomeni criminosi, imponendo un adeguamento degli strumenti non solo normativi, ma anche operativi e di indagine, necessari ad assicurare un efficace intervento a garanzia dei diritti e dei beni giuridici, anche primari, che vengono minacciati o violati nel *Cyberspace*.

Alla luce del diritto penale vigente, resta valida una basilare classificazione sistematica delle diverse forme di manifestazione dei *cybercrime*, distinguendo innanzitutto i reati che sono stati specificamente formulati dal legislatore per incriminarli, con nuove fattispecie *ad hoc*, includendo cioè, fra i loro elementi costitutivi, modalità di condotta, oggetti, mezzi, effetti connotati da un contenuto tecnico-informatico, inconcepibile se si prescindesse dalle TIC, che possono essere definiti "reati cibernetici" in senso stretto [17].

Questi sono esemplificativamente i delitti di accesso abusivo ad un sistema informatico (art. 615 *ter* c.p.), i danneggiamenti informatici (artt. 635 *bis, ter, quater, quinquies* c.p.), le falsità in documenti informatici pubblici (*ex* art. 491 *bis* c.p.), la frode informatica (art. 640 *ter* c.p.), ecc.

Tali nuove incriminazioni, per lo più raccomandate o imposte da fonti sovranazionali [18] (quali in specie la Convenzione *Cybercrime* del Consiglio d'Europa del 2001 e la Direttiva UE 2013/40), si sono rese necessarie per colmare lacune giuridiche che non sarebbe stato possibile superare in via interpretativa, per il divieto di analogia in *malam partem* discendente dal fondamentale principio di legalità in materia penale, benché spesso i fatti così incriminati si presentino con tratti di forte somiglianza rispetto a fattispecie tradizionali già vigenti, sia dal punto di vista dell'offesa a beni giuridici identici od analoghi, sia dal punto di vista dei livelli sanzionatori corrispondenti, prescelti dal legislatore, come dimostra il raffronto, rispettivamente, con il delitto di violazione di domicilio (art. 614 c.p.), con le falsità in documenti pubblici (artt. 476 ss. c.p.), con il danneggiamento comune di cose (art. 635 c.p.), con la truffa (art. 640 c.p.), ecc.

In un secondo gruppo si possono invece considerare tutte quelle altre fattispecie di reato che, per la loro struttura normativa e tecnica di formulazione, già si prestano a sussumere anche le nuove forme di manifestazione o commissione nel *Cyberspace*, senza violare il menzionato divieto di analogia in *malam partem*, dato che le locuzioni normative utilizzate sono idonee a ricomprendere nel loro ambito detti nuovi comportamenti o fatti, pur se non erano certo concepibili al momento dell'emanazione delle relative norme: per cui possono essere denominati "reati cibernetici" in senso ampio.

Gli esempi più chiari sono quelli della diffamazione (art. 595 c.p.), in cui l'offesa alla reputazione altrui può essere certamente commessa "comunicando con più persone" in qualsiasi forma, dunque anche con messaggi nel web; ovvero la già menzionata estorsione (art. 629 c.p.), realizzata con *malware* in grado di criptare dati e programmi di sistemi informatici altrui.

Nel campo dei delitti contro la persona, particolare rilievo possono assumere i delitti di violenza privata (art. 610 c.p.) e di minaccia (art. 612 c.p.), in cui il messaggio che prospetta il "male

tecnologie informatiche: una visione d'insieme, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 81 s. ed ivi ulteriori richiami.

[17] In argomento, sia consentito rinviare per una più analitica esposizione a L. PICOTTI, *Diritto penale e tecnologie informatiche*, cit., p. 33 s., in specie p. 55 s. con ulteriori richiami.

[18] Per un quadro delle fonti sovranazionali in materia si veda R. FLOR, Cyber-criminality: *le fonti internazionali ed europee*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 98 s.

ingiusto" e può perfino "costringere" il soggetto passivo a fare, tollerare od omettere qualcosa, contro la sua volontà, ben può essere veicolate nel web.
Figura più recente in quest'ambito è il delitto di atti persecutori, o *stalking* (art. 612 *bis* c.p.), in cui la condotta reiterata di "minaccia o molestia" ben può essere realizzata con comunicazioni informatiche o nel *Cyberspace*, oltre che con tradizionali mezzi di comunicazione, quali biglietti, lettere, telefonate od anche comportamenti concludenti. Ma la frequenza e la maggior carica di pericolosità del fenomeno, o forse il maggior allarme che suscita la commissione attraverso "mezzi informatici o telematici", ha portato poi lo stesso legislatore ad introdurre la menzionata circostanza aggravante di cui al nuovo 3° comma, per colpire con pena più severa queste ipotesi, considerate più insidiose.
Un elemento importante da sottolineare è che in talune fattispecie il momento consumativo del reato, in cui si concretizza l'offesa del bene giuridico e la piena violazione del diritto fondamentale tutelato dalla norma, si realizza materialmente in capo alla persona fisica, vittima del reato, pur se la condotta sia stata realizzata attraverso le TIC. Questo è il caso del *cyberstalking*, in cui la condotta incriminata di "molestie o minacce", posta in essere attraverso mezzi informatici, deve comunque determinare un effetto reale sulla persona della vittima, in termini di "stato di ansia o di paura" ovvero di "modifica delle abitudini di vita", costituenti gli eventi consumativi che devono essere causati dalle predette condotte poste in essere nel web, a dimostrazione della connessione inscindibile di questo con il mondo reale.
In altre fattispecie, invece, il fatto costitutivo di reato può interamente realizzarsi e consumarsi nel *Cyberspace*, come nel citato delitto di diffusione illecita di immagini o video sessualmente espliciti (nuovo art. 612 *ter* c.p.) o in quello di diffamazione *on-line* (art. 595, 3° comma, c.p.) od ancora di illecita comunicazione o diffusione di dati personali illecitamente acquisiti "su larga scala" (art. 167 *bis*, d.lgs. n. 196/2003 e successive modifiche) [19]: infatti gli effetti prodotti nel *Cyberspace* determinano già di per sé l'offesa della dignità ed identità, ovvero della reputazione, o ancora della *privacy* della vittima, perché è in detta nuova dimensione spaziale, temporale e sociale, in cui si svolge realmente gran parte della vita di tutti, si realizza anche, compiutamente, la conoscenza, l'acquisizione, la divulgazione ulteriore dei contenuti illeciti, lesivi dei diritti altrui.
Analoghe considerazioni valgono per tutti i reati che si concretizzano in una comunicazione o diffusione di contenuti illeciti nel web, come nei delitti di diffusione di materiale pedopornografico (art. 600 *ter*, 3° comma, c.p.) [20], o di rivelazione e diffusione nel web di comunicazioni riservate costituenti corrispondenza elettronica (art. 616, ult. comma, c.p.) o di particolari categorie di dati personali senza il consenso o anzi contro la volontà dell'avente diritto (art. 167 codice *privacy*).

5. Osservazioni conclusive

Le caratteristiche non solo tecnologiche, ma anche – o soprattutto – legate ai correlati comportamenti sociali, indotti nell'odierno mondo globalizzato, rendono evidente l'insidiosità delle nuove forme di criminalità cibernetica, che possono restare anche per lungo tempo occulte e

[19] Su tali nuovi delitti *supra*, nt. 5.

[20] In argomento si veda S. DELSIGNORE, *La tutela dei minori e la pedopornografia telematica: i reati dell'art. 600-ter c.p.*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *op. cit.*, p. 374 s.; volendo, L. PICOTTI, *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in M. BERTOLINO-G. FORTI (a cura di), *Scritti per Federico Stella*, vol. II, Jovene, Napoli, 2007, p. 1267 s.

sfuggire alla stessa tempestiva percezione e, dunque, possibilità di denuncia da parte delle vittime e dei titolari dei beni giuridici aggrediti. D'altro lato, però, le "tracce" elettroniche di detti comportamenti o fatti permangono per lo più in rete e possono essere reperite, raccolte ed acquisite, come prove utilizzabili nel processo penale, da parte di operatori esperti quali, in particolare, sono da noi le sezioni specializzate dalla Polizia postale o altri corpi ed autorità inquirenti.

Certamente la criminalità cibernetica richiede una risposta sempre più sofisticata ed evoluta, via via adeguata alle caratteristiche ed all'evoluzione della tecnologia che la veicola, apparendo indispensabile la convergenza di un'adeguata disciplina processuale, in particolare relativa alle attività di indagine e di raccolta, conservazione ed utilizzazione delle prove, accanto ad un'innovativa disciplina di diritto penale sostanziale, che adeguando via via le formulazioni normative non idonee od introducendo nuove fattispecie specifiche – come ad esempio quella più recente di cui all'art. 612 *ter* c.p. che incrimina il *revenge porn* – renda sicura o più agevole la punizione dei nuovi fenomeni delittuosi.

Altro aspetto peculiare è quello della necessaria presenza ed operatività di autorità pubbliche indipendenti, a partire dal Garante per la protezione dei dati personali, che con una specifica competenza tecnica e giuridica possano far fronte alle esigenze di tutela non solo degli interessi collettivi e pubblici che vengono in rilievo, ma anche dei diritti fondamentali delle singole persone, che gli stessi interessati non potrebbero essere in grado di assicurare pienamente, proprio per l'asimmetrica posizione di debolezza in cui si trovano, rispetto alle potenzialità, complessità, difficoltà di governo dello spazio cibernetico in cui pur devono partecipare.

È dunque compito del giurista, ed in particolare del penalista, adeguare le proprie conoscenze non solo normative, ma anche tecniche, indispensabili per cogliere la nuova dimensione, con cui ci si deve ormai confrontare, affinché possa essere garantita effettiva tutela, anche attraverso lo strumento estremo della sanzione penale, ai diritti fondamentali delle vittime offese dai reati menzionati, oltre che delle stesse persone indagate ed imputate nei relativi procedimenti penali, che devono svolgersi nel rispetto di garanzie processuali corrispondentemente adeguate alle nuove tecniche di indagine, fin dal momento della ricerca, acquisizione e raccolta delle prove elettroniche e della loro successiva utilizzazione nel giudizio o comunque nella decisione finale.