Omnia

Trattati giuridici

# CYBERCRIME

diretto da
Alberto Cadoppi, Stefano Canestrari,
Adelmo Manna, Michele Papa

UTET
GIURIDICA

Composizione: Integra Software Services Pvt.Ltd

Finito di stampare nel mese di gennaio 2019
dalla L.E.G.O. S.p.A.
Viale dell'Industria, 2 - 36100 - Vicenza

# SOMMARIO

**Capitolo II – Il cyberterrorismo di matrice religiosa**
*di Stefano Dambruoso con la collaborazione, in fase di ricerca, della Dott.ssa Ludovica Purini e dell'Avv. Guido Di Donato*



**Capitolo III – L'istigazione a delinquere via web**
*di Michele Boggiani*



**Capitolo IV – L'Istigazione a pratiche di pedofilia e di pedopornografia**
*di Michele Boggiani*

**Capitolo II – L'evoluzione delle categorie tradizionali: il documento informatico**
*di Paolo Tonini*



**Capitolo III – La prova informatica e il mancato rispetto della *best practice*: lineamenti sistematici sulle conseguenze processuali**
*di Carlotta Conti*



**Capitolo IV – La convenzione di Budapest del 2001 e la L. n. 48/2008**
*di Stefano Aterno*

# Capitolo II

## DIRITTO PENALE E TECNOLOGIE INFORMATICHE: UNA VISIONE D'INSIEME

*di Lorenzo Picotti*

La rivoluzione tecnologica, o meglio "cibernetica", ha avuto un forte impatto sui rapporti sociali e giuridici, determinando in circa mezzo secolo profondi cambiamenti anche per il diritto penale. Il primo elemento di novità, avente forti ricadute sull'ordinamento giuridico, è costituito dall'automazione, che ha via via sostituito porzioni progressivamente più estese ed importanti delle attività dell'uomo, come è riconosciuto anche nelle definizioni giuridiche di "dati" e "sistemi informatici" contenute nelle fonti sovranazionali. L'apertura di Internet al pubblico a metà degli anni '90 dello scorso secolo ha poi trasformato le reti di comunicazione in una dimensione globale, che grazie anche ai dispositivi mobili ed all'estensione delle coperture di connessione, rappresenta oggi uno "spazio" di costante comunicazione e scambio, il c.d. *Cyberspace*, nel quale si dislocano sempre più attività individuali e collettive di ogni tipo, dal tempo libero, al commercio, dall'economia, alla cultura, fino alla politica. In tale spazio cibernetico gli utenti possono essere al contempo autori e vittime di reati e di comportamenti illeciti, per la struttura interattiva che la Rete ha via via assunto e la crescente estensione ed importanza dei contenuti e dei dati da essi stessi caricati, diffusi e scambiati, che vengono memorizzati, elaborati e gestiti su piattaforme informatiche e reti sociali da sistemi esperti e motori di ricerca sempre più potenti, determinando una progressiva concentrazione di poteri in capo agli *Internet Service Provider* (ISP) che li controllano. Il riflesso immediato di questa "rivoluzione cibernetica" sul diritto penale è rappresentato dal passaggio dal concetto di *Computer crime* a quello di *Cyebrcrime*, di cui va sottolineata l'espansione crescente. Accanto ai "reati informatici in senso stretto" – che sono connotati dalla previsione, nella fattispecie legale, di specifici elementi di tipizzazione, contenenti un esplicito riferimento alle nuove tecnologie dell'informazione o della comunicazione (c.d. TIC), siano essi relativi alla condotta od ai mezzi, alle modalità o agli effetti o ad ogni altro elemento essenziale o circostanziale – sono oggi commissibili tramite o a danno di sistemi e strumenti informatici o, comunque, "nel" *Cyberspace*, reati di ogni altro tipo, i cui elementi costitutivi o circostanziali, in via alternativa od interpretativa, consentano in ogni caso di sussumerli nelle rispettive fattispecie legali: per cui può parlarsi di "reati informatici in senso ampio", oggi pressoché assorbiti nella più estesa categoria dei "reati cibernetici", a loro volta distinguibili fra quelli "in senso stretto" (ad es. il c.d. *cyberstalking*) ed "in senso ampio", a seconda che la commissione in Rete sia elemento espresso o solo interpretativamente compatibile con la

fattispecie legale (come si riscontra nei casi più frequenti di diffamazioni *on-line*, di diffusione di materiale pedopornografico, di istigazione alla discriminazione ed all'odio razziale, di estorsioni, di riciclaggio, di molte fattispecie di violazioni della *privacy* e dei diritti d'autore, ecc.).
Anche la collocazione sistematica di queste diverse categorie di reati informatici e cibernetici, ormai ampiamente presenti nel codice penale e nella legislazione speciale (in specie in materia di protezione dei dati personali e di diritti d'autore), evidenzia la grande varietà ed importanza dei beni giuridici protetti, che presentano peraltro, nella nuova dimensione cibernetica, specifici profili di novità.
In questo contesto, la disciplina restrittiva della responsabilità, anche penale, degli ISP, risalente alla Direttiva europea sul commercio elettronico del 2000, appare ampiamente inadeguata, stante il descritto sviluppo del *Cyberspace* e le crescenti esigenze di efficace protezione di diritti fondamentali della persona e di molteplici interessi giuridici dei singoli e della collettività che in esso emergono, come del resto dimostra l'evoluzione della giurisprudenza in materia, in particolare di quella europea sia della Corte di Strasburgo, sia della Corte di Lussemburgo.
In conclusione si prospetta la necessità di una profonda revisione di alcune fondamentali categorie dogmatiche, su cui si fonda la responsabilità penale, a partire da quelle di "azione" e di "evento" nel *Cyberspace*, alla luce dell'automazione, della dematerializzazione, dell'interazione fra utenti e con gli ISP, della diffusione e permanenza nel tempo e nello spazio degli effetti di ogni attività dell'uomo che vi si svolge, con importanti ricadute anche pratiche sulle regole d'imputazione oggettiva e soggettiva, sulla determinazione del momento e del luogo di consumazione ovvero di "esaurimento" del reato, sulla rilevanza penale di comportamenti anche successivi alla "formale perfezione" della fattispecie, che possono determinare la (cor)responsabilità penale di altri utenti, di terzi, degli stessi ISP, la cui categoria è oggi così ampia e diversificata, da esigere una nuova disciplina che ne differenzi il ruolo e le responsabilità, secondo criteri più adeguati rispetto a quelli adottati all'inizio del nuovo millennio.

RIFERIMENTI NORMATIVI: artt. 270-*ter*, 270-*quinquies*, comma 2, 392, 491-*bis*, 495-*bis*, 615-*ter*, 615-*quater*, 615-*quinquies*, 612-*bis*, comma 2; 616, 617-*quater*, 617-*quinquies*, 617-*sexies*, 621, comma 2, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*, 640-*ter*, 640-*quinquies* c.p.; L. 23.12.1993, n. 547; D.Lgs. 30.6.2003, n. 196 e succ. mod. (da ultimo con D.Lgs. 10.8.2018, n. 101); L. 8.3.2008, n. 48.

SOMMARIO: **1.** La rivoluzione tecnologica ed il suo impatto sui rapporti sociali e giuridici. – **1.1.** Mutamenti indotti dallo sviluppo tecnologico e "rivoluzione" cibernetica. – **1.2.** Dalla Rete al *Cyberspace*. – **1.3.** Reciprocità di condizionamento fra realtà cibernetica e diritto. – **2.** Rilevanza giuridico-penale dell'*automazione* quale "sostituzione" (parziale) dell'attività e del controllo dell'uomo. – **3.** Il passaggio dai *Computer crime* ai *Cybercrime*. – **4.** Il *web* interattivo ed il doppio ruolo degli utenti quali possibili autori e vittime di reati cibernetici. – **5.** Tecniche di tipizzazione dei reati informatici e cibernetici e relative partizioni classificatorie. – **5.1.**

Nuove condotte, estensioni "analogiche", nuovi oggetti materiali. – **5.1.1.** Nuove condotte e nuovi "fatti" di reato: le fattispecie paradigmatiche della frode informatica e dell'accesso abusivo. – **5.1.2.** Estensioni per "analogia" legislativa di fattispecie preesistenti a nuovi oggetti "materiali" e relative modalità di condotta. – **5.2.** Collocazione sistematica e beni giuridici protetti. – **5.3.** Partizioni dei reati informatici e cibernetici. – **5.3.1.** I reati informatici in senso stretto. – **5.3.2.** I reati informatici in senso ampio. – **5.3.3.** Reati cibernetici. – **6.** Obblighi di tutela penale degli *Internet Service Providers* e sviluppi della giurisprudenza europea. – **6.1.** Giurisprudenza CEDU. – **6.2.** Giurisprudenza CGUE. – **7.** Osservazioni conclusive: verso un mutamento di nozioni basilari quale quella di consumazione del reato nel *Cyberspace*?

## 1. La rivoluzione tecnologica ed il suo impatto sui rapporti sociali e giuridici

Il rapporto fra il diritto penale e le tecnologie informatiche (con cui per brevità si deve intendere l'ampia nozione, corrente nella terminologia internazionale, di nuove "tecnologie dell'informazione e della comunicazione": c.d. TIC, in inglese ICT) è da meno di mezzo secolo, anche a voler guardare oltreoceano[1], all'attenzione della dottrina e della giurisprudenza, che rappresentano il primo fronte d'impatto di ogni mutamento nei comportamenti, nei rapporti e nelle condizioni sociali rilevanti per l'applicazione del diritto vigente, non solo penale.

Mutamento, o meglio mutamenti, riconducibili alle TIC, che da allora hanno impegnato anche i più autorevoli organismi internazionali (dall'OCSE, al Consiglio d'Europa, fino all'Unione europea per restare in ambito continentale; ma anche il WTO, l'ONMPI, il G8, le Nazioni Unite, per estendere lo sguardo a livello globale)[2] e poi i legislatori di quasi tutti i paesi occidentali, quindi via via anche degli altri continenti[3], che sono intervenuti – spesso in modo disorganico

[1] Nella sterminata letteratura statunitense basti il rinvio al quadro storico e sistematico, di diritto penale sostanziale e processuale, offerto da Kerr, *Computer Crime Law*, Thomson West, St. Paul MN, 2006 ed alla normativa anche statale, bibliografia nonché giurisprudenza ivi richiamata. Tradizionalmente si considera quale punto d'avvio del dibattito dottrinale il volume di Parker, *Crime by Computer*, New York, 1976.

[2] Per un quadro d'insieme Sieber (ed.), *Information Technology Crime. National Legislation and International Initiatives*, Carl Heymanns Verlag, Köln, Berlin, Bonn, München, 1994, che raccoglie gli atti del Colloquio preparatorio tenutosi a Würzburg del XV Congresso Internazionale di Diritto penale organizzato dall'AIDP e svoltosi a Rio de Janeiro dal 4 al 10.9.1994, la cui II sezione era dedicata alla criminalità informatica. La risoluzione finale approvata è pubblicata in *Revue int. droit pénal*, 1994, 1; nonché, in traduzione italiana, con un commento volendo dei lavori della Sezione, in Picotti, *Le "Raccomandazioni" del XV Congresso Internazionale di Diritto penale in tema di criminalità informatica*, in *Riv. trim. dir. pen. economia*, 1995, 1279.

[3] Per un quadro comparato a livello globale delle diverse legislazioni cfr. già Sieber, *The International Handbook on Computer Crime. Computer-related Economic Crime and the Infringements of Privacy*, John Wiley & Sons, New York, Brisbane, Toronto, Singapore, 1986.

– ad "ondate" successive, a seconda delle diverse urgenze, condizioni politiche, culturali e di sviluppo tecnologico.

Un arco di tempo di relativamente pochi anni, rispetto alla storia plurisecolare del diritto penale.

Ma i mutamenti si stanno imponendo con una crescente forza ed inevitabile attenzione, non solo del legislatore e della magistratura, ma anche dei settori più tradizionalisti della dottrina penale, che si erano mostrati inizialmente indifferenti, se non apertamente scettici, circa la rilevanza ed autonomia di questo nuovo campo del diritto, da taluni visto addirittura quale frutto di tendenze arbitrariamente "espansionistiche" del legislatore nazionale ed ancor più europeo. Oggi, viceversa, emerge un esteso riconoscimento che esso merita non solo specifiche analisi ermeneutiche, ma anche un'adeguata elaborazione teorica e sistematica.

### *1.1. Mutamenti indotti dallo sviluppo tecnologico e "rivoluzione" cibernetica*

A tal fine occorre andare oltre un approccio che si potrebbe definire minimalista, secondo cui si dovrebbe individuare e trattare di un mero ramo "speciale" del diritto (penale e processuale, per quanto interessa), per assumere invece la consapevolezza di una prospettiva necessariamente nuova e diversa, da cui riguardare l'*intero* sistema penale (oltre che giuridico in genere), a partire certamente dalle nuove norme specificamente introdotte e dalla casistica concretamente emergente in sede applicativa per contrastare i fenomeni in esame, ma da leggere quali sintomi di un rivolgimento ben più profondo ed esteso, da riportare alla dinamica dei complessi rapporti fra diritto, sviluppo tecnologico e forme di organizzazione del sistema e dei rapporti sociali, con tutte le conseguenti ricadute anche sulla teoria generale del diritto[4] e, per quanto di competenza, del reato.

In altre parole, a quella che si deve definire "rivoluzione informatica" o, meglio – come si dirà *infra* § 1.2. – "cibernetica", si deve riconoscere un'importanza strutturale o, se si preferisce, strategica per l'evoluzione del diritto, non solo penale, in quanto rappresenta la frontiera più avanzata dell'innovazione e del cambiamento nell'odierna società globalizzata, avendo già determinato, e quotidianamente determinando un esteso e prolungato impatto sulle forme ed i modi di essere dei rapporti sociali, economici, politici, culturali, fino a quelli interpersonali e privati, che va dal loro instaurarsi, svilupparsi, articolarsi, fino al loro estinguersi.

[4] Oltre al capitolo introduttivo di Pagallo, *Profili tecnico-informatici e filosofici*, in questo volume, cfr. in specie Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014, soprattutto 61 s.; nonché Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.

Dunque, una "frontiera mobile" indicativa di future tendenze, con inesplorate potenzialità di ulteriore capillare incidenza, che già sono prefigurate dagli sviluppi dell'intelligenza artificiale e della robotica.

Si deve parlare di "rivoluzione" proprio perché il fenomeno investe ogni sfera della vita e degli interessi delle persone e della collettività, andando ben oltre la modificazione e dilatazione – comunque già di per sé straordinarie – delle modalità dell'informazione, della comunicazione e dello scambio delle conoscenze e dei saperi dell'umanità, tendenzialmente resi accessibili a chiunque, a qualsiasi distanza ed in qualsiasi luogo e momento.

La "rivoluzione" coinvolge lo stesso modo di essere e di svolgersi della vita privata, non meno di quella pubblica, dell'economia e del lavoro, della produzione e del commercio, della politica e della stessa democrazia, come è dimostrato dal fatto che per tutti questi ambiti si può stabilire, con una certa precisione, un "prima" ed un "dopo" rispetto ad essa.

Tale rivoluzione ha inevitabilmente determinato anche *nuovi* conflitti ed in specie, per quanto rileva in questa sede, reso possibili anche *nuovi* comportamenti illeciti, che violano o minacciano gravemente i diritti e gli interessi di persone, gruppi, collettività, meritevoli di protezione giuridica. Ma al contempo la rivoluzione informatica (e/o "cibernetica") ha altresì fatto sorgere *nuovi* interessi meritevoli di riconoscimento e di protezione giuridica, anche penale, come si vedrà, e dunque "nuovi diritti", compresi taluni fondamentali, da affiancare a quelli tradizionali, come ha evidenziato la più attenta ed avanzata dottrina[5]. Ed ha aperto altresì nuove tecniche, modalità, strategie di reazione e di tutela, che vanno anche al di là del campo strettamente giuridico.

Accanto alle nuove forme di prevaricazione e di soggezione[6], correlate a concentrazioni straordinarie di poteri e di corrispondenti forze e capacità di intimidazione, di controllo, di condizionamento delle informazioni, della volontà e delle scelte delle singole persone e dei gruppi sociali[7], si sono sviluppate e si

[5] Cfr. Rodotà, *Il mondo*, cit.

[6] Sul "controllo dentro le tecnologie" cfr. in specie Ziccardi, *Internet*, cit., 115 s.

[7] Basti richiamare i recenti colossali scandali che hanno riguardato i dati degli utenti di Facebook, non solo acquisiti in enormi quantità da *Analytica Cibernetica*, ma anche da case produttrici di smartphone o di gestione di carte di credito. Come è stato scientificamente dimostrato, la progressiva estensione delle connessioni, delle utenze e dunque della correlata accumulazione di dati prodotti e raccolti, ha un effetto moltiplicatore esponenziale, perché porta a preferire inevitabilmente, e sempre più, le aziende top di settore, che gestiscono la maggior quantità di informazioni e di connessioni ed offrono così i servizi *quantitativamente* più performanti: con l'effetto di una progressiva concentrazione in capo ad esse, che porta a restrizioni della concorrenza, fino a condizioni di tendenziale monopolio, come dimostrano in modo manifesto nei rispettivi campi anche l'espansione di Google, che ha assorbito *YouTube* nelle bacheche video e musicali, di Amazon, che domina il mercato globale delle vendite online, di Facebook, che ha

sviluppano nuove forme di aggregazione, di condivisione, di partecipazione, che utilizzano le inedite possibilità di incontro, scambio, creazione di "comunità" e gruppi di interessi, con obiettivi e valori comuni, che parimenti consentono la rapidissima circolazione e condivisione di informazioni, nonché estensione di iniziative per interventi, azioni collettive, espressioni di dissenso, solidarietà, ecc. ai più diversi livelli, in una dimensione parimenti globale, accessibile ai singoli ed alle aggregazioni sociali, in termini e tempi prima del tutto sconosciuti ed inimmaginabili.

Mentre nel campo più strettamente penale, accanto alle nuove forme di criminalità informatica o che, più in generale, nasce e si manifesta nella Rete a livello globale (che si può quindi a sua volta definire "criminalità cibernetica" come meglio si preciserà *infra* § 3), sorgono e si perfezionano nuove e penetranti tecniche d'indagine, di ricerca e di raccolta delle prove, con l'applicazione di strumenti tecnologicamente avanzati, che hanno capacità d'azione e potenzialità di sviluppo non meno impressionanti.

### *1.2. Dalla Rete al* Cyberspace

Di fronte a tali sviluppi, il concetto stesso di "Rete" o *web* – sia pur con la Erre maiuscola, e cioè Internet quale "rete delle reti" – appare oggi, se vogliamo, riduttivo, perché allude di per sé alla sola dimensione tecnica e materiale (di cavi, fibre ottiche, apparati di trasmissione e ricezione, snodi, router, connessioni, server, memorie, ecc. che operano con sempre più potenti e sofisticati elaboratori, processori, *software*, protocolli di comunicazione e di condivisione, ecc.), la quale costituisce certamente l'indispensabile supporto o "struttura" fisica che è alla base ed origine dei fenomeni richiamati, ma non coglie la profondità e complessità della ben più ampia dimensione sociale ed umana dell'insieme, che attraverso le nuove tecnologie informatiche (TIC) si svolge e si sviluppa – in particolare grazie all'espandersi dell'*automazione* ad ogni livello: cfr. *infra* § 2 – meglio esprimibile con l'idea di *Cyberspace* (o Cyberspazio).

Tale concetto associa, infatti, la "cibernetica" (termine derivato dal greco *kyber*, timoniere o pilota, scelto agli inizi del secolo scorso per indicare una nuova scienza, che intendeva studiare i meccanismi con cui uomini, animali e

assorbito nella messaggistica *Whats App*. Significative sono anche le sanzioni inflitte a Facebook, e più recentemente a Google dalla Commissione europea per abuso di posizione dominante (quest'ultima per l'imposizione del sistema Android – utilizzato, secondo stime attendibili, dall'80% degli *smartphone* in circolazione nel pianeta – ai produttori di telefonia mobile, con un pacchetto di applicazioni preinstallate che offrono motori di ricerca e browser di Google, nonché la gestione in generale di aggiornamenti e installazione di nuove *app* attraverso il negozio virtuale *Play Store* sempre riconducibile a Google).

macchine *comunicano* con l'ambiente esterno e lo *controllano*)[8] alla nozione pluridimensionale e dinamica, non meramente lineare, di "spazio" – impropriamente detto "virtuale" – che appare più idonea a rappresentare l'estensione pervasiva del nuovo mondo, nel quale, singolarmente e collettivamente, siamo tutti *realmente* (non solo "virtualmente") immersi, in quanto ormai permanentemente connessi ed interagenti, se non anche dipendenti. Proprio grazie allo sviluppo delle TIC, ad esempio, oggi disponiamo di sempre più sofisticati, potenti ed inseparabili dispositivi *mobile* (dagli *smartphone*, ai *tablet*, ai *laptop*, ecc.), in grado di operare e collegarsi ovunque nel *web*, grazie alla copertura tendenzialmente integrale delle reti di comunicazione di dati ed alla molteplicità delle tecniche di connessione ad Internet (dall'ADSL al WiMax, dalla fibra ottica al satellitare), di cui è emblematica la proliferazione in ogni ambiente pubblico e privato dell'offerta di connessioni *wi-fi*, per garantirci in ogni caso un *permanente* accesso e dunque la stabile "presenza" ed operatività, da qualsiasi luogo e momento, in detto *Cyberspace*.

Abbiamo così sempre a disposizione dei veri *alter ego*, che espandono non solo la nostra memoria, ma anche le nostre capacità di azione, interazione e scambio, oltre che d'informazione e di comunicazione: possiamo infatti acquisire istantaneamente i contenuti delle notizie giornalistiche o delle previsioni meteorologiche dai siti più consoni ai nostri orientamenti o alle nostre esigenze, culturali, spaziali e temporali; disporre delle nuove enciclopedie del sapere umano, in ogni suo ramo, cui concorrono permanentemente schiere di scienziati, esperti, o semplici appassionati, ai quali possiamo anche aggiungerci; accedere all'ubiquo *cloud*, in cui teniamo a disposizione, scambiamo o condividiamo ogni genere di file, compresi video ed audio, anche di grandi dimensioni; esplorare i più reconditi spazi del *deep web* o perfino del *dark web*[9], ma anche più comunemente acquistare e vendere legittimamente qualsiasi merce o bene, sia nuovo che usato, progettare e realizzare iniziative, da soli o con altri, agire, partecipare, resistere

[8] Il termine "cibernetica" fu coniato dal matematico Norbert WIENER – di cui si veda in tr.it. (a cura di Persiani), *Introduzione alla cibernetica. L'uso umano degli esseri umani* (1953), Torino, 1970 – che lo derivò dalla parola greca *kyber*, che significa "timoniere o pilota". La cibernetica studia i meccanismi con cui uomini, animali e macchine comunicano con l'ambiente esterno e lo controllano. Si tratta di una scienza multidisciplinare con forti interazioni con molte altre discipline ed aree tecnologiche: filosofia, psicologia, matematica, biologia, fisica, intelligenza artificiale, teoria dei controlli, teoria delle comunicazioni, robotica.

[9] Sui concetti di *deep web* (parte del *web* non indicizzata dai motori di ricerca, perché non accessibile, né esplorabile dai comuni *browser*) e *dark web*, che ne è la parte più "oscura", costituita da "reti oscure" che si raggiungono attraverso specifici software, configurazioni e accessi autorizzativi, in cui si svolgono frequentemente attività illecite, per le tecniche di anonimizzazione che mascherano la provenienza, basti qui il rinvio alle corrispondenti voci in *WikipediA*.

anche nei processi giudiziari e nei procedimenti amministrativi di ogni tipo e natura, via via informatizzati, entrare ed operare nelle reti sociali che ci avviluppano e risucchiano, nelle catene *peer to peer* in cui si può condividere qualsiasi contenuto e valore, dalla musica, ai film, ai materiali illeciti, fino alla disponibilità delle nuove valute c.d. virtuali (quali *bitcoin*, *ethereum*, ecc.), prodotte e validate solo da *blockchain* al di fuori del controllo (e della garanzia) di autorità monetarie emittenti e di regolazioni giuridiche statali (almeno per ora)[10]. Tutto diviene *electronic* o *digital*, dall'*e-commerce*, alla *digital economy*, dall'*e-tourism*, all'*e-art*, e così via.

Questa così complessa realtà, in perenne evoluzione ed espansione, ha determinato e determina ovviamente molteplici e talora deflagranti impatti sul diritto vigente, non solo penale.

### *1.3. Reciprocità di condizionamento fra realtà cibernetica e diritto*

Schematizzando al massimo, da un lato l'evoluzione tecnologica e la rivoluzione cibernetica stimolano ed anzi impongono l'adeguamento costante del diritto, indispensabile perché possa abbracciare, quale suo oggetto, i nuovi fenomeni e perpetuare la propria capacità e funzione regolatrice, ricorrendo a tutto l'armamentario di strumenti di cui dispone: dall'interpretazione evolutiva, all'applicazione analogica, seppur "indicibile" e necessariamente mascherata nella materia penale; dalla modifica o creazione legislativa di nuove norme, all'elaborazione di inedite categorie concettuali e dogmatiche.

Dall'altro lato, come ogni realtà strutturale che condiziona le sovrastrutture, la rivoluzione cibernetica modifica e ridetermina il suo stesso rapporto con il diritto, toccandone le funzioni e il modo di operare, per taluno ponendo a rischio proprio il suo nucleo essenziale, se non l'esistenza, in quanto la tecnologia sembra in grado di porsi in concorrenza o conflitto con la sua primaria funzione *normativa*: il "codice tecnico" si presenta con la pretesa di essere il nuovo codice giuridico – "*Code is Law*", per citare il famoso libro di Lawrence Lessig[11] – l'autotutela tecnologica e l'autoregolazione dei signori del *web* tende a divenire diritto od a sostituirlo, perché realmente ed immediatamente si applica od "autoapplica", configurando in tempo reale nuovi precetti muniti di relative ed efficaci sanzioni, compresa quella più drastica dell'esclusione da servizi, reti e connessioni, così

[10] Su alcuni profili di rilevanza penale connessi all'utilizzo delle valute virtuali sia consentito rinviare a Picotti, *Profili penali del* Cyberlaundering*: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. economia*, 2018 (in corso di pubblicazione).

[11] Lessig, *Code and Other Laws of Cyberspace* (1999), 2ª ed., Basic Books, New York, 2006.

da regolare, prepotentemente, i comportamenti degli utenti, dei concorrenti, dei terzi[12].

Da tempo è del resto palese l'infondatezza dell'utopistica o romantica idea di una "rete" quale spazio libero dal diritto[13], quale porto franco di anarchia e di totale libertà, non limitabile dai poteri degli Stati ancorati alla materialità dei loro territori e dei loro confini geografici, entro cui soltanto si potrebbe esercitare la sovranità. E si sono presto toccate con mano o sofferte come vittime – da parte di singoli individui od aziende, di enti di ogni genere o di strutture amministrative anche statali, comprese le più delicate – le nuove insidie della criminalità informatica e cibernetica, le nuove forme di aggressione ed offesa, talora conclamate e clamorose, talora occulte e silenti, riconducibili non solo ai cyber-criminali, ma anche alle nuove concentrazioni di poteri, legittimi ed illegittimi, formatesi nel *web*, che attentano ai diritti ed agli interessi individuali e sociali, non meno meritevoli di protezione giuridica, ed anzi ancor più bisognosi di efficace tutela, anche penale, proprio perché si collocano o proiettano nel *Cyberspace*.

Tanto che è già stata autorevolmente promossa e condivisa l'esigenza di un *Internet Bill of Rights*, di una "Costituzione per Internet"[14], vale a dire di un sistema di diritti fondamentali da riconoscere e garantire su scala globale, a partire dalla "rilettura" dell'insieme di quelli contenuti nelle Carte e Convenzioni

[12] Nell'esperienza quotidiana di ogni utente della rete, ci si imbatte costantemente nelle "opzioni chiuse" proposte dai gestori dei più diffusi servizi di messaggistica e di reti sociali, quali Facebook, Whats App, Instagram, ovvero *app* di ogni tipo, in base alle quali o si accettano, nei periodici aggiornamenti, le nuove "regole" e condizioni, non solo di comunicazione e configurazione dei servizi, ma anche di acquisizione e trattamento dei dati personali, compresa la possibile comunicazione a terzi, interconnessione, elaborazione per finalità di vario tipo, comprese quelle commerciali e di offerte pubblicitarie "personalizzate", o si è esclusi dalla fruizione delle *app*, dei servizi e/o dalla stessa rete sociale, in cui peraltro ormai sono dislocati tutti o la gran parte dei propri rapporti personali, professionali, sociali, per cui non è sostanzialmente possibile recedere ed è necessitato esprimere il "consenso" (con un semplice click!) alle nuove condizioni e modifiche, così di fatto "imposte".

[13] Per un'attenta esposizione sul tema basti qui il rinvio a Ziccardi, *Hacker. Il richiamo della libertà*, Milano, 2011, con ampi richiami casistici e bibliografici, specie all'esperienza americana.

[14] A partire dalla "*Internet Magna Carta*" di Tim Berners Lee e dallo studio del "Berkman Center" dell'Universitá di Harvard, si sono sviluppati a livello internazionale molteplici iniziative, fra cui i lavori dell'"*Internet Governance Forum*" e la "*Dynamic Coalition on Internet Rights and Principles*", ai quali si richiamano anche quelli svolti a livello nazionale dalla Commissione di studio presieduta da Stefano Rodotà, istituita dalla Presidenza della Camera dei Deputati del Parlamento italiano nel 2014, che ha presentato il 28 luglio 2015 una concisa, ma efficace "Dichiarazione dei diritti in Internet" (composta da un Preambolo e 14 articoli in cui sono riconosciuti altrettanti diritti), leggibile al sito *www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015* (ma ivi reperibile anche in numerose altre lingue).

internazionali, come elaborati dalle Corti e comunque via via applicati alla nuova dimensione sociale qui in esame[15].

Di fronte alla necessità di garantire un'effettiva e possibilmente equivalente tutela di questi diritti ed interessi a livello non solo nazionale o regionale, bensì globale, s'impone l'esigenza di rendere operativi sistemi "armonizzati" d'incriminazioni e sanzioni, se occorre anche penali, per condividere ed estendere buone ed efficienti prassi applicative, rafforzando la sempre più necessaria cooperazione a livello internazionale, che deve coinvolgere, oltre i singoli ambiti statali, anche il mondo dell'industria e delle diverse parti interessate, compresi enti ed associazioni esponenziali di interessi collettivi e diffusi.

Il criterio basilare deve essere che ciò che è illecito *off line* non può essere lecito *on line*, anche se si presenta in nuove ed inimmaginate modalità e forme. E tale principio deve trovare adeguati mezzi per rendersi effettivo, muovendo da una chiara individuazione di quello che ne è oggi l'oggetto, vale a dire delimitando giuridicamente, secondo detto criterio, i *contenuti* ed i *comportamenti* illeciti nel *Cyberspace*.

A tal fine la disciplina penale deve profondamente riplasmarsi ed adattarsi, riconoscendo la novità e complessità dei rapporti che si svolgono nel *Cyberspace*, non essendo adeguato un approccio "conservatore", secondo cui ogni questione sarebbe risolvibile con la mera estensione ermeneutica o concettuale, ai fenomeni nuovi, delle norme vigenti e delle categorie dogmatiche tradizionali.

Come dimostra anche l'esperienza dell'ordinamento italiano, non basta per contrastare efficacemente tali nuove minacce la perenne rincorsa legislativa, oltre che giurisprudenziale, diretta a colmare le lacune che di volta in volta si presentano nella prassi, moltiplicando le fattispecie penali con nuove incriminazioni, introducendo singole circostanze aggravanti[16], operando estensioni o adattamenti in via ermeneutica, che non consentono – in assenza di una sistematica visione d'insieme – di superare incertezze applicative e contrasti interpretativi, nascenti dai fenomeni nuovi[17].

Si palesa, dunque, la necessità di delineare un quadro giuridico generale, in cui collocare anche rinnovati criteri e regole d'imputazione della responsabilità penale, adeguati alla nuova realtà, definendo più chiaramente quali siano i con-

[15] Cfr. Rodotà, *Il mondo*, cit., 61 s., 69 s.; per la giurisprudenza delle Corti europei cfr. *infra* § 6.

[16] Si possono citare quali esempi le circostanze aggravanti introdotte per i delitti di frode informatica (art. 640-*ter*, nuovo comma 3, c.p.), di atti persecutori (art. 612-*bis*, nuovo comma 2, c.p.), di addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinquies*, nuovo comma 2, c.p.), su cui si tornerà *infra* § 5.2.

[17] Per un quadro paradigmatico in materia di protezione penale dei diritti e beni giuridici della persona sia consentito rinviare a Picotti, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Id. (cur.), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 29 s.

notati dei comportamenti e dei "fatti" penalmente rilevanti, che si commettono o manifestano nel *Cyberspace*, rispetto ai quali si impone o giustifica la previsione ed applicazione di sanzioni penali. Occorre, più in particolare, tener conto delle peculiari caratteristiche tecniche ed umane, che acquistano le "azioni" dei singoli o di gruppi, nel momento in cui si smaterializzano, interagiscono ed espandono nel *Cyberspace*. E riconoscere che nella nuova dimensione del *web* sono da esse coinvolte pluralità di soggetti e di strutture, operanti ed interdipendenti fra loro, con rilevanti e differenti funzioni: mentre gli "utenti" diventano sempre più anche autori di contenuti diffusi in rete, i destinatari delle comunicazioni interattive, nell'ambito delle reti sociali, reagiscono con approvazioni, preferenze, dissensi variamente espressi o modulati, che si concatenano fra loro; i partecipi di comunità virtuali o gruppi sociali convergono con i titolari di siti od intrecciano interventi con i vari *blogger*, mentre si espande e diversifica radicalmente la mutevole categoria degli *Internet Service Providers* (ISP, di cui si dirà *infra* § 6), di cui diviene difficile identificare il denominatore comune.

Nel contempo, si evidenzia anche la necessità ed urgenza di specifiche regole processuali, relative in particolare alle tecniche di ricerca, raccolta, validità ed utilizzabilità delle prove informatiche o, come tradizionalmente si dice, "elettroniche", nonché alle misure cautelari adottabili per acquisirle ovvero per porre fine agli effetti dannosi ed al protrarsi degli illeciti, salvaguardando in ogni caso i diritti fondamentali in tali inedite situazioni d'intervento delle autorità inquirenti e repressive.

Per queste molteplici ragioni il *novum* dell'evoluzione tecnologica ed, in specie, della rivoluzione cibernetica – proiettata a produrre ulteriori profondi cambiamenti sociali soprattutto in relazione ai menzionati sviluppi applicativi dell'intelligenza artificiale e della robotica – va pienamente riconosciuto e consapevolmente valorizzato sul piano giuridico-penale, per poter assicurare, di fronte all'indiscutibile necessità d'incisive riforme, l'esigenza parimenti primaria di consolidare i connotati ed i principi garantistici dello Stato di diritto in una società democratica, che non può abdicare dalla propria funzione regolatrice e quando occorre sanzionatoria, di fronte al "codice tecnico" ed alla regolazione "di fatto" dei rapporti di forza nel *Cyberspace*.

## 2. Rilevanza giuridico-penale dell'*automazione* quale "sostituzione" (parziale) dell'attività e del controllo dell'uomo

Per un corretto inquadramento giuridico occorre muovere dalla prima *qualità tecnica*, specifica dell'informatica, che interessa il penalista (ed il giurista), costituita dall'*automazione* dei trattamenti o processi di elaborazione dei dati, secondo *programmi* specifici, che consentono di pervenire, con l'esecuzione di appositi ed

evoluti algoritmi, a risultati *complessi* e straordinariamente più *precisi*, in tempi infinitamente più *rapidi* rispetto a quelli conseguibili con l'attività dell'uomo in carne ed ossa. Con l'"informatizzazione" l'uomo è *sostituito* in ambiti ed aspetti sempre più estesi ed articolati del suo agire, individuale e sociale, comprese in particolare le sue funzioni di acquisizione e memorizzazione di nuove informazioni, nonché controllo e svolgimento di attività sempre più articolate ed interdipendenti: dalla gestione di modelli previsionali in ogni settore, all'organizzazione della produzione e del lavoro, dalla selezione e gestione della pubblicità da indirizzare ad estese categorie od a singoli utenti (c.d. personalizzazione) a livello globale, fino alle ricerche statistiche, epidemiologiche, d'opinione o perfino alle diagnosi mediche, alla microchirurgia, od alla guida automatizzata di veicoli di ogni natura, comprese oggi le automobili, ecc.

Tale basilare connotato qualitativo dell'*automazione* filtra anche nelle definizioni *giuridiche* contenute nelle principali fonti sopranazionali, comprese quelle dirette a rafforzare ed armonizzare la risposta penale alla criminalità informatica ed ai *Cybercrime*.

Basti menzionare l'art. 1 della Convenzione *Cybercrime* del Consiglio d'Europa del 23.11.2001 e l'art. 2 della Direttiva 2013/40/UE del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione[18], che sostituisce (peraltro senza modifiche sul punto) la decisione quadro del Consiglio 2005/222/GAI.

Il *novum* riconosciuto da tali fonti è che l'informatica (ed ancor più quindi il suo sviluppo nella cibernetica) penetra fino alla radice dell'agire dell'uomo, andando ben oltre lo svolgimento "meccanizzato" di operazioni matematiche (come era nell'originario approccio in cui si parlava di semplici "*calcolatori* elettronici", sviluppando la c.d. macchina di Turing)[19], per toccarne tratti ben più caratterizzanti, quali in specie:

[18] Queste le definizioni d'interesse contenute nella citata Direttiva:

a) «sistema di informazione»: un'apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un *trattamento automatico* di dati informatici *secondo un programma*, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione;

b) «dati informatici»: una *rappresentazione* di fatti, informazioni o concetti *in una forma che può essere trattata* in un sistema di informazione, *compreso un programma* atto a far svolgere una funzione a un sistema di informazione [corsivi aggiunti].

[19] Turing, *On computable numbers, with an application to the Entscheidungsproblem* (1936), propose per primo un modello matematico capace di simulare il processo di calcolo umano, scomponendolo nei suoi passi ultimi, eseguibili così anche da una meccanica. Sull'importanza di tale ideazione per il successivo sviluppo dell'informatica si rinvia al soprastante contributo storico-filosofico di Pagallo.

1) le capacità *cognitive*, vale a dire di conoscere ed apprendere dall'esperienza del mondo "esterno", ricercando ed acquisendo direttamente informazioni e dati, come si verifica nei c.d. sistemi esperti, che individuano, riconoscono e memorizzano ogni sorta d'informazioni, immagini, suoni, utili ai fini della successiva *elaborazione automatizzata* (paradigmatici sono i sistemi di riconoscimento non solo di impronte, di visi e di voci, ma anche di comportamenti anomali o situazioni di pericolo, ad es. nel percorso di aeromobili e di veicoli, ovvero in luoghi pubblici quali aeroporti, stazioni ferroviarie, ecc.);

2) la capacità, ancor più rilevante, strettamente connessa con le predette, di *auto-determinarsi* di conseguenza, sulla base dell'elaborazione o, se si vuole, "conoscenza" e selezione (a sua volta *automatizzata*) dei dati e delle informazioni utili da considerare, esprimendo ed attuando immediatamente "decisioni" e *scelte operative*, fra possibili opzioni alternative. Per cui si parla a buon diritto di "intelligenza artificiale", che a partire dalle applicazioni più note dei motori di ricerca – capaci di indicizzare e personalizzare, sulla base di frequenze, preferenze e correlazioni acquisite dalle ricerche e dai dati lasciati dagli utenti stessi (a partire dai *cookies* di vario genere) le informazioni più utili per offrire ad es. le pubblicità più incisive in termini individualizzati, od indicare i gruppi sociali di "amici" aventi interessi simili cui aderire, ecc. – vanno fino a quelle più sofisticate applicate alla robotica, alla domotica, alla guida di veicoli (compresi aerei, droni, missili, ecc.), ovvero al campo medico, bellico, ecc.

Oggi può parlarsi di un *equivalente* della "volontà" umana, espressa dai computer o, meglio, dai "sistemi" informatici (cibernetici), che trova già paradigmatici ed espressi riconoscimenti giuridici, di rilievo anche penale, concernenti ad es. la validità di atti, negozi, documenti, compresi i contratti, posti in essere e conclusi automaticamente dalle "macchine" (come nelle menzionate negoziazioni di borsa), che le persone (fisiche o giuridiche), cui si imputano quali "titolari", non avrebbero però potuto porre in essere negli stessi tempi, modi e contenuti[20].

Le nuove esigenze di specifica regolazione e tutela giuridica, di fronte a queste nuove realtà, per quanto riguarda gli aspetti penali, sono bene rappresentate dalla paradigmatica previsione del delitto di "frode informatica", introdotto fin

[20] È sintomatica di questa inevitabile tendenza la cautela con cui l'ordinamento giuridico limita, ma nel contempo riconosce in ipotesi sempre più estese, l'efficacia giuridica di decisioni "interamente" automatizzate che coinvolgano diritti ed interessi delle persone: si veda già l'art. 15 Direttiva europea 95/46 ed ora l'art. 22 GDPR secondo il cui par. 1. "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona", mentre nel par. 2 è elencata una serie assai ampia di eccezioni e condizioni, che sono molto meno stringenti nella corrispondente previsione dell'art. 11 Direttiva UE 680/2016 del 27.04.2016 sul trattamento di dati per fini di indagini e accertamento di reati.

dal 1993 sulla base delle fonti e dell'esperienza internazionali, in cui l'attività "manipolatrice" dell'autore, latamente intesa, s'indirizza *direttamente* al sistema informatico e determina l'esecuzione di "atti dispositivi" di contenuto patrimoniale, che non transitano perciò da una previa o contestuale decisione di una vittima in carne ed ossa, la quale – pur restando titolare del bene giuridico offeso – non coopera personalmente al proprio danno, come prevede invece la fattispecie comune della truffa[21]. Ma altrettanto significativi sono i delitti di falsità in "documenti informatici", che concernono "documenti" *prodotti* – in tutto o in parte – e poi trattati dai sistemi informatici, anziché redatti da un uomo, cui va riconosciuto equivalente valore probatorio nel traffico giuridico e quindi corrispondente tutela penale[22]. Per non parlare dell'emblematica incriminazione del delitto di "accesso abusivo" ad un sistema informatico[23], che colpisce "azioni" irriducibili al paradigma fisico-corporale di un movimento muscolare dell'uomo, perché *immediatamente* dirette ai sistemi informatici con comandi veicolati dal *software*, capaci di eluderne le misure di protezione e di "penetrarvi", per compiervi ulteriori "azioni" di analoga natura, non concepibili né realizzabili se non tramite la tecnologia informatica. Ed altrettanto dicasi delle intercettazioni di comunicazioni informatiche[24] che – a differenza di quelle telefoniche e telegrafiche – prescindono dal coinvolgimento di persone fisiche, che ne siano parte; e così via per ogni altro "reato informatico" (e cibernetico) di cui meglio si dirà (cfr. *infra* § 5.3).

## 3. Il passaggio dai *Computer crime* ai *Cybercrime*

Al predetto carattere basilare dell'informatica, si è aggiunto e correlato il passaggio epocale, collocabile a metà degli anni '90 dell'ultimo secolo del millennio scorso, rappresentato dall'apertura di Internet all'accesso del pubblico indistinto degli utenti, con trasformazione della rete (grazie ai protocolli di comunicazione fra reti e sistemi diversi, che hanno consentito la creazione del *world wide web*: il famoso *www*) in una Rete globale – o *web*, quale "rete di reti" – come è oggi, costituente la base tecnica e strutturale del *Cyberspace*, di cui si è detto (*supra*, § 1.2).

[21] Art. 640-*ter* c.p. (su tale reato si tornerà *infra* § 5.1.1).

[22] Art. 491-*bis* c.p. (su tali reati si tornerà *infra* § 5.1.2).

[23] Art. 615-*ter* c.p. (su tale reato si tornerà *infra* § 5.1.1).

[24] Artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p. (su tali reati si veda *infra* Salvadori, Parte II, cap. XVII).

Dal punto di vista non solo criminologico, ma anche giuridico penale, che qui interessa, si è così assistito al passaggio dalla categoria concettuale dei *Computer crime* (reati informatici) a quella dei *Cybercrime* (reati cibernetici)[25].

Ai primi si riferiva, emblematicamente, il legislatore italiano del 1993, con la (prima) legge contro la criminalità informatica[26], in cui detti reati erano concepiti come realizzabili in singoli sistemi *stand alone*, connessi solo eventualmente in reti telematiche chiuse o ad accesso circoscritto (ad es. interne a singole aziende od amministrazioni, ovvero tutt'al più a singoli settori, come quelli bancario od assicurativo)[27]. Pertanto la locuzione normativa frequentemente utilizzata nelle fattispecie allora introdotte: "*sistema informatico o telematico*" andava (e va) letta quale endiadi, che abbraccia anche sistemi articolati in più *client* con *server* e reti chiuse, ma non concepita per abbracciare la dimensione *globale* ed *aperta* di Internet, all'epoca inaccessibile al pubblico, benché in via interpretativa possa oggi esservi estesa. Al massimo si pensava a banche di dati private o pubbliche, accessibili "da remoto", qual era il famoso CED della Suprema Corte di Cassazione, antesignano di un'informatizzazione della giustizia italiana (percepita come indispensabile ed urgente da magistrati lungimiranti[28]), che purtroppo ha poi segnato a lungo il passo; ovvero all'anagrafe tributaria, comunque ad accesso ristretto, od al CED del Ministero dell'Interno, istituito con la legge di riforma della Polizia di Stato del 1981, che aveva per questo introdotto anche un nuovo specifico "reato proprio" dei pubblici ufficiali legittimati all'accesso, in caso di comunicazione od uso di dati ed informazioni in violazione, anche colposa, delle

---

[25] Picotti, *Presentazione*, in Id. (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, VII.

[26] Sulla L. 21.12.1993, n. 547 si rinvia ai commenti articolo per articolo di Mucciarelli-Picotti-Rinaldi-Ugoccioni, raccolti in *Legislazione pen.* 1996, n. 1-2; nonché al volume collettaneo di Borruso-Buonomo-Corasaniti-D'Aietti, *Profili penali dell'informatica*, Milano, 1994. Per un attento riferimento anche ai lavori preparatori ed alle fonti ispiratrici cfr. Sarzana di Sant'Ippolito, *Informatica e diritto penale*, Milano, 1994; per uno sguardo d'insieme Pica, *Diritto penale delle tecnologie informatiche*, Torino, 1999; Pecorella, *Il diritto penale dell'informatica* (2000), 2ª ed., Milano, 2006; volendo Picotti, *Reati informatici*, in *Enc. Giur.*, agg. VIII, Roma, 2000.

[27] Ne sia riprova la circostanza aggravante speciale prevista per il delitto di accesso abusivo ad un sistema informatico, costituita (tutt'oggi) dalla "violenza sulle cose o alle persone, ovvero se [il colpevole] è palesemente armato": art. 615-*ter*, comma 2, n. 2, c.p.

[28] Si vedano gli interventi raccolti nell'incontro di studio organizzato dal C.S.M., *Il diritto dell'informatica: problemi e prospettive*, Roma, 1983; nonché fra i molteplici contributi successivi, Borruso, *L'informatica giudiziaria in Italia*, in *Dir. informaz. e informatica*, 1985, 92 s.; Giannantonio, *Introduzione all'informatica giuridica*, Milano, 1984; e sul sistema *Italgiure Find* in specie Novelli-Giannantonio, *Manuale per la ricerca elettronica dei documenti giuridici*, 2ª ed., Milano, 1985.

disposizioni previste dalla stessa legge[29]: reato poi "soppiantato" nella prassi giurisprudenziale dal più severo e prodromico delitto di "accesso abusivo ad un sistema informatico o telematico", di cui al citato art. 615-*ter* c.p. – introdotto nel 1993, ma che ha trovato espansione applicativa solo dopo il menzionato sviluppo del *web* – specificamente aggravato, ai sensi del comma 2, n. 1), nell'ipotesi in cui il fatto sia "commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione od al servizio" (su cui cfr. *infra* § 5.1.1).

Anche in materia di tutela del diritto d'autore la protezione penale è stata inizialmente estesa a più riprese ai nuovi "prodotti" informatici ed in specie ai "programmi per elaboratore" (a partire da quelli dei videogiochi) e, quindi, alle "banche di dati", assimilati – non senza qualche forzatura – alle "opere dell'ingegno", ma senza che vi fossero significative modificazioni o riformulazioni anche delle condotte punibili per contrastare le nuove modalità di aggressione *on line*, che solo successivamente si sono manifestate in modo massiccio[30].

Il forte cambiamento si è infatti avuto con la menzionata apertura al pubblico di Internet, che ha reso possibili ed anzi sempre più frequenti e soverchianti gli "attacchi informatici" in rete o tramite la rete e, quindi, i c.d. "reati cibernetici", da intendere in prima approssimazione (per una più precisa definizione e partizione sistematica vedi *infra* § 5.3.3) quali reati realizzabili da chiunque nel *web*, in grado di colpire potenzialmente qualsiasi vittima ad esso connessa, od anche ad esso estranea, come dimostra l'esempio paradigmatico della diffamazione *on line*, giuridicamente configurabile senza necessità di nuove specifiche previsioni normative, che può offendere anche vittime che non siano utenti di Internet.

I reati informatici *strettamente* intesi (su cui cfr. *infra* § 5.3.1) sono naturalmente i primi ad essere commissibili tramite la rete, a partire dagli accessi abusivi ad un sistema informatico, balzati al primo posto dell'attenzione dei legislatori e della giurisprudenza[31]. Ma grande rilievo hanno via via assunto anche

[29] L. 1.4.1981, n. 121, recante *Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*, il cui art. 12 rubricato '*Sanzioni*' prevede: "Il pubblico ufficiale che comunica o fa uso di dati ed informazioni in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a tre anni. Se il fatto è commesso per colpa, la pena è della reclusione fino a sei mesi". Per un commento sulla sua struttura sia consentito rinviare a PICOTTI, *Studi di diritto penale dell'informatica*, Verona, 1992, 123 s.

[30] Cfr. FLOR, *Tutela penale ed autotutela tecnologica de diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010, in specie 159 s.; ed *infra* ID., parte II, cap. XXVI.

[31] Se nelle Raccomandazioni del Consiglio d'Europa del 1989 contro la criminalità informatica (n° R(89) 9 adottate il 13.9.1989) l'accesso non autorizzato ad un sistema informatico erano al quinto posto della c.d. lista obbligatoria dei nuovi reati da incriminare, nella Convenzione Cybercrime del 2001, adot-

tutti i delitti implicanti o consistenti nella "comunicazione" e soprattutto "diffusione" (da intendere anche quale mera "messa a disposizione" ad un numero indeterminato di utenti[32]) di contenuti penalmente illeciti in rete, che presentano un'estrema facilità di realizzazione ed una dimensione, un'estensione, nonché un impatto lesivo incommensurabilmente più grandi. Oggi, nella nostra giurisprudenza, è pacificamente considerato come commesso "pubblicamente" il fatto realizzato in Internet, da equiparare (peraltro dovendosi distinguere diversi ambiti di comunicazione) ad un "mezzo di propaganda" diverso dalla stampa, *ex* art. 266, comma 4, n. 1, c.p.[33], tanto che alla diffamazione tramite un sito *web* accessibile ad una generalità indeterminata di utenti si applica la circostanza aggravante dell'utilizzo di "altro mezzo di pubblicità" (diverso dalla stampa o dalla radio o televisione), di cui al comma 3 dell'art. 595 c.p.[34].

Si sono poi avuti anche più specifici ed incisivi interventi di contrasto a tali nuove forme di criminalità "cibernetica" a partire dagli organismi internazionali, che hanno riguardato innanzitutto la *pornografia minorile*, di per sé già esistente ed in parte sanzionabile quale "oscenità" anche a prescindere dalla rete, ma la cui specifica punibilità è stata stabilita espressamente dal Protocollo opzionale della Convenzione di New York sulla protezione dei diritti del fanciullo (risalente al 1989), adottato dall'Assemblea delle Nazioni Unite il 25.5.2000, rispetto a cui si è avuta un'anticipazione nel nostro ordinamento già con L. 3.10.1998, n. 269, che ha introdotto gli artt. 600-*ter* e 600-*quater* c.p. Successivamente la L. 6.2.2006, n. 38 ha portato significative modifiche, fra cui l'estensione della punibilità alla c.d. "pornografia virtuale" – implicante il ricorso ad un'elaborazione grafica specificamente informatica: cfr. il nuovo art. 600-*quater*.1 c.p. – per dare attuazione anche all'art. 9 della citata Convenzione *Cybercrime* del 2001 (nonché alla corrispondente previsione della Decisione quadro dell'Unione europea 2004/68/GAI, poi sostituita dall'ultima Direttiva 2011/93/UE)[35]; mentre con L.

---

tata dal medesimo Consiglio, il delitto di accesso abusivo è diventato il primo (art. 2); e nei repertori giurisprudenziali e nelle statistiche giudiziarie recenti è sicuramente oggi il delitto informatico più ricorrente.

[32] Sul punto sia consentito rinviare a Picotti, *Profili penali delle comunicazioni illecite via* Internet, in *Dir. informaz. e informatica*, 1999, n. 2, 283 s.

[33] Ma sulla necessità di distinguere forme di comunicazione "private" e "pubbliche" in Internet (seppur nei delitti di diffusione di materiale pedopornografico) cfr. in giurisprudenza Cass., sez. I, 15.5.2017, n. 24103.

[34] In tal senso già Picotti, *Profili penali*, cit., 303 e la successiva dottrina e giurisprudenza, sui cfr. *infra*, Lasalvia, Parte II, cap. IX.

[35] In argomento, fra i moltissimi contributi, sia consentito rinviare a Picotti, *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in Bertolino-Forti (cur.), *Scritti per Federico Stella*, Napoli, 2007, vol. II, 1267 s.; ed anche per aggiornati richiami *infra*, L'insalata, Parte III, cap. IV.

1.10.2012, n. 172 è stata infine data attuazione anche alla Convenzione di Lanzarote del 2007 per la protezione dei minori dagli abusi sessuali, con l'introduzione nel nostro codice penale dei nuovi delitti di istigazione a pratiche di pedofilia e di pedopornografia (art. 414-*bis* c.p.), nonché di adescamento di minori (art. 609-*undecies* c.p.), che si manifestano e sono da contrastare specificamente e soprattutto in rete[36].

Altri significativi interventi di penalizzazione dei "reati cibernetici" (ampiamente intesi) hanno riguardato la propaganda ed istigazione ad atti di odio e discriminazione razziale, oggetto del Protocollo addizionale alla Convenzione *Cybercrime* adottato dal Consiglio d'Europa il 28.1.2003 per contrastare il razzismo e la xenofobia in rete, sottoscritto dall'Italia soltanto il 9.11.2011, cui non è ancora stata data specifica attuazione, ma che sul piano del diritto penale sostanziale trova riscontri nelle disposizioni già contenute negli artt. 1 ss., D.L. 26.4.1993, n. 122, recante "Misure urgenti in materia di discriminazione razziale, etnica e religiosa" convertito con modificazioni in L. 25.6.1993, n. 205 (c.d. legge Mancino)[37].

Altrettanto può dirsi per i numerosi delitti, via via introdotti per combattere il terrorismo che si manifesta anche nella rete, utilizzata sia come luogo di propaganda e proselitismo, sia come mezzo di "arruolamento", "addestramento", organizzazione anche di altre attività preparatorie, specificamente criminalizzate, quali i viaggi all'estero in territori prescelti per attività terroristiche, nonché per il finanziamento anche tramite raccolte *on line*[38].

---

[36] Sul tema si veda la recente monografia di Salvadori, *L'adescamento di minori. Il contrasto al* child-grooming *tra incriminazione di atti preparatori ed esigenze di garanzia*, Torino, 2018.

[37] In particolare, l'art. 1 dispone che "*[...] è punito con la reclusione fino a un anno e sei mesi o con la multa fino a 6.000 euro chi* propaganda *idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi [...]*". Mentre è "*[...] punito con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo,* incita *a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi [...]*" (evidenz. agg.). Non essendo specificate le modalità con cui si possano realizzare la "*propaganda*" o l'"*incitamento*", queste condotte possono pacificamente ritenersi penalmente rilevanti anche quando siano commesse in rete o comunque con mezzi informatici. La piena attuazione del Protocollo, anche sotto altri profili processuali e di cooperazione internazionale, è però ferma ai lavori preparatori relativi ad un d.d.l. presentato nella scorsa Legislatura.

[38] Cfr. Picotti, *Terrorismo e sistema penale: realtà, prospettive, limiti* (Relazione di sintesi del VII corso di diritto e procedura penale "Giuliano Vassalli" per dottorandi e giovani penalisti – SII e Gruppo italiano AIDP, Noto, 11-13 novembre 2016), in *Riv. trim. dir. pen. contemporaneo*, 2017, 249 s.; sull'emblematica, ma criticabile circostanza aggravante prevista per il delitto di "addestramento" se "commesso attraverso strumenti informatici o telematici" (art. 270-*quinquies*, comma 2, c.p., aggiunto dal D.L. 18.2.2015, n. 7, convertito dalla L. 17.4.2015, n. 43) cfr. altresì Id., *Quale diritto penale nella dimensione globale del cyberspace?* in Wenin-Fornasari (cur.), *Diritto penale e modernità*, Trento, 2017, 309 s. ed *infra* D'Ambruoso, Parte II, cap. I.

Nel campo della protezione dei diritti d'autore e dei diritti connessi – su cui cfr. *infra*, Flor, Parte II, Cap. 26 – è stata fortemente "anticipata" la soglia della rilevanza penale, introducendo nuove formulazioni che consentono di sanzionare comportamenti *prodromici* all'effettiva violazione di tali diritti in rete, proteggendosi penalmente anche gli strumenti e le tecniche di "autotutela tecnologica" via via adottati dai titolari dei diritti sulle opere e sui prodotti digitali, attraverso l'incriminazione, come autonomi reati "preparatori", delle violazioni delle "misure tecniche di protezione", come pure le contraffazioni o manipolazioni degli apparecchi di accesso a trasmissioni criptate (c.d. *decoder*).

Di fronte alla nuova realtà è cambiato, dunque, di passo l'approccio alla criminalità informatica, a sua volta divenuta "criminalità cibernetica" o, meglio, criminalità "nel" *Cyberspace*.

Tale categoria non può essere più circoscritta ad un numero chiuso o limitato di reati e, quindi, di vittime potenziali, che suscitava l'interesse soltanto degli specialisti dei delitti ad alta tecnologia (TIC), ma include oggi una crescente e potenzialmente indefinita molteplicità di illeciti e di modalità di offesa di diritti ed interessi altrui, taluni anche di nuova creazione, in quanto frutto dello stesso sviluppo tecnologico, comprendendo – oltre ai delitti informatici in senso stretto, con relative tipologie di condotte *normativamente* descritte: *infra* § 5.3.1 – qualsivoglia altro od almeno molteplici altri reati, che presentano modalità *esecutive* concretamente nuove, non necessariamente espresse sul piano della tipicità penale, ma in concreto correlabili all'elaborazione, comunicazione, trasmissione, trattamento in rete di dati, informazioni e contenuti "digitali" di ogni tipo.

Esemplificando: è un "nuovo" crimine cibernetico (in senso ampio), se ed in quanto realizzato nel *Cyberspace*, l'estorsione commessa con la criptazione illecita dei dati di un sistema informatico altrui, tramite un *malware* abusivamente installatovi da remoto, che realizzi così una forma di *violenza* c.d. informatica alla quale definita dall'art. 392, comma 3, c.p., aggiunto dalla L. n. 547/1993, su cui cfr. *infra* § 5.1.2 – per mezzo della quale la vittima è "*costretta*", per riacquistare la libera disponibilità dei propri dati, a corrispondere un prezzo ingiusto di riscatto (spesso esigito in *bitcoin* od altra valuta virtuale da corrispondere o trasferire nel c.d. *dark web*) per ottenere l'indispensabile chiave di decriptazione, consumandosi in tal modo, con il duplice evento di profitto ingiusto e di danno altrui, consapevolmente voluti dall'agente, il delitto di cui all'art. 629 c.p.

Un altro esempio di delitto comune, che presenta caratteri "nuovi" – anche di pericolosità, diffusività, difficoltà di prevenzione e repressione – se commesso in rete, è il riciclaggio, che può essere realizzato con trasferimenti elettronici di fondi, investimenti od "*altre operazioni*" via *web* (o nel *dark web*), ad esempio movimentando e scambiando valute virtuali come *bitcoin* od *ethereum*, idonee ad "*ostacolare l'identificazione*" della provenienza delittuosa del denaro, dei beni o delle "*altre utilità*" di cui all'art. 648-*bis* c.p. (c.d. *Cyberlaundering*).

Emerge dunque, in primo luogo, una grande novità, estensione e varietà delle modalità di condotta e delle tecniche di commissione dei reati cibernetici, la cui rapida evoluzione segue quella del *Cyberspace*, andando ben oltre l'ambito di quelli consistenti nella "comunicazione" o "diffusione" di un pensiero o di contenuti illeciti in rete, che pur mantengono un ruolo di grande rilievo.

In secondo luogo si ha una corrispondente espansione e diversificazione dei *beni giuridici* meritevoli di tutela penale e, corrispondentemente, delle vittime – che ne sono titolari – da proteggere, spesso ignare o "vulnerabili", siano esse individui ovvero entità o categorie collettive, a partire dai minori fino a quelle esposte a discriminazioni, nonché più in generale – applicando la definizione della Direttiva europea in materia – "*non aventi cittadinanza*" negli Stati membri in cui il reato cibernetico, che è strutturalmente transnazionale, è commesso[39].

Si pensi emblematicamente alla riservatezza, assurta, da un lato, alla nuova dimensione della "riservatezza informatica", quale autonomo bene giuridico ed, anzi, diritto fondamentale della persona, da intendere come diritto ad uno *spazio* informatico *esclusivo*, che a prescindere dai contenuti che vi siano presenti, trattati o comunicati, deve essere lasciato *libero da intrusioni* e manomissioni di terzi, in quanto strumento essenziale per l'odierna vita individuale e sociale, che neppure l'Autorità pubblica può violare o comprimere, se non nei casi e modi previsti tassativamente dalla legge e con le garanzie del controllo giudiziario[40]. Dall'altro, alla *privacy* in senso stretto, quale più specifico diritto alla tutela dei *propri* "dati personali", ovunque e da chiunque siano rispettivamente localizzati o trattati, che ha assunto caratteristiche e dimensioni peculiari – rispetto all'originaria categoria di derivazione anglosassone, concepita quale difesa della vita privata (diritto ad essere "lasciati soli") dalle intrusioni ingiustificate dei nuovi *mass media*, all'epoca rappresentati dalla stampa[41] – richiedendo oggi nuove e complesse discipline di tutela, finalizzate a garantire la possibilità di "controllo" da parte della persona cui si riferiscono le informazioni ed il bilanciamento con la contrapposta esigenza di circolazione e di accessibilità anche da parte di terzi, in quanto ele-

[39] Cfr. Dir. 2012/29/UE del Parlamento Europeo e del Consiglio del 25.10.2012.

[40] Sull'individuazione della "riservatezza informatica" quale nuovo bene giuridico, distinto dalla più generale riservatezza delle comunicazioni nonché dalla *privacy* strettamente intesa, sia consentito rinviare a Picotti, voce *Reati informatici*, cit., 20; per un quadro aggiornato *infra*, Salvadori, Parte II, cap. XVII; nella giurisprudenza fondamentale è la sentenza della Corte cost. tedesca sui limiti e le condizioni di ammissibilità delle c.d. perquisizioni in rete (*online-Durchsuchung*): cfr. Bundesverfassungsgericht, 27.2.2008,379/2007-595/2007, su cui si veda in italiano il commento di Flor, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online-Durchsuchung, in *Riv. trim. dir. pen. economia*, 2009, 695 s.

[41] Si rinvia sempre allo storico contributo di Warren-Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 15.12.1890.

menti spesso essenziali per infinite attività e servizi in ogni settore della società contemporanea[42]. Le TIC ne hanno infatti determinato, per un verso, la grande estensione e facilità di raccolta e trattamento, per l'altro, l'importanza fondamentale per lo svolgersi di molteplici attività e rapporti – non solo nel *Cyberspace* – nell'interesse della stessa persona cui si riferiscono, da regolare sulla base del "consenso" e comunque, secondo il modello europeo, di dettagliate disposizioni affidate alla vigilanza ed aggiornamento costanti di un'Autorità garante, munita di penetranti poteri di autorizzazione, d'indagine e sanzionatori [43].

Si pensi altresì alla "sicurezza informatica", bene giuridico parimenti nuovo, non soltanto *strumentale* alla protezione degli altri interessi e diritti della persona meritevoli di tutela, a cominciare dalla riservatezza informatica e dalla *privacy*, appena menzionate, ma a sua volta meritevole e bisognoso di un'*autonoma* efficace protezione giuridica, compresa quella penale, nel *Cyberspace*, in quanto assurge ad una funzione di *garanzia* "preventiva" di tutti gli altri interessi e diritti che emergono e vi si esercitano, tanto da divenire, a certe condizioni, "indisponibile" per gli stessi titolari dei sistemi informatici, perché *collettivamente* condiviso, nella dimensione globale e di stretta interdipendenza che hanno i rapporti e le attività in rete[44].

Proprio questa dimensione sovraindividuale e di stretta interdipendenza, che assumono la sicurezza e la riservatezza, ma anche altri beni e diritti nel *Cyberspace*, di cui si dirà (per un'elencazione meramente sintomatica cfr. *infra* § 5.2), dimostra l'importanza crescente del ruolo degli *Internet Service Providers* (ISP), che in relazione ai diversi servizi ed alle plurime attività che vi svolgono, diventano necessariamente anche centri d'imputazione di responsabilità – civili, penali ed amministrative – il cui fondamento positivo e la cui delimitazione precisa pongono però rilevanti problemi giuridici (oltre che di politica del diritto), certamente non risolti dalla vetusta regolamentazione, d'ispirazione sopranazionale, risalente all'originario modello delineato dal *Millennium Copyright Act* statunitense del 1997 e dalla Direttiva CE 2000/31 sul commercio elettronico, che in parte lo ha ricalcato, sulla cui inadeguatezza, rispetto all'impressionante evoluzione successiva, si avrà modo di ritornare (*infra* § 6).

---

[42] Per il riconoscimento della nascita di tale "nuovo" diritto come diritto al controllo su propri dati e la loro circolazione, cfr. nella dottrina italiana i fondamentali contributi di Rodotà, a partire da *Elaboratori elettronici e controllo sociale*, Bologna, 1973 fino ad *Intervista su privacy e libertà*, Bari, 2005 ed altri successivi; nella dottrina penale Patrono, *Privacy e vita privata*, in *Enc. Dir.*, XXXV, Milano, 1985, 557 s.; volendo, per la distinzione dai diritti relativi al trattamento di dati personali, Picotti, *Tutela dei dati personali e tutela della persona*, in Cammelli-Guerra (cur.), *Informazione e funzione amministrativa*, Rimini, 1997, 297 s.

[43] Basti qui il richiamo allo specifico contenuto dell'art. 8 della Carta di Nizza.

[44] Picotti, *Sicurezza, informatica e diritto penale*, in Donini-Pavarini (cur.), *Sicurezza e diritto penale*, Bologna 2011, 217 s.

Oltre ai menzionati interventi di armonizzazione legislativa da parte degli organismi sovranazionali, concernenti le incriminazioni penali e le relative responsabilità di natura *sostanziale*, estese pressoché sistematicamente anche alle persone giuridiche[45], occorre richiamare l'altro aspetto emblematico di questa evoluzione, cui sopra si è già fatto cenno: quello dell'importanza crescente che sono venuti ad assumere il rafforzamento e l'armonizzazione della disciplina *processuale*, con l'introduzione di nuovi istituti che riguardano, innanzitutto, la ricerca, l'acquisizione, la conservazione, la circolazione e l'utilizzazione delle "prove elettroniche", indispensabili per assicurare un'effettiva repressione dei reati (di ogni natura) commessi nel *Cyberspace*, e non solo: e, quindi, un'efficace cooperazione sovranazionale, giudiziaria e di polizia al riguardo; e via via anche una molteplice serie di misure, soprattutto cautelari, dirette a contrastare e se possibile far cessare o non lasciar protrarre i comportamenti illeciti in rete ed i loro effetti dannosi, potenzialmente espansivi nel tempo e nello spazio.

Nel nostro ordinamento, se nel primo ricordato intervento legislativo contro la criminalità informatica del 1993 la novella si era limitata, nel campo processuale, alla sola timida previsione delle "intercettazioni di comunicazioni informatiche o telematiche"[46], con la L. 18.3.2008, n. 48, di ratifica ed attuazione della Convenzione *Cybercrime* del 2001 (che dedica ben due parti su tre al diritto processuale, rispettivamente nella materia della ricerca, raccolta, circolazione delle prove elettroniche e degli strumenti cautelari da utilizzare, nonché della cooperazione internazionale, giudiziaria e di polizia) sono state introdotte molteplici nuove disposizioni nel codice di procedura penale, concernenti non solo, ma soprattutto, le menzionate prove elettroniche[47]. Pur con gli innumerevoli limiti e difetti

[45] Anche nel campo degli strumenti di contrasto alla criminalità informatica si è ormai consolidata l'esigenza di sanzionare le persone giuridiche e gli enti per i reati commessi da soggetti apicali e subordinati nell'interesse dell'ente stesso. Sulle formulazioni pressoché standardizzate delle relative previsioni contenute nelle Direttive dell'Unione europea in materia penale emanate dopo l'entrata in vigore del Trattato di Lisbona, ma sostanzialmente rinvenibili anche in altre fonti precedenti, si può vedere PICOTTI, *European Union's Directives in Substantive Criminal Law: What Discontinuity in Respect to the Pre-Lisbon Instruments?*, in AA.VV., *Toward Scientific Criminal Law Theories*, Beijing, 2015, 1248 s.

[46] Cfr. l'art. 266-*bis* c.p.p. inserito dall'art. 11, L. 23.12.1993, n. 547, che nel prevederne la possibilità, rinvia in toto – secondo un criterio di mera analogia normativa – alla disciplina delle intercettazioni telefoniche. In argomento cfr. RUGGIERI, *Profili processuali nelle indagini sui reati informatici*, in *Il diritto penale dell'informatica nell'epoca di Internet* (a cura di Picotti), Padova, 2004, 153 s.; ed *infra* TORRE, parte IV, cap. VII.

[47] Per un quadro d'insieme cfr. i vari contributi raccolti in LUPARIA (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 8 marzo 2008, n. 48)*, Milano, 2009, 113 s.; volendo, per taluni accenti critici, anche PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, 2008, 437 s.

evidenziati dalla dottrina ed emersi in giurisprudenza (per cui si rinvia agli specifici contributi in questo volume, parte IV), esse rappresentano oggi un presupposto basilare per svolgere "indagini informatiche", che possono riguardare *qualsivoglia* tipo di reato, anche non cibernetico, per cui però emerga la rilevanza di "tracce" elettroniche. Mentre la giurisprudenza, con interventi estensivi al limite dell'analogia, frequentemente ricorre all'applicazione del sequestro preventivo per fermare la diffusione o disponibilità di contenuti illeciti in rete[48].

Infine è significativo del profondo cambiamento in esame il fatto che la "criminalità informatica" (ampiamente intesa) con il Trattato di Lisbona del 2007, entrato in vigore nel 2009, sia divenuta oggetto di espressa competenza penale concorrente dell'Unione europea[49], per quanto concerne sia le norme di diritto penale sostanziale, dirette a definire reati e sanzioni, ai sensi dell'art. 83, par. 1, TFUE, sia le norme di diritto processuale penale, ai sensi dell'art. 82 TFUE. E tutte le fonti dell'Unione europea, che hanno dato e danno applicazione al principio del "mutuo riconoscimento" dei provvedimenti degli Stati membri in materia penale, di cui al citato art. 82 TFUE (già art. 31 TUE), e le relative anche se spesso tardive disposizioni nazionali d'attuazione, hanno incluso ed includono (a partire dal 2002) la sfera della "criminalità informatica" nella "lista dei reati" per cui deve prescindersi dal requisito della doppia incriminazione, così da renderne più sicura e celere l'esecuzione da parte dello Stato richiesto e rafforzare la cooperazione internazionale, sul presupposto, oltre che di una reciproca fiducia, di un sufficiente grado di armonizzazione dei sistemi penali nazionali in questo settore[50].

## 4. Il *web* interattivo ed il doppio ruolo degli utenti quali possibili autori e vittime di reati cibernetici

Un ultimo importante passaggio, che occorre sottolineare per dar conto dell'evoluzione del diritto penale dell'informatica e dei problemi che oggi si presentano, è costituito dal superamento dell'originaria architettura "unidirezionale" del *web*, in cui l'utente era il destinatario passivo di informazioni e comunicazioni,

[48] Cass., SS. UU., 29.1.2015 (dep. 17.7.2015), n. 31022, in *www.penalecontemporaneo.it* (9.3.2016), con nota di Melzi D'Eril.

[49] Competenza già esercitata con la citata Direttiva 2013/40 contro gli attacchi informatici. In argomento sia consentito rinviare a Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. economia*, 2011, n. 4, 827 s.

[50] Cfr. volendo Picotti, *Il mandato d'arresto europeo fra principio di legalità e doppia incriminazione*, in Bargis-Selvaggi (cur.), *Mandato d'arresto europeo. Dall'estradizione alle procedure di consegna*, Torino, 2005, 33 s.; nonché, con specifico riguardo ai reati informatici, Id., *Il campo di applicazione del mandato d'arresto europeo: i reati "in lista" e "fuori lista" e la disciplina della legge italiana di attuazione*, *ivi*, 127 s.

alle quali poteva accedere e che poteva leggere o acquisire, ma la cui produzione, circolazione e diffusione dipendeva dai gestori degli accessi e dei servizi in rete (ISP e, più in generale, c.d. *webmaster*).

Da tempo (2000-2006) si è parlato di un *web* 2.0, caratterizzato invece dalla progressiva interazione attiva degli utenti, posti in grado di creare e condividere contenuti in *blogs*, *forum*, *social network*. Quindi si è ravvisato un ulteriore passaggio al *web* 3.0, caratterizzato dalla multimedialità delle comunicazioni e dei contenuti condivisibili, grazie allo sviluppo della grafica ed espansione delle capacità di memoria e di connessione, che consentono l'utilizzabilità ed adattabilità – anche a dispositivi mobili e terminali di qualsiasi tipo – di audio, video, immagini, anche a tre dimensioni. Oggi si prefigura il *web* 4.0, dominato dall'intelligenza artificiale, in cui gli utenti – divenuti sistematici creatori e diffusori di informazioni e contenuti caricano, condividono, fanno circolare in rete – sono la "merce" da cui vengono sistematicamente estrapolati (a loro insaputa o meno), anche tramite precise configurazioni degli spazi e delle attività da svolgere nel *web,* dati ed informazioni di ogni genere, riguardanti qualsiasi azione, espressione, preferenza e tendenza, poi immediatamente ed incessantemente elaborati dai c.d. sistemi esperti, che si autoalimentano e si perfezionano, grazie ad algoritmi sempre più sofisticati e penetranti, determinando un impressionante sviluppo di attività economiche, commerciali, imprenditoriali, produttive e di ogni genere, comprese quelle politiche, nel *Cyberspace*.

Il rischio già palesatosi è che nella misura in cui la vita di chiunque (persona fisica, impresa, ente o gruppo) si viene a trasferire – per parti sempre più importanti – nel *Cyberspace*, la raccolta, l'analisi, la memorizzazione, l'elaborazione automatizzate delle relative tracce elettroniche, in quantità gigantesche, possibile oggi con le TIC, va non solo a "personalizzare" ma anche a condizionare e guidare significativamente le scelte, i rapporti, le relazioni da instaurare e sviluppare, i prodotti da acquistare, i gruppi e gli orientamenti da seguire (da quelli del tempo libero, sportivi, ideologici, culturali, fino a quelli politici), i comportamenti da tenere anche nel mondo "esterno", ormai indissolubilmente intrecciato con quello cibernetico.

Il *Cyberspace* si struttura e sviluppa sempre di più come un'enorme base di dati di ogni tipo (per cui si parla a ragione di *Big Data*), i cui contenuti sono indicizzati e trattati dai potentissimi motori di ricerca e sistemi di intelligenza artificiale, che correlano parole chiave e sintagmi o, meglio, creano una "semantica del *web*" sempre più raffinata, con cui non solo si reperiscono ed elaborano informazioni sempre più performanti, ma – per il livello raggiunto di automazione tecnologica e di potenza nella raccolta, memorizzazione e trattamento dei dati – si creano quegli *alter ego* digitali, cui si già fatto cenno, che si "sostituiscono" in parte crescente agli individui, nel conoscere e quindi decidere, in parallelo a pre-

occupanti fenomeni di concentrazione, se non tendenziale monopolio in disparati settori di attività, in capo ai colossi del *web*, come è già emerso dalle indagini e dagli interventi antitrust in specie della Commissione europea nei confronti di Facebook, Google, Amazon, ecc.

Senza qui entrare in ulteriori analisi tecniche, né approfondire considerazioni giuridico-filosofiche (per cui valga il rinvio al capitolo introduttivo di questo volume), occorre riconoscere che uno dei fondamentali fattori moltiplicatori e propulsori, non solo della comunicazione e dell'informazione, bensì proprio dello sviluppo e del rilievo economico e commerciale, oltre che culturale e politico, del *Cyberspace*, è costituito oggi dall'*azione* ed *estensione* costante del numero sempre più grande di utenti, che godono di un'*apparente autonomia* d'iniziativa e di gestione, disponibile a ciascuno in rete, ma promossa, suggerita, condizionata e persino insistentemente sollecitata ed indirizzata dai gestori dei vari servizi o, come detto, "signori del web".

Se la rete è stata configurata tecnicamente, fin dalla sua origine, quale struttura non centralizzata, articolata in una molteplicità di possibili connessioni alternative, nodi di scambio e di ritrasmissione, per garantirne la funzionalità anche in caso di attacchi atomici od incidenti catastrofici che ne coinvolgessero grandi parti o rami, senza che per questo ne venisse bloccato il funzionamento complessivo, oggi questa architettura, moltiplicata e sviluppata all'ennesima potenza, offre la possibilità tecnica a ciascuno di operare da ogni suo punto, anche in modo del tutto autonomo e diretto, immettendo, caricando o scaricando dati, informazioni, immagini, video, musica, contributi di ogni genere, e nel contempo condividendo, modificando, approvando, respingendo o stimolando interventi, scambi, contributi, condivisioni, inviti altrui.

Ma con questa tentacolare articolazione, la libertà formidabile che la sua architettura assicura, si riflette anche in una parallela e speculare capacità, altrettanto capillare nell'intero *Cyberspace*, di raccolta, connessione, interrelazione, incrocio, analisi e controllo dei dati e delle informazioni provenienti dagli stessi utenti, che non possono sfuggirvi, se non "uscendone" ovvero operando nel *deep web* od agendo con la copertura dell'anonimato o di pseudonimi, compresa l'impersonificazione illecita in "identità digitali" altrui. Dunque: con comportamenti criminosi o illeciti.

In sintesi: la personalità di ciascun individuo è radicalmente "potenziata" nelle sue capacità di esprimersi, comunicare, informarsi e svilupparsi, grazie alla disponibilità ed accessibilità del *Cyberspace*; ma nel contempo è esposta ad un "prelievo" sistematico di dati, informazioni, tracce, aggressioni, che possono condizionarla, soggiogarla, persino "espropriarla" nelle relazioni che vi si svolgono e di cui diviene, con rapidità ed intensità crescenti, quotidianamente e permanentemente parte integrante, tanto da non potervisi sottrarre, se non violando i limiti di legittimazione della sua "appartenenza" al *Cyberspace*.

Alla radice di tali processi resta, infatti, sempre il necessario dato *tecnico* dell'accesso alla rete e all'operatività e disponibilità delle funzioni desiderate, tramite *software*, *browser*, connessioni e configurazioni, veicolati dai fornitori dei corrispondenti servizi (ISP).

Questi hanno dunque (sempre) la possibilità tecnica, ma non necessariamente anche l'abilitazione giuridica, di regolare, aggiornare, modificare, sostituire il sostrato indispensabile all'effettivo svolgimento di tutte dette attività e relazioni, le cui tracce ed informazioni restano da essi più o meno esplicitamente, consensualmente o legittimamente acquisite e trattabili. Per cui si afferma ironicamente che, se i servizi messi a disposizione (sempre più numerosi e diversificati) sono gratuiti – e basta verificare l'impressionante quantità e varietà di "app" offerte per averne un'idea – ciò significa che "la merce sei tu".

L'utente così diviene nel *Cyberspace* potenziale vittima e bersaglio, oltre che possibile autore di prevaricazioni ed offese dei diritti ed interessi altrui, meritevoli di protezione anche penale[51], in parallelo del resto con quanto si verifica nella vita reale, seppur con modalità e condizioni totalmente nuove. E gli interessi e diritti da proteggere vanno quindi dall'onore e reputazione, quale essenziale diritto al riconoscimento e rispetto dovuti alla qualità di "persona" di ciascuno anche nel *Cyberspace*, all'immagine ed "identità" individuali, che possono essere riflesse in una o più "identità digitali"; dalla riservatezza, nelle varie accezioni già viste, al controllo effettivo della diffusione od utilizzazione dei dati personali, fino all'esclusiva sui prodotti dell'ingegno e sui relativi contenuti digitali, comprendendo categorie di diritti e interessi sia privati, come quelli patrimoniali, che pubblici od anche soltanto comuni di gruppi e collettività, come la menzionata sicurezza informatica, fino alle libertà fondamentali, al divieto di discriminazioni, al generico interesse ad un "corretto" svolgimento degli scambi e del traffico giuridico in genere nella nuova realtà cibernetica, che non può restare avulsa dall'ordinamento giuridico.

L'ambito più delicato di soggetti "vulnerabili" in cui è emersa questa doppia posizione di autore potenziale di reati e di vittima particolarmente esposta ad essi nel *Cyberspace* è senz'altro quello dei minori, che ormai accedono al ed utilizzano il *web* come parte integrante, talora patologicamente condizionante, della loro vita quotidiana di "nativi digitali": per cui – accanto allo straordinario potenziamento delle abilità e capacità di accesso ad informazioni e rapporti sociali, nonché attività di ogni tipo in tutto lo spazio cibernetico – si sviluppano fenomeni altamente allarmanti, che vanno dal *sexting* al *cyberbullismo*, con tutte le varianti dei giochi e delle sfide anche mortali (*Blue wahle* ne è un esempio tra-

[51] Picotti, *I diritti fondamentali nell'uso ed abuso dei Social Network. Aspetti penali*, in *Giur. di Merito*, 2012, n. 12, 2522 s.

gitto), nonché di rapporti devastanti che si instaurano o cui si espongono, in grado di pregiudicarne irreparabilmente lo sviluppo personale e l'inserimento proficuo nella vita reale[52]. Anche o soprattutto a loro tutela non può certo mancare, benché sicuramente non basti, il diritto penale.

## 5. Tecniche di tipizzazione dei reati informatici e cibernetici e relative partizioni classificatorie

Sulla base di tale indispensabile ricostruzione storica e strutturale del quadro globale in cui deve oggi operare il diritto penale, si può ora delineare un inquadramento sistematico dei singoli reati informatici e cibernetici previsti dal diritto positivo in vigore nel nostro ordinamento, distinguendo e classificando le diverse fattispecie legali alla stregua della loro formulazione tecnica e modalità di tipizzazione (§ 5.1), per fare poi cenno ai vari beni giuridici protetti, che ne determinano la collocazione topografica (§ 5.2), concludendo, infine, con una ripartizione fra le distinte categorie dogmatiche, in cui possono essere suddivisi (§ 5.3).

### *5.1. Nuove condotte, estensioni "analogiche", nuovi oggetti materiali*

A partire dalla prima legge contro la criminalità informatica del 1993, il legislatore italiano ha fatto ricorso a diverse tecniche di tipizzazione dei "reati informatici" (non concepibili cioè a prescindere dalle TIC e dall'ambiente informatico: cfr. *infra* § 5.3), tutte però sostanzialmente caratterizzate dall'esigenza di non discostarsi eccessivamente dai paradigmi delle fattispecie legali comuni, considerate più vicine alle nuove. Ha scelto quindi denominazioni, collocazione sistematica e livelli sanzionatori il più possibile analoghi. Esemplificando: accanto alla truffa comune (art. 640 c.p.) ha collocato la frode informatica (art. 640-*ter* c.p.); accanto alla violazione di domicilio (art. 614 c.p.), il delitto di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.) e quelli ad esso considerati prodromici (artt. 615-*quater* e 615-*quinquies* c.p.); fra i delitti di falsità in atti (artt. 476 s. c.p.), quelli di falsità in documenti informatici (art. 491-*bis* c.p.); accanto al danneggiamento comune di cose (art. 635 c.p.), quelli di dati e sistemi informatici (artt. da 635-*bis* a 635-*quinquies* c.p.). Ma diverse sono state le modalità con cui ha attuato questa scelta di fondo di politica criminale, diretta a legittimare le nuove incriminazioni rendendone evidente la *ratio* di tutela e più facile il reperimento nel codice, con il rischio tuttavia di perpetuare orientamenti interpretativi e concetti giuridici formatisi sulle ben diverse fattispecie preesi-

[52] Basti rinviare al riguardo ai dati forniti dai principali organismi internazionali e nazionali che si occupano della tutela dei minori: riferimenti in SALVADORI, *infra*, Parte II, cap. XIII.

stenti e di comprimere, quindi, la portata innovativa degli elementi introdotti, tanto più importante da riconoscere, invece, di fronte agli sviluppi ulteriori. Di qui l'opportunità di una seppur solo paradigmatica analisi critica.

*5.1.1. Nuove condotte e nuovi "fatti" di reato: in particolare le fattispecie paradigmatiche della frode informatica e dell'accesso abusivo*

Innanzitutto, vengono in rilievo le fattispecie appositamente create dal legislatore delineando, in autonomi articoli, *condotte nuove* o, meglio, "fatti tipici" inediti, costitutivi di nuovi reati.

Paradigmatici sono i delitti di frode informatica e di accesso abusivo ad un sistema informatico o telematico, introdotti nel 1993, cui già si è fatto cenno (*supra* § 2), che meritano ora un breve approfondimento sulla loro struttura normativa, visto che sono anche fra i più frequentemente applicati nella prassi giurisprudenziale.

*La frode informatica* – La prima nuova fattispecie legale, collocata fra i delitti contro il patrimonio, appare ispirata al modello della truffa comune, alla quale si affianca, presentando lo stesso livello di disvalore penale in termini di limiti edittali di pena e gli stessi eventi consumativi (il danno altrui ed il profitto ingiusto per sé o per terzi), causalmente prodotti da condotte *lato sensu* manipolatorie e, quindi, sotto questo profilo "fraudolente". Ma l'azione del reo non è indirizzata al soggetto passivo persona fisica, da indurre psicologicamente in errore mediante artifici o raggiri, così da portarlo ad un atto di disposizione patrimoniale che realizzi quella "cooperazione artificiosa" della vittima che si autodanneggia, bensì si indirizza *direttamente* al sistema informatico o, meglio, al trattamento *automatizzato* di dati, che viene piegato all'interesse del reo mediante l'"alterazione" del suo funzionamento (rispetto a quella che avrebbe dovuto essere la regolare elaborazione alla stregua della volontà del suo titolare) ovvero mediante qualsiasi altro "intervento senza diritto" su dati, informazioni o programmi. La sostituzione dell'uomo in carne ed ossa, quale vittima dell'inganno (c.d. soggetto passivo della condotta), con il sistema informatico, porta ad una profonda riconfigurazione della struttura stessa del "fatto" delittuoso, spostandone il perno dall'induzione in errore all'"abuso" delle procedure tecniche o dei dati ad esse inerenti. Il legislatore non offre però definizioni stringenti al riguardo, ma ricorre a clausole aperte circa le concrete "modalità" di condotta, che devono essere soltanto tali da determinare la produzione degli eventi consumativi da parte dello stesso sistema informatico, alla stregua delle cui "regole" di corretto funzionamento esse vanno quindi determinate, restando in ogni caso esclusa la necessità di una disposizione patrimoniale *voluta* concretamente dalla vittima.

Tale condizione non ricorre nelle pur frequenti truffe realizzate nel *web* attraverso effettivi "artifici e raggiri" indirizzati a vittime in carne ed ossa, spesso

sprovvedute ed ignare delle possibilità di manipolazione dei dati e dei siti informatici, come accade nelle vendite a distanza, in cui si trasmettano false bolle di spedizione della merce, per conseguirne il pagamento, disposto poi dalla vittima; od in molte ipotesi di c.d. *phishing*, in cui l'autore induce la vittima (ad es. inviando una falsa e-mail che appare provenire dall'istituto bancario presso cui è appoggiato un suo conto corrente gestibile *on line*) a fornire i propri dati riservati d'accesso ai servizi *home banking* (ID e PW), poi utilizzati per operare trasferimenti od operazioni a danno del titolare, per vero a sua insaputa, con ingiusto profitto degli autori o di terzi. In tali casi, la mera circostanza che le condotte si realizzino nel *Cyberspace* non ne trasforma la natura in frodi informatiche tecnicamente intese, riscontrandosi un'effettiva "induzione in errore" del soggetto passivo che è *causa* determinante – grazie alla sua artificiosa "cooperazione" – degli eventi consumativi, benché questi conseguano senza un'*ulteriore* concreta "disposizione patrimoniale", ma *tramite* l'utilizzo abusivo delle credenziali dallo stesso volontariamente fornite (a seguito dell'errore in cui è stato indotto), che consentono l'effettivo trasferimento patrimoniale[53].

In questa fase successiva l'utilizzazione "senza diritto" delle credenziali fraudolentemente carpite integra oggi la fattispecie aggravata, introdotta dalla L. 15.10.2013, n. 119, di conversione del D.L. 14.8.2013, n. 93, che ha aggiunto un nuovo comma 3 all'art. 640-*ter* c.p., per superare le incertezze insorte al riguardo e rafforzare la tutela penale contro questi fatti illeciti, prevedendo un elemento *specializzante* così formulato: "se il fatto è commesso con *furto* o *indebito utilizzo* dell'identità digitale in danno di uno o più soggetti" (corsivi agg.). Al di là della palese improprietà terminologica del legislatore (il "furto di dati" appare essere una nozione atecnica sul piano giuridico, non essendovi alcuna sottrazione di "cosa" mobile) è chiaro che si tratta di un'ipotesi circostanziata che prevale – in base al principio di specialità *ex* art. 15 c.p. – sulla truffa comune, di cui assorbe comunque il disvalore; mentre l'ampia configurazione degli elementi modali delle condotte tipizzate dal comma 1 dell'art. 640-*ter* c.p. (alterazione "in *qualsiasi modo*"... intervento "senza diritto con *qualsiasi modalità*"....) consente di ricondurvi sia l'invio di e-mail non autentiche, sia la predisposizione di siti che appaiano falsamente essere quelli di istituti bancari o di credito, ecc.

Nonostante i limiti evidenziati, è dunque da valutare positivamente la novella, che ricorrendo ad un elemento specificamente riferibile alla *tecnologia* informa-

[53] Sulle complesse questioni giuridiche sollevate da tale poliedrico fenomeno, si vedano CAJANI-COSTABILE-MAZZARACO (a cura di), *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008; CAJANI, *Profili penali del phishing*, in *Cass. pen.*, 2007, n. 6, 2294 s.; FLOR, Phishing, identity theft e identity abuse: *le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2007, 899 s.

tica, dà espressa rilevanza penale anche ad un *nuovo* interesse, se non diritto della persona, emerso con lo sviluppo delle TIC e meritevole di apposita tutela nel *Cyberspace* (accanto al patrimonio, in questo caso): vale a dire l'"identità digitale", che si sostituisce, quale bene giuridico indirettamente protetto, alla libertà di disposizione patrimoniale, tradizionalmente considerata offesa in seconda battuta dalla truffa comune, giustificando il più severo trattamento sanzionatorio rispetto a quello delle due ipotesi base. La notazione critica da esprimere è che tale bene giuridico non rileva soltanto nel campo dei delitti contro il patrimonio, oggetto dell'intervento d'urgenza del legislatore, ma si correla strettamente alla ben più ampia sfera dei diritti della personalità, particolarmente bisognosa di protezione nella nuova dimensione globale del *Cyberspace*, a partire da quella dei dati personali, che soltanto trovano presidio contro "trattamenti" illeciti nell'ambito della disciplina generale della *privacy* (art. 167 Codice privacy, la cui formulazione è stata ora dall'art. 15 D.Lgs. 10.08.2018, n. 101, emanato per dare attuazione al Regolamento UE 689/2016 del 27.4.2016, su cui si veda lo specifico contributo di Labianca *infra*, Parte II, cap. XXIV).

*L'accesso abusivo* – La seconda fattispecie paradigmatica che merita attenzione per la tipizzazione di condotte inconcepibili al di fuori del contesto informatico è quella che punisce l'accesso abusivo ad un sistema informatico o telematico, cui fanno da contorno le fattispecie prodromiche di cui agli artt. 615-*quater* (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*) e 615-*quinquies* c.p. (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*).

Si tratta di un delitto a sua volta prodromico rispetto a molteplici altre condotte delittuose nel *Cyberspace*, non a caso collocato al primo posto della lista dei reati da incriminare sia nella Convenzione *Cybercrime* del 2001, sia negli strumenti di armonizzazione europei del 2005 e del 2013, laddove nelle risalenti Raccomandazioni del Consiglio d'Europa del 1989 aveva una posizione secondaria, tanto da essere stato collocato soltanto alla lettera e) della c.d. lista obbligatoria e da non aver neppure trovato ingresso in importanti ordinamenti giuridici, quale quello della Repubblica federale tedesca, che non lo aveva previsto fra i reati informatici introdotti nel codice penale dalla c.d. seconda legge contro la criminalità economica del 1986 (2. WiKG)[54].

In effetti è stata la possibilità di commissione in rete – "da remoto" – che lo ha reso particolarmente temibile dopo l'apertura al pubblico di Internet, in cui trova frequente realizzazione in molteplici contesti e con svariate modalità e scopi.

[54] Per un'analitica ricostruzione in lingua italiana sia consentito rinviare Picotti, *Studi*, cit., 33 s.

La formulazione del nostro codice riecheggia le condotte incriminate dal delitto di violazione di domicilio di cui all'art. 614 c.p., per la dichiarata analogia che il legislatore del 1993 ravvisava fra "domicilio informatico" e domicilio fisico tradizionalmente inteso, la cui tutela sarebbe parimenti fondata costituzionalmente sull'art. 14 Cost. Per cui non solo presenta analoghi limiti edittali di pena, ma si articola altresì nelle due condotte dell'"introduzione" abusiva ed – a differenza di quanto previsto a livello internazionale e nella maggioranza degli altri ordinamenti – anche del "mantenimento" (dopo un accesso legittimo) contro la volontà del titolare dello *jus excludendi*.

La diversità strutturale di queste due ipotesi è però ben presto emersa, sia con riferimento alla necessità di definire la condotta di "introduzione" nel sistema, ovviamente alla stregua della tecnologia informatica, con non poca difficoltà di fissare il correlativo *tempus* e soprattutto *locus commissi deliciti*; sia con riguardo alla specifica delimitazione della condotta di "mantenimento" penalmente rilevante, logicamente successiva ad un'introduzione autorizzata, che resterebbe altrimenti assorbita nell'accesso abusivo.

Le Sezioni unite della Corte di Cassazione sono già state chiamate in tre occasioni a definire un orientamento coerente su tali questioni, riuscendovi solo in parte, di fronte alle perduranti incertezze e ai contrasti giurisprudenziali.

Quanto al primo profilo, la sentenza del 2015 (ric. Rocco) ha individuato il *luogo di commissione* in quello in cui si trova l'autore che opera l'accesso, introducendosi o mantenendosi così nel sistema, non invece in quello del server del sistema aggredito (nella fattispecie: il terminale periferico di accesso in Napoli, anziché il server centrale della motorizzazione civile in Roma), data l'affermata "unitarietà" ed "immaterialità" della stessa nozione di sistema informatico[55]. Ma restano forti perplessità concettuali e difficoltà di applicazione, acuite dai sempre più frequenti casi di ricorso a dispositivi mobili, che aumentano gli ostacoli per le attività investigative e per l'esigenza di prossimità alla prova, non agevolando l'azione di tutela delle vittime.

In realtà il *momento* consumativo dell'"introduzione" (che non coincide esattamente con il concetto prodromico di "accesso" utilizzato invece nella rubrica e nella terminologia delle fonti sovranazionali) può ravvisarsi solo quando e laddove si sia esplicato un effettivo controllo *informatico* delle credenziali od azioni d'accesso, che in rete avviene tramite *connessione* telematica fra terminale e server, presso il quale ultimo soltanto può dirsi precisamente *perfezionata* l'"introduzione", come fase finale della procedura, distinta dalla previa mera

[55] Cass., SS. UU., 26.3.2015 (dep. 24.4.2015), Rocco, n. 17325, in *Dir. pen. e processo*, 2015, 1296 s., con nota critica di Flor, *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite*. Più in generale cfr. Id., *infra* cap. IV.

"immissione" dei dati, che ancora non implica alcun effettivo *trattamento* automatizzato operato dal sistema *nell'ambito* degli "spazi informatici" di cui è titolare la vittima.

Quanto alla condotta di "mantenimento", essa può assumere rilevanza penale solo quando e laddove infranga – in un momento *successivo* all'"introduzione" – le regole e le disposizioni dell'avente diritto, circa le "azioni" che si possono porre in essere *in* detti spazi informatici. Per cui *a fortiori*, sotto il profilo della tecnologia informatica, quest'attività si svolge nel luogo in cui è posto il server (ivi comprendendosi il *cloud* e qualsiasi altro dispositivo o memoria, in cui si collochino fisicamente gli spazi informatici, disponibili esclusivamente in capo al loro titolare), non certo nel luogo in cui è posto invece il terminale periferico da cui vengono soltanto immessi i dati.

Come si è premesso (cfr. *supra* § 2), non è infatti il mero segmento dell'azione umana materialmente intesa (quella dell'operatore che agisce al terminale digitando dati), che può integrare il "fatto" tipico, concretamente *offensivo* degli interessi giuridici protetti, ma solo la sua connessione con il trattamento *automatico* che ne consegue e che la "sostituisce" nelle ulteriori decisive fasi, realizzate in base al *software* dal sistema informatico, il quale solo idealmente e fittiziamente può però ridursi ad un'unitaria ed in tal modo indistinta realtà "immateriale", come ipotizza la Suprema Corte, non coincidendo affatto con l'intero *Cyberspace*.

Quanto al secondo profilo, concernente i requisiti più specifici della condotta di "mantenimento" illecito, una prima sentenza delle Sezioni unite del 2011 (ric. Cusani) ha stabilito che è penalmente rilevante la condotta del soggetto che, pur legittimato all'accesso, violi *oggettivamente* le condizioni ed i limiti imposti dal titolare per disciplinarlo, anche con misure organizzative o prassi aziendali, a nulla rilevando gli scopi e le finalità soggettive dell'autore che si "mantenga" nel sistema in contrasto con quelle disposizioni (nella specie un pubblico ufficiale, utilizzando le proprie credenziali di autenticazione e di accesso, si era introdotto nel sistema informatico S.D.I., protetto da misure di sicurezza, operando poi per finalità diverse da quelle istituzionali)[56].

Tuttavia una più recente sentenza del 2017 (ric. Savarese) ha precisato – per vero con riguardo all'ipotesi aggravata di cui al comma 2, n. 1 dell'art. 615-*ter* c.p., che fa espresso riferimento al pubblico ufficiale od incaricato di pubblico servizio, che commetta il fatto "con *abuso* dei poteri o *violazione* dei doveri ine-

[56] Cass., SS. UU., 27.10.2011 (7.2.2012) Casani, n. 4694, *ex multis* in *www.penalecontemporaneo.it* (2.5.2012), con nota di FLOR, *Verso una rivalutazione dell'art. 615* ter *c.p.?* a commento vedi anche SALVADORI, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615*-ter *c.p.*, in *Riv. trim. dir. pen. economia*, 2012, 369 s.

renti alla funzione od al servizio" (corsivi aggiunti) – che il delitto è commesso anche quando l'agente "pur non violando le prescrizioni formali impartite dal titolare" del sistema per delimitarne l'accesso, vi acceda o vi si mantenga "per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita" (nella specie un cancelliere accedendo al Registro informatico delle notizie di reato REGE aveva visionato il fascicolo processuale di un conoscente)[57].

In tal modo, più che dar rilievo alle finalità soggettive dell'agente, e dunque senza affatto entrare in contrasto per tale aspetto con la precedente sentenza Cusani, come da taluno sostenuto, la Corte di legittimità ha sovrapposto il concetto di "abusività" – quale violazione delle specifiche regole di gestione del sistema informatico – all'"abuso" o, meglio, allo "sviamento" dei poteri e doveri *pubblicistici* dell'agente, in questi termini qualificato ai fini dell'applicazione dell'aggravante. Ma l'esito non sembra criticabile, se si considera che viene utilizzato un criterio pur sempre oggettivo e di natura normativa, analogo a quello che traspare dalla struttura del delitto di rivelazione o utilizzazione di segreti d'ufficio, di cui all'art. 326 c.p., in cui parimenti converge la tutela del bene giuridico "finale" (del buon andamento e dell'imparzialità della pubblica amministrazione) con quella del bene giuridico "strumentale" della segretezza delle notizie conosciute per ragioni d'ufficio. E non diversa è la natura delle "ragioni d'ufficio" per cui è conferita e, dunque, necessariamente *limitata* – con "regole" di condotta di carattere *anche* generale, non solo tecniche – la facoltà d'accesso del pubblico ufficiale al sistema informatico dell'amministrazione cui è addetto, che rappresentano dunque un elemento normativo extrapenale della fattispecie in esame, non necessariamente coincidente con disposizioni di natura tecnico-informatica che specificamente debbano disciplinare l'accesso al sistema stesso ed il suo utilizzo.

In definitiva, la norma incrimina ogni *oggettiva* violazione dell'esclusiva disponibilità", in capo al titolare, degli *spazi* informatici cui ha diritto (*jus excludendi alios*), in quanto instaura un *rapporto conflittuale* apprezzabile con riguardo non solo alle procedure informatiche che *tecnicamente* abilitano e legittimano l'"introduzione" e l'utilizzo del sistema, ma anche con riguardo alle regole e disposizioni generali, pur se non strettamente informatiche, aventi contenuto precettivo, poste dal titolare del sistema od a lui riferibili anche per rego-

[57] Cass., SS. UU., 18.5.2017 (8.9.2017) Savarese n. 41210, in *www.penalecontemporaneo.it* (3.10.2017), con nota di BERTOLISI, *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere*; cfr. anche FLOR, *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir. pen. e processo*, 2018, 506 s.

lare il successivo "mantenimento" in tali spazi, che è da qualificare *contra jus* se in *contrasto* con la sua "volontà". Questa non è naturalmente da intendere in termini psicologici o soggettivi, essendo del resto ben difficilmente concepibile e riconoscibile in capo ad un ente o ad un'amministrazione, quanto sul piano *oggettivo* delle regole e disposizioni con cui viene ad esternarsi, che sono anche indirettamente integrate dalla disciplina delle competenze e delle attività d'ufficio, come di regola avviene nel caso di organizzazioni complesse, sia private che pubbliche, costituendo pertanto il requisito dell'abuso dei poteri o della violazione dei doveri (richiesto dall'aggravante di cui al comma 2 dell'art. 615-*ter* c.p.) un elemento normativo extrapenale, che integra la tipizzazione del "fatto" oggettivamente costitutivo del reato.

*5.1.2. Estensioni per "analogia" legislativa di fattispecie preesistenti a nuovi oggetti "materiali" e relative modalità di condotta*

In altre ipotesi, il legislatore non ha formulato fattispecie incriminatrici integralmente nuove, essendosi limitato a ridefinire o aggiungere oggetti passivi o materiali "nuovi", ovvero talune "nuove" modalità di condotta, alla tipizzazione di fattispecie comuni già esistenti, secondo un criterio di "analogia" che per il resto rinvia direttamente ad esse o ne riproduce gli elementi essenziali.

*Le falsità informatiche* – Emblematiche di questa tecnica di tipizzazione sono le falsità informatiche, create dal legislatore italiano con una semplice formula normativa di estensione espressa, con cui ha dichiarato applicabili le fattispecie di "falsità in atti" contenute nel capo III del titolo VI del libro secondo del codice penale, quando abbiano ad oggetto i "documenti informatici" sia "pubblici" che "privati", secondo le rispettive ripartizioni. Ed in un primo momento ha offerto anche un'autonoma definizione, ai soli effetti penali, di "documento informatico" (art. 491-*bis*, parte seconda, c.p., nella formulazione introdotta dalla L. n. 547/1993), non esistendo allora, nell'ordinamento giuridico interno, una nozione extrapenale cui riferirsi e non potendosi estendere per analogia, con effetti *in malam partem* in ambito penale, la nozione tradizionale di "documento", come pure la giurisprudenza ha in taluni casi inaccettabilmente affermato[58]. In un secondo tempo, la criticabile definizione di documento informatico, analogicamente imperniata sul requisito del "supporto informatico" visto quale equivalente fisico-materiale del supporto cartaceo, è stata opportunamente soppressa, avendone il successivo sviluppo tecnologico dimostrato l'inconsistenza,

[58] Cass., sez. V, 24.11.2003 (dep. 12.3.2004), n. 11915 con riguardo a falsi dati inseriti nell'Albo nazionale costruttori.

del resto fin da subito denunciata in dottrina[59]. La natura essenzialmente logica ed immateriale del "documento informatico", destinato per sua natura a circolare nella rete, in cui si svolge il traffico giuridico, è stata colta infatti meglio in sede extrapenale, a seguito anche della segnalata apertura di Internet all'accesso del pubblico: tanto che già con il D.P.R. 10.11.1997, n. 513, recante le prime disposizioni sulla formazione e comunicazione di documenti informatici nella pubblica amministrazione e sulle firme elettroniche, era stata data (all'art. 1, lett. a) una definizione giuridica del tutto indipendente dal legame con qualsivoglia "supporto", imperniata su un elemento normativo extragiuridico di natura tecnica (il carattere "*informatico*" della "rappresentazione...di atti, fatti o dati"), idoneo a recepire ogni modalità e sviluppo anche futuri delle TIC, ed uno di natura giuridica (che essi siano "*giuridicamente* rilevanti"), il quale rinvia alle specifiche discipline dei diversi settori dell'ordinamento, applicandosi dunque a quello penale. Definizione poi transitata senza modificazioni nell'art. 1 (R) D.P.R. 28.12.2000, n. 445 ed, infine, nel vigente testo unico denominato Codice dell'amministrazione digitale (D.Lgs. 7.3.2005 e succ. mod.), il cui art. 1, lett. p) recita ancora: "*Documento informatico*: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

La L. n. 48/2008, di ratifica della Convenzione *Cybercrime*, è stata l'occasione per sopprimere dal testo dell'art. 491-*bis* c.p. l'infelice definizione offerta "agli effetti penali" dal legislatore del 1993, recuperandone solo la "finalità probatoria", che appare più stringente nel selezionare la qualità "documentale" dei dati e delle informazioni meritevoli di protezione penale, ai sensi delle specifiche norme in materia di falsità in atti, rispetto al requisito generale della "rilevanza giuridica" contenuto nella riportata definizione extrapenale di documento informatico, lasciando tuttavia irrisolti i problemi di coordinamento sistematico, nascenti anche dalla deprecabile tecnica del rinvio all'insieme indiscriminato delle fattispecie penali contenute nel menzionato capo VII del codice penale, e peraltro solo ad esse[60]. Da ultimo è da segnalare che con l'art. 4, comma 5, D.Lgs. 15.1.2016, n. 7, di attuazione della delega contenuta nella L. 28.4.2014, n. 67, sono stati esclusi dal novero delle fattispecie oggetto del rinvio di cui all'art. 491-*bis* c.p. i delitti di falsità in documenti informatici "privati", che al pari di quelli di falsità in scritture private tradizionali sono ora trasformati in "illeciti civili sot-

[59] Sia consentito rinviare a Picotti, *Commento art. 3 L.23.12.1993, n. 547 (art. 491* bis *c.p.)*, in *Legislazione pen.*, 1996, 62 s., in specie 73-74, riprendendo peraltro notazione già anticipate in Id., *Problemi penalistici in tema di falsificazione di dati informatici*, in *Dir. informaz. e informatica*, 1985, 939 s.

[60] Volendo Picotti, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e processo*, 2008 n. 6, 700 s. Sulle numerose altre ipotesi di falsità documentali, sanzionate in disposizioni collocate in diversi capi del codice penale od in leggi speciali, vedi già Picotti, *Commento art. 3*, cit., 91.

toposti a sanzioni pecuniarie". Ma i problemi applicativi segnalati non sono certo con questo risolti, bensì estesi anche alla nuova disciplina extrapenale.

*La c.d. violenza informatica* – In altri casi, il legislatore è ricorso ad una tecnica legislativa ancor più criticabile, perché ha semplicemente dilatato concetti tradizionali – come quello di "violenza sulle cose", di cui all'art. 392, comma 2, c.p., ovvero di "corrispondenza", di cui all'art. 616, ultimo comma, c.p., applicabili a diverse fattispecie penali: cfr. *infra* – fino a ricomprendervi anche altre ipotesi, riferibili alla ben diversa realtà informatica. In specie, con la L. n. 547/1993 ha aggiunto un nuovo comma 3 all'art. 392 c.p., per ricondurre alla nozione di "violenza sulle cose" *anche* ("altresì") quella c.d. informatica, che si ha quando "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" (corsivi aggiunti). Scelta tecnicamente criticabile, perché confonde piani e concetti eterogenei, con un'inaccettabile equiparazione fra un intervento di danneggiamento – seppur anche funzionale – su un oggetto fisco-materiale, qual è la "cosa", ed uno invece variamente realizzabile di "manipolazione" del *software* o anche dell'*hardware* di sistemi informatici o telematici, che ne determini solo un'alterazione o un "turbamento" nel funzionamento. In tal modo si rarefà, fino a farla scomparire, la distinzione basilare fra *mezzo* "violento" e *mezzo* "fraudolento" di commissione dei delitti, su cui il codice penale fonda invece la stessa distinzione sistematica di quelli contro il patrimonio (rispettivamente fra quelli del capo I e quelli del capo II del titolo XIII). Si tratta di una "rarefazione" che, seppur non colta dal legislatore che mantiene un nominale concetto unitario di "violenza", riflette le caratteristiche peculiari dell'informatica. Infatti l'automazione dei processi e delle attività non comporta solo un mutamento dell'"oggetto" dei comportamenti penalmente rilevanti (che in queste ipotesi era la "cosa"), ma – a monte – per l'evidenziata "sostituzione" dell'azione fisica dell'uomo con quella del sistema informatico, anche una trasformazione strutturale delle *modalità* di realizzazione – come dimostra esemplarmente il ricordato caso dell'estorsione *on line* mediante criptazione illegittima di dati altrui: cfr. *supra* § 3 e come si vedrà esaminando di seguito i delitti di danneggiamento informatico – anche quando l'effetto nel *rapporto* con la vittima titolare del sistema aggredito e, dunque, il suo disvalore giuridico possano essere sostanzialmente equivalenti.

*I danneggiamenti informatici* – Un chiaro riflesso di tale processo d'incidenza delle TIC sulla struttura dei reati informatici si manifesta anche nell'ambito dei delitti di danneggiamento. Il legislatore del 1993 era intervenuto una prima volta, inserendo un nuovo art. 635-*bis* dopo l'art. 635 c.p., per punire il danneggiamento avente ad oggetto "dati, informazioni e programmi informatici" anziché "cose mobili o immobili altrui", cui quelli non potevano essere assimilati. Non aveva però portato sostanziali modifiche alla tipizzazione delle condotte puni-

bili ("distruggere, disperdere, deteriorare o rendere in tutto o in parte inservibili"), salva l'aggiunta di due autonome e più gravi ipotesi delittuose nell'art. 420 c.p., che punisce – fra i reati contro l'ordine pubblico di cui al Titolo V della parte speciale – l'"attentato a impianti di pubblica utilità", sanzionando "fatti diretti" a danneggiare anche programmi, dati o sistemi di interesse pubblico. Con la menzionata novella legislativa del 2008, dando attuazione – in maniera non del tutto condivisibile, sul piano tecnico normativo e su quello delle scelte di politica criminale – agli artt. 4 e 5 della Convenzione *Cybercrime* del 2001, che distinguono fra "interferenze" rispettivamente sui dati e sui sistemi, il legislatore italiano ha interamente rivisto i reati in esame, delineando un microsistema di ben quattro fattispecie delittuose[61]. Da un lato ha voluto tener conto della menzionata bipartizione prevista dalle fonti sovranazionali fra attacchi ad "informazioni, dati e programmi" (art. 635-*bis* c.p., profondamente riformulato e punibile a querela nell'ipotesi base) ed attacchi a "sistemi informatici o telematici" (nuovo art. 635-*quater* c.p.); dall'altro ha inteso mantenere anche la distinzione fra tali ipotesi e quelle più gravi, formulate come fattispecie autonome, relative rispettivamente ad informazioni, dati e programmi di "pubblica utilità" (art. 635-*ter* c.p.) ovvero sistemi informatici di "pubblica utilità" (art. 635-*quinquies* c.p.), derivate dall'originaria previsione dell'art. 420 c.p., di cui sono stati corrispondentemente soppressi i commi 2 e 3. Ma di questi ultimi è stata mantenuta la struttura di delitti di attentato, in luogo di quella di evento, che caratterizza i comuni danneggiamenti, e gli stessi elevati limiti edittali.

Meritano di essere segnalate anche le modifiche ed estensioni che si sono inoltre avute nella formulazione delle condotte delittuose, emblematiche del passaggio dai *Computer Crime* ai *Cybercrime*. Accanto a quelle basilari espresse dai verbi "distruggere, deteriorare, cancellare, alterare o sopprimere" in tutto o in parte (artt. 635-*bis* e 635-*ter* c.p.), si è aggiunta – nelle fattispecie concernenti gli attacchi a sistemi informatici – la modalità specifica dell'"introduzione" o "trasmissione" di *malware*, nonché l'ipotesi del tutto nuovo dell'"ostacolare gravemente il funzionamento" del sistema (artt. 635-*quater* e 635-*quinquies* c.p.), che tiene conto dell'esperienza criminologica, in particolare degli attacchi c.d. di DoS (*denial of service*) od analoghi, specificamente concepibili nel *Cyberspace*, in cui la molteplicità insostenibile di richieste o accessi contemporanei ad un sito, pur se singolarmente leciti, ma organizzati su larga scala – per lo più per ragioni di protesta o dimostrative – con appositi *malware* previamente diffusi illegittimamente nei computer di migliaia di ignari utenti, impediscono al sistema attaccato di rispondere regolarmente e ne "intasano", per periodi più o meno lunghi, il

[61] Cfr. SALVADORI, *Il microsistema normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. e proc. pen.*, 2012, 204 s.

funzionamento, anche se di per sé non lo "danneggiano" materialmente nelle strutture né nel *software*, creando però gravissimi danni e perturbazioni.

Si ha così un evidente riscontro positivo che, modificando l'*oggetto* "materiale" dei fatti di reato, rispetto a quelli comuni "analoghi", ma imperniati su tradizionali modalità dell'azione fisicamente intesa, l'incidenza delle TIC e della nuova dimensione del *Cyberspace* va necessariamente a toccare ed innovare anche la configurazione delle condotte tipiche ed il contenuto lesivo dei "fatti" costitutivi di reato, integranti l'offesa di beni giuridici corrispondentemente "rinnovati" rispetto a quelli tradizionali. Nelle ipotesi in esame, questi si collocano al di là della dimensione patrimoniale che connota la tutela dell'*integrità* delle "cose" nei comuni delitti di danneggiamento, abbracciando quell'aspetto *funzionale* specificamente discendente dall'*automazione* dei trattamenti, secondo i programmi predisposti dai rispettivi titolari, e la loro utilità per una pluralità di soggetti ed interessi comuni, già in parte emerso con la pur infelice estensione normativa del concetto generale di "violenza sulle cose".

*La corrispondenza informatica* – Con il comma 4 aggiunto all'art. 616 c.p., il legislatore ha stabilito fin dal 1993 che: "Agli effetti delle disposizioni di questa sezione [V del capo III del titolo XII, dedicata all'inviolabilità di segreti] per corrispondenza si intende quella epistolare, telegrafica, telefonica, *informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza*" (corsivi aggiunti). Dunque neppure in tal caso si è fatto ricorso ad una definizione *ad hoc* dell'oggetto materiale delle condotte punibili, ma si è soltanto estesa l'applicabilità di tutte le fattispecie in materia di corrispondenza alle nuove forme di "comunicazione", addirittura chiudendo l'elencazione con una formula aperta all'evoluzione tecnologica futura ("*ogni altra forma* ..."), che rischia, per la sua indeterminatezza, di consentire estensioni analogiche *in malam partem*, evitabili solo circoscrivendo concettualmente il *genus* cui possano ricondursi le varie *species*, comprese quelle non (ancora) espressamente denominate o disciplinate dal legislatore[62]. Operazione non semplice, vista la peculiarità strutturale e soprattutto varietà delle nuove forme telematiche di comunicazione, che come sopra evidenziato coinvolgono "attivamente" una possibile pluralità di destinatari e consentono la circolazione, simultanea o meno, nell'ambito di gruppi, reti sociali, *chat* aperte, ecc.

Inoltre, appare spesso problematica la distinzione fra comunicazioni informatiche e telematiche che devono ricadere sotto la disciplina (meno severa) della "corrispondenza" e quelle invece da ricondurre alla disciplina più rigorosa delle "intercettazioni", parallelamente estesa a quelle informatiche e telemati-

[62] Cfr. PECORELLA, *Il diritto penale cit.*, 292 s.; volendo anche PICOTTI, *Commento art. 5 L.23.12.1993, n. 547 (art. 616, comma 4 c.p.)*, in *Legislazione pen.*, 1996, 109 s., in specie 115 s.

che (nuovi artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p., parimenti introdotti dalla L. n. 547/1993). Distinzione che ha rilevanti ricadute non solo sul piano dei requisiti di tipicità dei relativi reati e delle pene applicabili, ma anche in campo processuale, con specifico riguardo alla diversa disciplina dei sequestri, da un lato (in specie *ex* artt. 254, 254-*bis* ss. c.p.p.), e delle intercettazioni, dall'altro (art. 266-*bis* c.p.p.)[63].

Anche in tali ipotesi, dunque, si palesa la necessità di rileggere le diverse fattispecie penali alla luce dei caratteri specifici delle TIC, che vanno ad incidere – a seconda delle varie procedure *automatizzate* di trasmissione, memorizzazione, messa a disposizione in rete di dati di ogni genere, sia scritti che vocali o visivi, e ad un numero limitato ovvero indiscriminato di destinatari od utenti, ecc. – sulla struttura stessa delle modalità di "comunicazione" fra persone, e dunque sulle varie condotte punibili di "presa di cognizione", "sottrazione", "distrazione", "distruzione", "soppressione", "rivelazione", richiedenti (*ex* art. 616, commi 1 e 2, c.p.) l'ulteriore individuazione dei requisiti per definire una "corrispondenza informatica" come "chiusa"[64]. Inevitabili sono le ripercussioni anche sulla definizione del bene o dei beni giuridici tutelati, che non possono circoscriversi alla dimensione meramente "privata" della relazione comunicativa fra mittente e destinatario, che è alla base del "segreto" epistolare, lasciata alla piena disponibilità del titolare del relativo diritto, anche di querela, *ex* art. 616, comma 3, c.p., dato che ora viene invece in rilievo anche la generale sicurezza e correttezza, oltre che riservatezza, delle varie forme di scambio e circolazione nel *web*, capaci di coinvolgere contemporaneamente od a catena pluralità assai ampie o indeterminate di utenti.

### *5.2. Collocazione sistematica e beni giuridici protetti*

Per riassumere in un quadro sinottico, seppur senza pretesa di completezza, i principali reati informatici "in senso stretto" (con qualche riferimento ad alcuni qualificabili "in senso ampio": sulla distinzione cfr. *infra* § 5.3.2), previsti nel nostro codice penale, seguendone la collocazione sistematica voluta dal legisla-

[63] In argomento si veda PECORELLA, *Il diritto penale*, cit., 302 s.; ed *infra* Parte IV, cap. 6.

[64] Il recente D.Lgs. n. 101/2018 contenente disposizioni di adeguamento del Codice privacy al GDPR dell'Unione europea 2016/679, al nuovo comma 1-*bis* dell'art. 121 relativo ai "servizi interessati" contiene alla lettera m) la seguente definizione di "posta elettronica": "messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza". Seppur non direttamente traslabile nella disciplina penale in esame, la definizione è rilevante perché tipizza il carattere comunicativo fra persone del messaggio, che è destinato alla "conoscenza" del suo contenuto da parte del ricevente, avvenuta la quale perde il suo requisito distintivo rispetto ad altre categorie di dati.

tore per conservare il più possibile la corrispondenza e la vicinanza rispetto alle fattispecie comuni preesistenti, poste a tutela di beni giuridici ritenuti simili – pur se con scelte non sempre convincenti e condivisibili – si può procedere ad un'elencazione schematica, che muove dal nome dei titoli, dei capi o delle sezioni in cui si trovano, ma diretta ad evidenziare la molteplicità dei beni giuridici protetti ed, in molti casi, la loro *novità* o specificità, rispetto a quelli "analoghi" cui sono correlati.

Nel Titolo I del Libro II, fra i "delitti contro la personalità dello Stato", si trovano nel capo I – che tutela la "personalità internazionale" – alcuni delitti contro il terrorismo, introdotti a partire dagli attentati dell'11.9.2001 di fronte alla recrudescenza del terrorismo islamista, che palesemente riflettono – rispetto agli analoghi reati preparatori od accessori in materia – la nuova dimensione globale del *Cyberspace*, in cui anche tali fenomeni ormai si manifestano: quali l'assistenza agli associati (art. 270-*ter* c.p.), che prevede fra le varie condotte consumative anche quella di "fornire....strumenti di comunicazione" (fra cui possono ovviamente rientrare anche quelli informatici o telematici: per cui il reato può essere un reato informatico e cibernetico "in senso ampio"), nonché l'addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinquies* c.p.), che prevede al comma 2 l'esaminata ipotesi aggravata della commissione "attraverso strumenti informatici o telematici" (da considerare invece per questo "in senso stretto": cfr. *infra* § 5.3.1).

Nel Titolo III, fra i "delitti contro l'amministrazione della giustizia" si colloca invece nel capo III, che sanziona la "tutela arbitraria delle proprie ragioni", la norma definitoria di cui al nuovo comma 3 dell'art. 392 c.p., contenente l'esaminata nozione generale di violenza c.d. informatica, equiparata a quella "sulle cose" (cfr. *supra* § 5.1.2).

Nel Titolo VII, che raccoglie l'ampio novero dei "delitti contro la fede pubblica", ed in specie nel suo capo III dedicato alle "falsità in atti", si colloca la norma estensiva di cui all'art. 491-*bis* c.p., con cui vengono punite le falsità informatiche (cfr. *supra* § 5.1.2); mentre nel capo IV, dedicato alla "falsità personale", è collocato il nuovo art. 495-*bis* c.p., che punisce le "false dichiarazioni al certificatore di firme elettroniche" concernenti "l'identità o lo stato o altre qualità della propria o dell'altrui persona" rilevanti per ottenere i servizi di certificazione, garantendo tutela penale all'articolata disciplina in materia di firme elettroniche, contenuta oggi nel Codice dell'amministrazione digitale (D.Lgs. n. 82/2005 e succ. mod.), in cui sono previsti, oltre a molteplici obblighi a carico dell'utente, non tutti presidiati da pena, molti altri a carico del "certificatore", la cui violazione è invece sempre (seppur genericamente) e più severamente punita dall'art. 640-*quinquies* c.p. Questa fattispecie è peraltro inopinatamente rubricata: "frode informatica del soggetto che presta servizi di firma elettronica" ed

è impropriamente collocata fra i delitti contro il patrimonio "mediante frode" di cui al capo II del Titolo XIII: ma la condotta punibile si esaurisce nella mera "violazione" di tutti i richiamati obblighi incombenti sul soggetto qualificato ed il reato proprio che viene così tipizzato non richiede alcun connotato di fraudolenza, né alcun evento di danno, essendo sufficiente il dolo specifico di arrecarlo, in alternativa a quello di "procurare a sé o ad altri un ingiusto profitto"[65]. Per cui è evidente che il bene giuridico protetto non è il patrimonio, ma la fede pubblica nello specifico campo dei documenti informatici.

La maggior parte dei reati informatici si colloca nel Titolo XII fra i "delitti contro la persona", ed in specie nel suo ampio capo III, dedicato ai "delitti contro la libertà individuale", ripartiti fra le diverse sezioni.

Nella prima, che riguarda i "delitti contro la personalità individuale", si trovano quelli a tutela dei minori contro le c.d. nuove schiavitù, e dunque tutti i delitti di pedopornografia (artt. 600-*ter*, 600-*quater*, 600-*quater*.1 c.p.), mentre nella sezione II, che riguarda i "delitti contro la libertà personale", è collocato il delitto di adescamento di minorenni (artt. 609-*undecies* c.p.), che prevede fra i suoi reati-fine anche molti delitti sessuali, collocati nella medesima sezione, ma anche di prostituzione minorile, di schiavitù, di pedopornografia, ecc., per cui può qualificarsi come reato cibernetico (in senso ampio: *infra* § 5.3.3).

Nella sezione III, fra i "delitti contro la libertà morale", si colloca il delitto di atti persecutori aggravato dall'uso di "strumenti informatici o telematici" (artt. 612-*bis*, comma 2, c.p., qualificabile come reato cibernetico: *infra* § 5.3.3); mentre nella sezione IV, dedicata all'"inviolabilità del domicilio", si collocano i delitti di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.) ed i relativi reati prodromici (artt. 615-*quater* e 615-*quinquies* c.p.), che sono reati informatici in senso stretto (cfr. *infra* § 5.3.1).

Infine, nella sezione V, che raccoglie i "delitti contro l'inviolabilità dei segreti", vi sono le fattispecie poste a tutela sia della corrispondenza, anche "informatica" o "telematica" (art. 616 c.p. su cui cfr. *supra* § 5.1.2), sia delle altre comunicazioni, anche "informatiche o telematiche", contro le intercettazioni illecite (artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p.). Da richiamare è altresì l'art. 621 c.p., che punisce la rivelazione del contenuto di "documenti segreti", il cui comma 2, aggiunto dalla L. n. 547/1993, espressamente include "anche qualunque supporto informatico contenente dati, informazioni o programmi", riproducendo l'infelice espressione che era stata usata dal legislatore

[65] Sulle ragioni di tale impropria collocazione e denominazione, dirette ad escludere connotati pubblicistici nei servizi di certificazione delle firme elettroniche, in malinteso ossequio alle direttive europee intese a garantire la natura privatistica e la concorrenza nel settore, sia consentito rinviare a PICOTTI, *La ratifica della Convenzione*, cit., 704.

per definire la nozione di "documento informatico" nella formulazione originaria dell'art. 491-*bis* c.p. Ma mentre questa è poi stata opportunamente soppressa nel 2008, in conformità all'evoluzione tecnologica della rete, sopra richiamata (*supra* § 5.1.2), non è stata modificata anche la disposizione in commento, che continua ad imperniare la nozione di "documento" – seppur non ai fini di tutela della fede pubblica – sull'obsoleto collegamento con un "supporto informatico".

Infine, la norma "di chiusura" della sezione V, di cui all'art. 623-*bis* c.p., introdotto nella sua formulazione originaria nel 1974 per contrastare le intrusioni nella riservatezza delle "comunicazioni e conversazioni telegrafiche [e] telefoniche", estendendo ad esse l'applicazione di tutte le disposizioni contenute nella sezione predetta[66], comprende – dopo la novella del 1993 – anche la menzione di quelle "informatiche o telematiche" e stabilisce che tutte tali disposizioni si applichino altresì "a qualunque altra trasmissione a distanza di suoni, immagini od altri dati", operando una discutibile apertura a possibili estensioni analogiche, in quanto risulta difficile delimitare *a priori* i caratteri identificativi della categoria (come già si è visto a proposito della simile clausola che chiude anche la definizione di "corrispondenza": cfr. *supra* § 5.1.2).

Anche l'ultimo Titolo XIII del Libro II del codice penale, dedicato ai "delitti contro il patrimonio", contiene importanti reati informatici (sia in senso stretto, che in senso ampio). Fra quelli del capo I, che raccoglie i delitti "mediante violenza", si collocano tutti quelli di danneggiamento informatico (artt. da 635-*bis* a 635-*quinquies* c.p.), compresi quelli relativi a dati e sistemi "di pubblica utilità", di cui si è detto (cfr. *supra* § 5.1.2), nei quali l'aspetto della tutela del patrimonio è quantomeno secondario. Mentre nel capo II, dedicato ai delitti "mediante frode", si colloca l'esaminato art. 640-*ter* c.p., che punisce la frode informatica, che ora prevede anche l'ipotesi aggravata della commissione "con furto o indebito utilizzo dell'identità digitale" introdotta nel 2013 (cfr. *supra* § 5.1.1), mentre dell'art. 640-*quinquies* c.p. si è appena criticata l'impropria denominazione e collocazione.

In conclusione, si ha un positivo riscontro della crescente espansione ed articolazione del diritto penale dell'informatica, cui è demandata, nel codice vigente, la tutela di essenziali beni giuridici, sia pubblici che privati, ed in particolare della persona, cui si devono aggiungere tutti quelli penalmente protetti nell'ampio campo della legislazione speciale, a partire dalla complessa disciplina in materia di dati personali, da un lato, e del diritto d'autore e dei diritti connessi, dall'altro

[66] Sulla finalità di tutela della riservatezza dalle intrusioni consentite dai nuovi strumenti tecnici di allora, quali microspie e teleobiettivi, perseguita dalla L. 8.4.1974, n. 98, si veda l'importante contributo di Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, 1079 s., ora in *Scritti diritto penale*, II, Tomo I, Milano, 1997, 2289 s.

(su cui si vedano *infra*, Parte II, i capitoli ad essi espressamente dedicati). Beni giuridici che pur configurandosi in termini di analogia, rispetto a quelli protetti dalle fattispecie comuni, cui le nuove vengono sistematicamente accostate, presentano indubbie peculiarità[67], che – come si è cercato di sottolineare – riflettono la diversa struttura dei rapporti (anche illeciti) che si svolgono, in tutto o in parte, nel *Cyberspace*.

### *5.3. Partizioni dei reati informatici e cibernetici*

Muovendo dalle esaminate previsioni legislative concernenti i reati informatici vigenti nel nostro codice penale, si può operare una più precisa classificazione sistematica, che parta dalla categoria dei "reati informatici in senso stretto" per estendersi poi alle altre nozioni finitime, da leggere quali cerchi via via più ampi, che abbracciano in termini progressivamente più generali quelle precedenti più specifiche, con le precisazioni che seguono.

#### *5.3.1. I reati informatici in senso stretto*

La prima categoria è costituita da quei reati che, alla stregua della formulazione legislativa della fattispecie incriminatrice, presentano almeno un elemento – essenziale o circostanziale – che richiama *espressamente* ed univocamente le TIC nella descrizione delle modalità di condotta, ovvero dei mezzi, degli oggetti, dell'evento, o di altre condizioni del reato: elemento che deve essere integrato ai fini della consumazione della fattispecie stessa (nella sua forma base o circostanziata). Ad esempio si possono citare alcune locuzioni, presenti nei reati già sopra esaminati: intervenire senza diritto su dati, informazioni o programmi *informatici*; introdursi o mantenersi in un sistema *informatico o telematico*; alterare od ostacolare il funzionamento di un sistema *informatico o telematico*; contraffare, alterare o sopprimere un documento *informatico*; prendere cognizione, sopprimere od alterare corrispondenza *informatica o telematica*, ecc.

Tale categoria di reati coincide solo in parte con l'elenco tassativo di quelli riservati alla competenza "specializzata" della Procura distrettuale (*ex* art. 51, comma 3-*quinquies*, c.p.p., introdotto dall'art. 11, comma 1, L. n. 48/2008 di ratifica ed attuazione della Convenzione *Cybercrime*), che da un lato ne prevede soltanto alcuni, seppur tra i più significativi, quali in specie l'accesso

[67] Per una precisa differenziazione e partizione dei beni giuridici protetti dalle fattispecie penali vigenti nell'ordinamento positivo tedesco, si veda esemplarmente SIEBER, *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag*, Verlag C.H. Beck, Munchen, 2012, in specie 18 s. per l'ordinamento italiano si veda volendo già PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 s., in specie 53 s.

abusivo ad un sistema informatico *ex* art. 615-*ter* c.p. ed i reati prodromici di cui agli artt. 615-*quater* e 615-*quinquies* c.p.; le intercettazioni informatiche *ex* artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p., oltre a due delitti concernenti invece quelle telefoniche e telegrafiche *ex* artt. 617-*bis* e 617-*ter* c.p.; i danneggiamenti informatici *ex* artt. da 635-*bis* a 635-*quinquies* c.p.; nonché le frodi informatiche *ex* artt. 640-*ter* e 640-*quinquies* c.p. D'altro lato si estende – a seguito della L. n. 172/2012 di ratifica ed attuazione della Convenzione di Lanzarote del 2007 contro lo sfruttamento sessuale dei minori – anche a delitti ulteriori, che non possono essere considerati reati informatici "in senso stretto", e taluni neppure "in senso ampio", quali in specie quelli di prostituzione minorile *ex* art. 600-*bis* c.p., di pornografia minorile *ex* artt. 600-*ter* e 600-*quater*, compresa quella virtuale *ex* art. 600-*quater*.1 c.p., le iniziative turistiche volte allo sfruttamento della prostituzione minorile, *ex* art. 600-*quinquies* c.p., l'adescamento di minori *ex* art. 609-*undecies* c.p. e l'istigazione a pratiche di pedofilia e pedopornografia *ex* art. 414-*bis* c.p. (di cui appresso si dirà). La loro inclusione non risponde, quindi, soltanto a criteri di specializzazione tecnica, e tantomeno di rispetto di una rigorosa ripartizione sistematica[68], ma piuttosto ad una scelta di politica criminale, che si è evidentemente fatta carico – sulla base delle stesse indicazioni provenienti dalle fonti sovranazionali – degli allarmanti sviluppi che la criminalità in danno dei minori ha assunto nel *Cyberspace*.

### *5.3.2. I reati informatici in senso ampio*

Sono da qualificare "reati informatici in senso ampio" quelli che *possono* realizzarsi *anche* mediante strumenti informatici o su oggetti informatici, ovvero con modalità di condotta od effetti che coinvolgono le TIC, ivi compreso quindi il *web* (per cui, in quest'ultima ipotesi, vanno a ricadere nella più vasta categoria dei "reati cibernetici", di cui appresso si dirà). Gli elementi distintivi compaiano quindi nella formulazione della fattispecie legale soltanto quale *possibile* modalità, oggetto, strumento o risultato della condotta, in alternativa ad altri considerati normativamente "equivalenti" che prescindono invece dalle TIC; od addirittura *non* compaiano espressamente nella norma, ma sono da essa ricavabili in via ermeneutica o sono comunque con essa *compatibili*.

Per cui solo alla luce della concreta modalità di commissione del reato, si potrà dire se si è da trattare e qualificare come reato informatico (in senso ampio).

Quali esempi si possono menzionare tutti i reati in materia di pornografia minorile, che possono riguardare – oltre a materiale informatico o digitale –

[68] Criticamente sull'elenco dei reati di competenza della Procura distrettuale cfr. già CASSIBBA, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in LUPARIA (a cura di), *Sistema penale*, cit., 113 s.

*anche* materiale cartaceo, fotografico, cinematografico od a stampa, compreso il materiale prodotto "con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali" (c.d. pornografia virtuale) di cui all'art. 600-*quater*.1 c.p., che rimanda ad un elemento tecnico, per lo più, ma non necessariamente, di natura informatica; ovvero, al di fuori del codice penale, fanno parte della categoria i reati in materia di disciplina dei dati personali, che possono essere trattati sia in forma digitale, sia in forma cartacea, le cui violazioni configurano in molte ipotesi un illecito penale (*ex* artt. 167 ss. del Codice privacy, riformulati dal citato D.lgs. n. 101 del 2018, su cui cfr. *infra*, Parte II, Di Florio, Labianca); od ancora le violazioni del diritto d'autore e dei diritti connessi, che possono riguardano *anche* opere in formato digitale, mentre sono certamente da considerare reati informatici in senso stretto quelli, più recentemente introdotti, che consistono in condotte che violino le "misure tecniche di protezione" o la criptazione di trasmissioni riservate (cfr. *infra*, Flor, Parte II, Cap. XXVI).

In sintesi, lo sviluppo delle TIC e l'estensione sociale del *Cyberspace*, da cui abbiamo preso le mosse per l'analisi giuridica, porta inevitabilmente ad ampliare sempre più l'ambito di questa categoria "spuria", in quanto un numero via via maggiore di reati viene commesso o può essere commesso in rete, o comunque avvalendosi od a danno di mezzi od oggetti informatici, benché il legislatore non faccia necessariamente dipendere la perfezione del reato da tale eventualità, da verificare in concreto, caso per caso: come nei già descritti esempi dell'estorsione, realizzata con la criptazione di dati informatici altrui mediante un *malware* installato da remoto, o del c.d. *cyberlaundering*, che si può consumare nel *dark web* (cfr. *infra* Plantamura, Parte II, cap. XXI).

Oggi appare più semplice parlare sinteticamente, non solo sul piano criminologico, di "reati cibernetici" (*Cybercrime*), di cui si fornirà appresso la definizione giuridica, rispetto ai quali appare irragionevole, se non arbitraria, l'inclusione solo di *alcuni* – non necessariamente i più gravi, né frequenti – nella lista di quelli riservati alla competenza specializzata della Procura distrettuale (ai sensi del citato art. 51, comma 3-*quinquies*, c.p.p.), visto che non solo la ricerca, la raccolta, la valutazione delle "prove elettroniche", ma anche il corretto inquadramento giuridico-penale, alla stregua delle fattispecie legali in cui i fatti vanno sussunti, per formulare pertinenti imputazioni, determinare la competenza territoriale (o giurisdizione, in caso sia coinvolto il territorio di Stati esteri), ecc., richiedono una specializzazione, anche tecnica, di tutto il personale giudiziario e di polizia, oltre che adeguate strumentazioni disponibili.

### *§ 3.3. Reati cibernetici*

"I reati cibernetici" sono tutti quelli che si commettono o si possono commettere in rete o nel *web* o, meglio, "nel" *Cyberspace*, in quanto la formulazione

legale delle relative fattispecie incriminatrici contiene un elemento essenziale o circostanziale che *espressamente* richiama la rete ("reati cibernetici in senso stretto"), ovvero prevede elementi di tipizzazione del "fatto" di reato che solo *implicitamente* od in via ermeneutica sono *compatibili* con la concreta realizzazione nel *Cyberspace* ("reati cibernetici in senso ampio").

Pertanto anche in questa categoria si possono distinguere i (pochi) reati cibernetici "in senso stretto", nei quali cioè la commissione "in rete" costituisce un requisito specifico essenziale, o circostanziale, *espressamente* ed univocamente previsto dal legislatore; ed i reati cibernetici "in senso ampio", in cui la "rete" compare solo quale *eventuale* o compatibile modalità, oggetto o risultato della condotta costitutiva del "fatto" di reato, che è quindi possibile sussumere anche solo *in via interpretativa* nella fattispecie base o circostanziata, alla stregua degli elementi che la costituiscono.

Tutti i "reati cibernetici *in senso stretto*" sono logicamente *anche* "reati informatici *in senso stretto*", dato che l'elemento che richiede la commissione "in rete" od in Internet o nel *Cyberspace* implica necessariamente un riferimento esplicito alle TIC. Ma non è vero l'inverso, in quanto non tutti i reati *informatici* in senso stretto sono anche reati *cibernetici* in senso stretto, potendo astrattamente l'elemento che richiama le TIC non richiedere necessariamente *anche* la commissione "in rete", seppur quest'ultima sia l'ipotesi maggiormente ricorrente: ad es. nel caso di frode informatica aggravata dal furto di identità digitale (art. 640-*ter*, comma 3, c.p.), la commissione potrebbe concepirsi anche in un sistema chiuso, per l'utilizzo abusivo delle credenziali d'accesso ad un computer, che identificano la persona legittimata. Per cui il reato (informatico "in senso stretto") deve qualificarsi come reato *cibernetico* "in senso ampio", perché solo eventualmente (anche se sempre più frequentemente) è realizzabile nel *Cyberspace*, ed è anzi stato proprio questo il motivo dell'introduzione della menzionata circostanza aggravante.

Paradigmatico della prima categoria ("reati cibernetici in senso stretto") è invece il c.d. *cyberstalking*, di cui all'art. 612-*bis*, comma 2, c.p., inserito dal D.L. n. 93/2013, conv. dalla L. n. 119/2013, che prevede un'ipotesi aggravata del delitto di atti persecutori: "Se il fatto è commesso attraverso strumenti informatici o telematici" (cfr. *infra*, Macrì, Parte II, cap. XV). Poiché tale modalità o mezzo di realizzazione, che tipizza normativamente l'aggravante con un elemento che richiama espressamente le TIC, inerisce a "condotte reiterate" di necessaria *comunicazione* con la vittima ("minaccia o molesta"), le stesse condotte non possono che realizzarsi nel *Cyberspace* – tramite la rete Internet, o altre reti di telefonia mobile o messaggistica, ecc. – pur producendo poi eventi consumativi nel mondo reale ("cagionare un perdurante e grave stato di ansia o di paura" ovvero "ingenerare un fondato timore per l'incolumità…" od ancora "costringere … ad alterare le … abitudini di vita").

Altrettanto può dirsi, ad esempio, per la già citata ipotesi aggravata del delitto di "addestramento ad attività con finalità di terrorismo anche internazionale", di cui all'art. 270-*quinquies*, comma 2, c.p., che contiene un'analoga formulazione normativa (sul punto cfr. *supra* § 5. 2).

Fra i molteplici esempi di *reati cibernetici* "in senso ampio", che abbracciano, innanzitutto, i reati informatici – sia in senso stretto, che in senso ampio – paradigmatica ed assai frequente è, fra i reati "comuni", la c.d. diffamazione *on-line*: infatti la condotta richiesta dall'art. 595 c.p. per la causazione dell'offesa alla reputazione altrui ("*comunicando* con più persone": corsivo aggiunto), pur non menzionando le TIC, è però sicuramente compatibile con ogni modalità di comunicazione nel *Cyberspace*; ed anzi la giurisprudenza, equiparando Internet ad un "qualsiasi altro mezzo di pubblicità" diverso dalla stampa, considera in tali casi il reato aggravato ai sensi del comma 3, con una generalizzazione che va in realtà circoscritta, a seconda delle caratteristiche concrete del tipo di comunicazione telematica utilizzata, perché se questa è limitata a singole persone determinate, appare ingiustificata l'applicazione dell'aggravante[69].

Fra i reati di più recente formulazione, va richiamato invece l'adescamento di minori, di cui all'art. 609-*undecies* c.p., che rientra in questa categoria perché la norma lo definisce come "qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere *anche* mediante l'utilizzo della rete internet" (corsivo aggiunto): proprio l'avverbio "anche" esclude che si possa considerare la fattispecie come reato cibernetico (ed informatico) *in senso stretto*. Ma altrettanto vale per il delitto di assistenza agli associati fornendo "strumenti di comunicazione" (*ex* art. 270-*ter* c.p., di cui già si è detto *supra* § 5.2).

È oggi in ogni caso evidente l'estensione progressiva dell'ampia categoria dei reati cibernetici, per le ragioni strutturali ampiamente analizzate, di cui anche il legislatore, non solo penale, tiene ormai conto, per combattere fenomeni allarmanti qual è, ad es., quello del c.d. cyberbullismo, oggetto della L. 29.5.2017, n. 71: pur non introducendo, opportunamente, alcun "nuovo" né specifico reato, la normativa in questione richiama possibili diverse fattispecie penali applicabili, non tutte riconducibili alle diverse categorie in esame, per introdurre piuttosto misure di sensibilizzazione e prevenzione, a partire dall'ambito scolastico ed educativo, nonché meccanismi del tutto nuovi di intervento sui comportamenti illeciti, per farli cessare, attivabili da una molteplicità di soggetti, compresi i minori degli anni 14, la cui attuazione in termini stringenti incombe poi sugli ISP, a dimostrazione, da un lato, dell'indissolubile legame od anzi immersione della vita reale "nel" *Cyberspace* già a partire dalla più giovane età e, dall'altro, del ruolo e della responsabilità degli ISP, da riconoscere in termini sempre più

[69] Cfr. *supra*, § 3 e nota 33.

incisivi, per garantire l'effettivo rispetto dei diritti e degli interessi degli utenti in rete, in particolare di quelli più vulnerabili.

Per tutta questa estesa ed eterogenea categoria di reati cibernetici si pongono questioni giuridiche comuni di carattere generale, cui già si è fatto cenno, in quanto coinvolgono la ridefinizione anche dogmatica, parzialmente nuova, di nozioni basilari di teoria del reato: quali quelle di azione e di evento, eventualmente anche di causalità e, più in generale, di "fatto" di reato nel *Cyberspace*, con relativi riflessi non solo sulla determinazione del *locus* e del *tempus commissi delicti*, ma anche delle sue forme di manifestazione (dal tentativo al concorso di persone), nonché sull'elemento soggettivo del dolo e della colpa, da adattare al nuovo contesto, connotato dall'*automazione* tecnologica, dalla *delocalizzazione* spaziale e temporale, dall'*interazione* nonché *interdipendenza* fra utenti e con soggetti terzi, compresi gli ISP. Insomma, un terreno fertile di sfide per la giurisprudenza e di stimolo per nuove ricerche scientifiche ed elaborazioni teoriche.

Va in chiusura sottolineato che, come emerge testualmente anche dall'art. 14, par. 2, lett. c) della Convenzione *Cybercrime* del 2001, *ogni altro* reato, di qualsiasi tipo, che pur *non* si commetta con azioni, strumenti od effetti "nel" *Cyberspace*, può richiedere l'acquisizione di "prove elettroniche" ed eventualmente la cooperazione ed assistenza giudiziaria internazionale per la loro ricerca, acquisizione, conservazione, circolazione, utilizzazione. Si pensi alle "tracce" di una comune corruzione, ovvero di un'associazione criminosa od anche di un omicidio, rinvenibili in file o dati elettronici di ogni genere, come *log*, *cookies*, dati di traffico, ecc., contenuti in computer, server, dispositivi esterni di memoria, nel *cloud*, ecc.[70]. Solo *impropriamente* si potrebbe parlare in questi casi di "reati cibernetici", perché sotto il profilo *sostanziale* il "fatto" costitutivo di reato *non* si colloca neppure in parte nel *Cyberspace*. Sul piano *processuale*, tuttavia, anche in questi casi l'accertamento probatorio coinvolge la ricerca, la verifica tecnica, l'acquisizione, la conservazione, la valutazione di elementi informatici e cibernetici, con tutta le connesse problematiche relative alla validità, utilizzabilità, acquisizione anche da soggetti ed ordinamenti giuridici diversi, che richiedono l'apporto indispensabile della *computer forensic*[71] e della cooperazione internazionale, oltre che – come ora si dirà – degli ISP.

[70] Basti qui il richiamo a clamorosi casi giudiziari recenti, quali l'omicidio di Garlasco od alcuni scandali per tangenti in appalti nella sanità.

[71] In argomento cfr. ZICCARDI, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in LUPARIA (a cura di), *Sistema penale*, cit., 165 s.; più in specifico i contributi periodici a cura di IISFA (*Information Forensic*) di cui v. il sito *www.iisfa.it*.

## 6. Obblighi di tutela penale degli *Internet Service Providers* e sviluppi della giurisprudenza europea

Il dibattito sui fondamenti e limiti della responsabilità penale (e non solo: ma è di questa che ci si occuperà in questa sede) degli ISP, ha segnato importanti sviluppi nell'ultimo decennio, nonostante la mancata modifica delle regole generali di esonero o di limitazione della loro responsabilità, introdotte all'inizio del nuovo millennio sulla base della menzionata Dir. CE 2000/31 sul commercio elettronico. Come noto i suoi artt. 12, 13 e 14 (sostanzialmente riprodotti negli artt. 14, 15 e 16, D.Lgs. 9.4.2003, n. 70, che vi ha dato attuazione nel nostro ordinamento) garantiscono ad essi un *safe harbour* escludendo – con diversa intensità di condizioni – che le attività rispettivamente di *mere conduit*, di *caching* e di *hosting*, cui vengono ridotti schematicamente i loro servizi in rete, possano essere fonte di responsabilità, a condizione che il "fornitore di servizi della società dell'informazione" (come viene definito l'ISP nel linguaggio giuridico europeo) si limiti ad un'attività sostanzialmente tecnica ed automatica, conforme alla tecnologia esistente, e non abbia effettiva conoscenza di eventuali contenuti illeciti. L'assenza di obblighi giuridici di controllo preventivo (l'art. 15, Dir. CE 2000/31, recepito dall'art. 17, D.Lgs. n. 70/2003, fa espresso divieto agli Stati membri di imporre "ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite"), ed *a fortiori* di impedimento di reati commessi dagli utenti o da terzi sfruttando i servizi offerti, esclude, in linea di principio, la configurabilità di una responsabilità penale non solo *ex* art. 40 cpv. c.p., ma anche a titolo di concorso nel reato *ex* art. 110 c.p., benché un contributo causale, sotto il profilo strettamente tecnico-materiale, sia ravvisabile in forza delle attività e strutture messe a disposizione dall'ISP[72].

[72] Cfr. volendo già PICOTTI, *Fondamento e limiti della responsabilità penale dei Service-providers in* Internet, in *Dir. pen. e processo*, 1999, n. 3, 379 s., e con specifico riguardo al nostro ordinamento lo, *La responsabilità penale dei* Service-providers *in Italia*, *ivi*, n. 4, 501 s., per il rilievo che *de jure condito* la responsabilità penale degli ISP poteva fondarsi sui principi generali del concorso di persone *ex* art. 110 c.p., in caso di consapevole e voluto contributo causale ai reati che fossero realizzati dagli utenti, potendosi configurare invece una responsabilità per omesso impedimento dell'evento-reato, *ex* art. 40 cpv. c.p., soltanto se sussistessero positivi obblighi giuridici di impedimento, la cui osservanza avrebbe evitato la commissione del reato da parte di terzi (ad es. utenti), peraltro ravvisabili solo in singoli determinati ambiti, come quello del contrasto alla diffusione della pedopornografia in Internet (*ex* L. n. 269/1998: contra però MANNA, *Considerazioni sulla responsabilità penale dell'*internet provider *in tema di pedofilia*, in *Dir. informaz. e informatica*, 2001, 145 s.) o della tutela dei dati personali (all'epoca L. 31.12.1996, n. 675). Per una posizione più restrittiva circa i possibili ambiti di responsabilità penale degli ISP si era espresso SEMINARA, *La responsabilità penale degli operatori su Internet*, in *Dir. informaz. e informatica*, 1998, 745 s., mentre per un quadro del dibattito sviluppatosi alla luce della Direttiva

D'altro lato, gli ISP sono stati progressivamente destinatari di molteplici obblighi e richieste di cooperazione con le attività di polizia e giudiziaria, oltre che con autorità di controllo anche amministrativo (quale ad es. il Garante della privacy, nel nostro ordinamento), per consentire o facilitare la raccolta e conservazione di prove, l'identificazione di utenti, la ricerca di tracce elettroniche di comportamenti illeciti, la cessazione concreta di violazioni o lesioni di diritti ed interessi meritevoli di protezione, non solo penale. Significativa è al riguardo la citata Convenzione *Cybercrime* del 2001, che oltre ad offrire un'ampia e generale definizione giuridica degli ISP (art. 1, lett. c), li menziona espressamente quale oggetto di molte disposizioni sia nella parte processuale (cfr. in particolare gli artt. 17, 18, 20, 21) sia in quella dedicata agli strumenti di cooperazione internazionale (ad es. art. 30).

Ma in questa sede interessa soprattutto il richiamo alla giurisprudenza europea, sia della Corte dei diritti dell'uomo di Strasburgo (in seguito: Corte EDU), sia della Corte di Giustizia comunitaria (ora dell'Unione: in seguito CGUE) di Lussemburgo, che hanno dato progressivo spazio alle nuove esigenze di tutela emergenti con l'evoluzione del *Cyberspace* e l'espansione dei rapporti che vi si svolgono, di cui si è detto (*supra* § 2), estendendo già *de jure condito* in via interpretativa possibili profili di responsabilità, anche penale, degli ISP, con corrispondenti limitazioni dei *safe harbours* introdotti dalla citata Direttiva europea, al fine di garantire la protezione di prevalenti interessi giuridici e, comunque, dei diritti fondamentali delle persone nella realtà in continua espansione della Rete.

Proprio l'affermazione dei diritti fondamentali della persona nel *Cyberspace* ha, d'altro lato, condotto la Corte di Giustizia UE a circoscrivere gli stessi obblighi di conservazione dei dati di traffico e di ubicazione degli utenti, gravanti sui fornitori di servizi di comunicazione elettronica, previsti inizialmente in termini generali ed indiscriminati dalla c.d. direttiva Frattini 2006/26 per consen-

comunitaria del 2000 e relative norme di attuazione, cfr. PETRINI, *La responsabilità penale per i reati via Internet*, Napoli, 2004. Il dibattito si è ravvivato in anni più recenti per il processo penale ai responsabili di Google Italia in relazione al caso c.d. *Vivi Down*, definito con la loro assoluzione in appello (App. Milano, 21.12.2012, n. 8611, in *www.penalecontemporaneo.it* [4.3.2013] con nota di Ingrassia), confermata in Cassazione (Cass., sez. III, 17.12.2013 [dep. 3.2.2011], n. 5107, in *Cass. pen.*, 2014, n. 6, 2060 s. con nota di Troncone; nonché in *Dir. informaz. e informatica*, 2013, 479, con nota di Resta, ivi, 502 s.; ed *in www.penalecontemporaneo* [6.2.2014] con nota di Ingrassia), dopo un'iniziale condanna in primo grado per trattamento illecito di dati personali *ex* art. 167 Codice privacy (Trib. Milano, 24.2.2010 [dep. 12.4.2010], n. 1972 in *Cass. pen.*, 2010, n. 11, 3994 s. con nota di Lotierzo). A sostegno di detto esito finale cfr. per tutti MANNA, *I soggetti in posizione di garanzia*, in *Dir. informaz. e informatica*, 2010, 779 s.; criticamente CAJANI, *Quella Casa nella Prateria: gli Internet Service Providers americani alla prova del caso Google Video*, in PICOTTI-RUGGIERI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 223 s.

tirne l'acquisizione a fini di indagini e per l'accertamento di reati da parte delle forze di polizia e dell'autorità giudiziaria: direttiva integralmente annullata dalla nota sentenza della Grande Camera dell'8.4.2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238; c.d. sentenza *Digitals Rights*), la cui portata è stata poi precisata ed in parte circoscritta nei suoi effetti sulla legislazione degli Stati membri – nel senso che essa non ne comporta *ipso jure* la contrarietà al diritto europeo – dalla successiva sentenza della medesima Grande camera del 21.12.2016 (cause riunite C-203/2015 e C-698/15, Tele 2 Servige relativa alla legislazione svedese e Watson et al. relativa a quella inglese)[73].

### *6.1. Giurisprudenza CEDU*

Muovendo dalla giurisprudenza della Corte CEDU vanno segnalate quattro sentenze importanti rispettivamente del 2008 (caso KU v. Finlandia), del 2013 (The Pirate Bay), del 2015 (Delfi v. Estonia) e del 2017 (Rolf Anders v. Svezia)[74].

In tutte, la *ratio decidendi* è fondata sul necessario *bilanciamento* fra i diritti fondamentali protetti dalla CEDU ed i sacrifici che a carico degli ISP possono conseguire per le misure da adottare, secondo un essenziale parametro di *proporzione*.

Con la prima sentenza è stata condannata la Finlandia, per non aver adempiuto al suo "obbligo positivo" di protezione del diritto alla *privacy* (*ex* art. 8 CEDU) di un minore, il cui profilo era stato postato, da un utente rimasto anonimo, su un sito di incontri *on line* con l'annuncio che il ragazzo sarebbe stato in cerca di una relazione intima. L'ISP aveva rifiutato di rivelare alla polizia l'identità

[73] La CGUE ha precisato che pur non comportando, la sentenza resa nel 2014, la contrarietà *ipso jure* al diritto dell'Unione delle normative nazionali di attuazione, queste devono comunque rispettare i principi e le condizioni posti dalla Dir. 2002/58/CE relativa alla vita privata nelle comunicazioni elettroniche e, segnatamente, il suo art. 15, come modificato dalla Dir. 2009/136/CE. Per cui, per rispettare i diritti fondamentali, le norme nazionali in materia devono stabilire che la conservazione dei dati relativi al traffico ed all'ubicazione degli utenti, che sono di per sé idonei a stabilirne il profilo, avvenga soltanto per finalità di lotta contro la criminalità grave (quali terrorismo e criminalità organizzata), rappresentando un'eccezione ai sensi del par. 1 dell'art. 15 Dir. Di conseguenza, occorre una limitazione allo stretto necessario del tempo di conservazione e una delimitazione delle categorie di dati, dei mezzi di comunicazione interessati, delle persone riguardate, con un controllo preventivo di un giudice o di un'autorità indipendente e la garanzia che i dati siano conservati nel territorio dell'Unione, nella misura e per la durata necessaria, con adeguate misure di sicurezza e protezione. Analogamente anche l'accesso a detti dati deve essere consentito alle autorità nazionali solo per corrispondenti finalità ed a condizioni chiare e precise, nonché soggetto all'autorizzazione preventiva di un giudice o di un'autorità amministrativa indipendente. In materia si veda ora la Dir. UE 2016/680 del 27.4.2016, relativa alla protezione dei dati personali di fronte ad Autorità competenti per le indagini penali e l'esecuzione di sanzioni, cui è stata data recente attuazione in Italia con D.Lgs. 18.5.2018, n. 51.

[74] Reperibili al sito ufficiale della Corte di Strasburgo: *www.echr.coe.int*.

dell'utente autore del *post*, invocando la confidenzialità delle telecomunicazioni prevista dalla legge finlandese e vista come fondamento della libertà di espressione in Internet, protetta dall'art. 10 CEDU. Questa tuttavia non poteva essere considerata assoluta, per la Corte, di fronte ad altri imperativi legittimi, come quello di prevenire reati e proteggere i diritti di terzi. Con la conseguenza che lo Stato avrebbe potuto e dovuto coinvolgere gli operatori della rete, seppur soggetti privati, non titolari di funzioni di pubblico interesse[75].

Nella seconda sentenza del 2013 la Corte di Strasburgo ha ritenuto legittima la condanna penale per concorso intenzionale, nella diffusione di materiale protetto da *copyright* in violazione dei diritti degli autori, pronunciata a carico dei responsabili del famoso sito *The Pirate Bay* che indicizzando i c.d. *Bit Torrent protocol*, consentiva ai propri utenti di condividere con software *peer2 peer* materiali cinematografici, musicali, teatrali e video giochi. Per la Corte europea, il diritto alla libertà di espressione di cui all'art. 10 CEDU, invocato dall'ISP, doveva essergli riconosciuto nella sua attività, ma bilanciato con il diritto alla proprietà intellettuale, alla stregua degli indici di cui al secondo paragrafo dello stesso art. 10, in forza del quale possono essere apposte al suo esercizio formalità, condizioni, restrizioni ed anche sanzioni, se previste dalla legge e perseguano uno o più dei fini indicati nel predetto paragrafo, nonché siano necessarie in una società democratica al loro raggiungimento.

Conseguentemente, è stata ritenuta conforme alla Convenzione la negazione, da parte dei giudici svedesi, dell'esonero da responsabilità dell'ISP, da questi invocato sulla base della citata Dir. CE 2000/31.

Anche nel terzo caso del 2015 la Corte di Strasburgo ha ritenuto che non violasse l'art. 10 CEDU la condanna penale, da parte di giudici estoni, di un ISP (denominato Delfi), che gestiva un sito di *news* ricavando profitti dalle inserzioni pubblicitarie, nel quale consentiva agli utenti di caricare liberamente anche propri commenti, con un sistema peraltro di *notice and take down* e meccanismi di rimozione automatica di quelli contenenti determinati termini considerati osceni, perché tali strumenti di protezione da violazioni della reputazione altrui (nella specie: di un servizio di traghetti pubblici SLK), nonostante la successiva rimozione dei contenuti diffamatori, sono stati considerati "insufficienti" a contrastare efficacemente gli illeciti *on line*. In specie, la Corte EDU ha riconosciuto il ruolo "attivo" del *provider* nel caso concreto, che aveva portato i giudici estoni ad escludere l'applicazione del regime di esonero da responsabilità di cui alla menzionata Dir. CE 2000/31, in quanto la sua attività non era meramente tecnica ed automatica, o "passiva", ma gli permetteva di esercitare un controllo sulle infor-

[75] POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?* in *Dir. Un. Eu.*, 2014, n. 3, 601 s., 621.

mazioni e sui commenti presenti sul proprio portale, di cui pur non era l'autore. Di conseguenza, dovevano considerarsi conformi ai parametri del secondo paragrafo dell'art. 10 CEDU le limitazioni della libertà d'espressione, non mancando la Corte di sottolineare che i doveri e le responsabilità inerenti alla gestione dei "nuovi" portali in Internet possono essere valutati in termini differenti da quelli concernenti le tradizionali forme di pubblicazione, in specie a stampa, fino a potersi esigere "misure di rimozione" senza ritardo, *non subordinate* alla previa notifica di una richiesta da parte della vittima o di terzi.

Nella più recente sentenza del 2017, la Corte sembrerebbe essere giunta a conclusioni opposte rispetto a quelle appena esaminate: tuttavia le circostanze di fatto da cui ha preso le mosse erano diverse. Il sig. Rolf Anderson lamentava infatti che i tribunali svedesi non avessero condannato il gestore di un *blog*, che aveva rimosso solo dopo la richiesta un *post* diffamatorio, in cui lo si accusava di avere legami con un partito nazista. *Post* che pur cancellato era ancora reperibile nel *web*, attraverso motori di ricerca.

La Corte EDU ha richiamato, in questo caso, l'ampio margine di discrezionalità lasciato agli Stati nell'adempiere agli "obblighi positivi" di tutela su di essi incombenti, bilanciando i diritti egualmente protetti dalla Convenzione, quali quelli di cui agli artt. 8 e 10 CEDU. Di conseguenza, non era da censurare la legge svedese sulla responsabilità dei gestori di bacheche elettroniche, che non prevede la semplice diffamazione fra i reati per cui è tassativamente previsto l'obbligo di rimozione, essendo da distinguere diversi livelli di responsabilità, in relazione al diverso contenuto degli scritti immessi dagli utenti. Se nel caso di chiaro contenuto illecito, quale l'incitamento all'odio ed alla violenza, l'intermediario che ne abbia avuto conoscenza è immediatamente tenuto ad eliminarlo, nel caso invece di violazione della *privacy* o di diffamazione non è responsabile se si attiva solo dopo una formale richiesta.

### *6.2. Giurisprudenza CGUE*

Nella giurisprudenza della Corte di Giustizia dell'Unione spicca, innanzitutto, la storica sentenza sul caso Google del 2014, che ha affermato il c.d. diritto all'oblio nel *Cyberspace*[76], la cui portata trova oggi ampio riscontro nell'esplicito riconoscimento del diritto della persona alla "cancellazione dei dati" che ad essa si riferiscano da parte non solo del titolare del sito che li abbia inizialmente pubblicati, ma anche dei responsabili dei motori di ricerca che ne consentano a chiunque in tempi successivi il reperimento in Internet, quando tali dati non siano

[76] CGUE (Grande Camera), 13.5.2014, C-131/12, Google Spain e Google Inc. c. AEDP e M. Costeja González.

più necessari per le finalità per le quali sono stati raccolti o sussistano le altre condizioni, previste ora dall'art. 17 del nuovo Regolamento generale dell'Unione Europea sulla protezione dei dati 2016/679 del 27.4.2016 (c.d. GDPR), che sostituisce la Dir. CE 95/46.

La menzionata sentenza è particolarmente importante per il tema della responsabilità anche penale degli ISP, perché afferma in capo ad essi un "obbligo di protezione" dei diritti della personalità, fra cui rientra quello alla "protezione dei dati personali", espressamente fondato sull'innovativo art. 8 della Carta dei diritti fondamentali dell'Unione europea (di seguito: Carta di Nizza), che si aggiunge al più generale diritto alla protezione della vita privata e familiare di cui al suo art. 7 (invece pressoché identico all'art. 8 CEDU). Obbligo di protezione che è correlato all'ingerenza che gli stessi ISP abbiano nel trattamento dei dati, seppur ricevuti o caricati da terzi, in quanto siano tecnicamente nelle condizioni di determinarne le finalità e le modalità: con la conseguenza che possono esserne considerati "responsabili" ai fini della disciplina della *privacy*, con ogni connessa conseguenza di natura eventualmente anche penale.

Anche nel controverso ambito della protezione dei diritti di proprietà intellettuale (che trovano invece fondamento nell'art. 17 della Carta di Nizza) è evidente la marcata evoluzione della giurisprudenza della Corte nel bilanciamento fra il predetto diritto e quelli di libertà d'iniziativa economica (*ex* art. 16 Carta di Nizza) degli ISP, nonché di libertà d'informazione (*ex* art. 11 Carta di Nizza) che essi possono far valere.

Nelle sentenze c.d. SABAM del 2011 (caso Scarlet C-70/10) e del 2012 (caso Netlog C-360/10) la CGUE aveva ritenuto che non potessero ingiungersi agli ISP misure che li obbligassero a realizzare una vigilanza attiva su tutti i dati di ciascuno dei loro clienti, per prevenire qualsiasi futura violazione dei diritti di proprietà intellettuale, in quanto avrebbero dovuto predisporre un sistema complesso, costoso, permanente, a loro carico, non rispettoso dell'esigenza di proporzionalità rispetto alle violazioni del diritto d'autore, la cui tutela non è assoluta.

Viceversa, l'adozione di misure tecniche, non eccessivamente onerose in termini economici e di tempo, in grado di contrastare i comportamenti illeciti *on line*, è stata incentivata nelle successive sentenze del 2014 e del 2016, riguardanti rispettivamente i casi Telekabel v. Costantin Film (C-314/12) e Mc Faden v. Sony (C-484/14).

Nella prima decisione, l'ingiunzione richiesta dalla ditta di produzione cinematografica Costantin al fornitore di accesso austriaco Telekabel, di vietare ai suoi clienti l'accesso ad un sito gestito da terzi, che consentiva di scaricare opere in violazione dei diritti d'autore, è stata ritenuta compatibile con il diritto alla libertà d'impresa (di cui all'art. 16 Carta di Nizza), perché pur limitando il libero esercizio delle risorse a disposizione dell'ISP, non pregiudicava la sostanza stessa

del diritto in questione, lasciandogli l'onere di determinare le misure concrete da adottare per raggiungere il risultato in termini adeguati alle proprie capacità e consentendogli così di sottrarsi alla propria responsabilità con la dimostrazione di aver adottato tutte le misure ragionevoli. D'altronde, non era da considerare pregiudicato neppure il diritto alla libertà d'informazione degli utenti (di cui all'art. 11 Carta di Nizza), che comprende anche quello di riceverle, poiché le misure in questione devono essere rigorosamente mirate a porre fine alla violazione del diritto d'autore, senza pregiudicare la predetta libertà degli utenti, cui è data la possibilità di ricorrere al giudice laddove ciò avvenga in quanto le misure non risultino congrue.

Nella seconda decisione la Corte ha ritenuto che sarebbe stata contraria all'art. 15 della Dir. CE 31/2000 una misura che avesse imposto l'esame di tutte le connessioni *wi-fi* – offerte gratuitamente ai propri clienti, per ragioni promozionali della propria attività commerciale, dal sig. Mc Fadden, qualificato per questo come un "fornitore d'accesso" – al fine di prevenire violazioni dei diritti d'autore sulle opere musicali da essi molto spesso così scaricate; ma che era da ritenere "lecita" una misura che prevedesse la protezione della connessione tramite una *password*, in grado di evitare la fruizione anonima del servizio, dal momento che questa non intaccava né la libertà d'impresa, né quella di informazione, e poteva essere sufficiente a dissuadere gli utenti dal violare i diritti d'autore.

In definitiva, il *safe harbour* garantito in termini molto ampi e generali dalla Dir. CE 2000/31 a tutti gli ISP, differenziati soltanto in relazione a tre schematiche e basilari categorie di attività (fornitura d'accesso, *caching* ed *hosting*), è apparso ed appare oggi del tutto inadeguato di fronte agli impressionanti sviluppi tecnologici (cfr. *supra* § 1.1) ed ai mutamenti sociali intervenuti in questi 18 anni nel *Cyberspace* (cfr. *supra* § 1.2 nonché §§ 2 e 4).

Se all'inizio del millennio si giustificava l'esigenza di promuovere lo sviluppo di Internet e dei correlati servizi, tecnicamente limitati, oggi l'emergere della nuova categoria degli *hosting* c.d. attivi, che riflette la sempre più penetrante attività di selezione, trattamento, gestione seppur ampiamente automatizzata dei dati degli utenti e di terzi, nonché dei nuovi portali e delle potenti piattaforme i cui contenuti possono essere direttamente generati e caricati dagli utenti, ma il cui controllo e beneficio economico-commerciale resta saldamente in capo ai rispettivi ISP, il ruolo sempre più performante dei grandi motori di ricerca, l'espansione pervasiva delle reti sociali, i nuovi allarmanti fenomeni che coinvolgono vittime vulnerabili ed in specie i minori, quali il *cyberbullismo*, il *sexting*, il c.d. *Revenge Porn*, ecc., non può non portare a riconsiderare radicalmente quelle scelte di immunizzazione, al fine di garantire un più adeguato bilanciamento degli interessi e dei diritti da salvaguardare nel *Cyberspace*, in particolare di quelli fondamentali, che risultano particolarmente esposti alle nuove tipologie e modalità di offesa, rese possibili dallo stesso sviluppo tecnologico.

In questo percorso, la Corte di Strasburgo ha in definitiva svolto (e potrà svolgere ancora) un ruolo da battistrada, perché meno vincolata dalle più rigide previsioni restrittive del diritto comunitario. Ma anche la Corte di giustizia UE ha dimostrato progressiva attenzione alle esigenze di tutela dei diritti fondamentali nel *Cyberspace*, che comportano il coinvolgimento della responsabilità degli ISP.

In attesa di auspicabili interventi riformatori del diritto dell'Unione[77], residuano in ogni caso significativi spazi di manovra al legislatore interno ed alla giurisprudenza, in particolare sulla base dell'art. 12, par. 2, dell'art. 13, par. 2 e dell'art. 14, par. 3 Dir. CE 31/2000, secondo cui è sempre "impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione" [78], considerando che le violazioni anche penalmente rilevanti– come si preciserà nel paragrafo conclusivo – assumono nel *Cyberspace* un peculiare carattere espansivo nel tempo e nello spazio, di cui non si può non tenere conto.

Per cogliere le esigenze di (maggior) sicurezza nel *Cyberspace* e le tendenze future al riguardo, si può menzionare infine la Dir. 2016/1148 del Parlamento Europeo e del Consiglio del 6.7.2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, la quale impone tassativi obblighi agli operatori di servizi essenziali e ai fornitori di servizi digitali, specificamente individuati, nell'ambito di una "strategia nazionale in materia di sicurezza della rete e dei sistemi informativi" che preveda fra l'altro "gruppi di intervento per la sicurezza informatica in caso di incidente («CSIRT»)" in un contesto di "essenziale collaborazione" tra il settore pubblico e il settore privato.

Tale chiara e condivisibile esigenza di profonda differenziazione fra i vari "fornitori di servizi della società dell'informazione", basata sulla loro diversa

[77] Significativa è la recentissima approvazione, nel settembre 2018, da parte del Parlamento europeo, dopo una precedente bocciatura in luglio, della proposta di Direttiva per la protezione del diritto d'autore nel "mercato unico digitale" (COM/2016/0593 final – 2016/0280 (COD)), in cui viene enucleata la nuova categoria dei "prestatori di servizi di condivisione di contenuti online" – in luogo di quella più generica di "prestatori che svolgono un ruolo attivo" contenuta nell'originaria proposta della Commissione – come si evince chiaramente dagli emendamenti ai considerando (38) e (39) e soprattutto all'art. 13, che stabilisce che gli stessi con la loro attività "svolgono un atto di comunicazione al pubblico" e quindi (essendo "responsabili del loro contenuto": considerando 38), sono tenuti a concludere "accordi equi e adeguati di licenza con i titolari dei diritti" od in ogni caso a "cooperare [con essi] in buona fede per garantire che non siano disponibili sui loro servizi opere o altro materiale protetti non autorizzati".

[78] Al riguardo si può segnalare una recente sentenza del Tribunale civile di Torino, 7.4.2017, n. 1928, che sulla base di un'opportuna ed anzi indispensabile consulenza tecnica-forense, ha ritenuto che i gestori della piattaforma *YouTube* avessero la possibilità agevole di provvedere ad impedire, seppur con minime possibilità di insuccesso, che un video gioco già censurato fosse nuovamente caricato da terzi, mediante il calcolo di un valore *hash* od il ricorso ad un *software Content Id*, introducendo dunque un adeguato sistema di controllo successivo.

importanza e capacità di intervento (cui è stata data recente attuazione in Italia con il D.lgs. 18.5.2018, n. 65), supera la ristretta prospettiva della Dir. 2000/31 CE, fondata sulla semplice distinzione fra servizi di mero accesso, di *caching* o di *hosting*, e dimostra che non è più giustificata un'estesa garanzia di *safe harbour*, salvo marginali distinzioni nei requisiti applicativi ed eccezioni sostanzialmente collegate alle specifiche richieste dell'Autorità.

Oggi lo sviluppo tecnologico – per la gigantesca potenza qualitativa ed estensione quantitativa dei trattamenti di dati – consente quantomeno ai più grossi *provider*, veri "signori" o giganti del *web* quali Google o Facebook, un "controllo" e una possibilità di ingerenza su larga scala non immaginabili agli inizi del millennio, che coinvolge milioni di utenti di tutto il mondo. Per cui il livello elevato di "sicurezza informatica" da garantire nel *Cyberspace* non può riguardare solo le infrastrutture della "Rete" fisicamente intesa, ma deve estendersi ad un analogo livello di *effettiva* garanzia degli (altri) diritti fondamentali delle persone e dei gruppi, con corrispondenti strategie di tutela, che includano in particolare nuove ed articolate discipline giuridiche relative agli obblighi (ed alle responsabilità) incombenti sugli ISP, parametrate all'importanza, al valore economico ed all'estensione dei servizi e delle attività che svolgono, da rispettare in termini generali, non solo a seguito di singole specifiche richieste delle Autorità, di fronte a già avvenute violazioni concrete, come oggi sostanzialmente avviene.

Per presidiare *effettivamente* i diritti e gli interessi giuridici di più elevata importanza è ovviamente indispensabile anche il ricorso a sanzioni (non solo penali) proporzionate, efficaci e dissuasive, che sia gli Stati, sia gli organismi e le giurisdizioni sovranazionali (in Europa, ad es., non solo la Commissione europea sul piano amministrativo, ma in prospettiva futura anche la neo-istituita Procura europea, per gli aspetti penali)[79] possano irrogare o quantomeno richiedere.

## 7. Osservazioni conclusive: verso un mutamento di nozioni basilari quale quella di consumazione del reato nel *Cyberspace*?

La questione aperta dei presupposti e limiti della responsabilità anche penale degli ISP, per reati ed attività illecite che si commettono nel *Cyberspace*, rimanda,

[79] La Procura europea (EPPO), istituita con il Regolamento (UE) 2017/1939 del Consiglio del 12.10.2017 relativo all'attuazione di una cooperazione rafforzata al riguardo, ha competenza (*ex* art. 22 ed in conformità all'art. 86 TFUE) soltanto "per i reati che ledono gli interessi finanziari dell'Unione di cui alla direttiva (UE) 2017/1371" e per quelli "indissolubilmente connessi con essi": ma tale competenza potrebbe essere estesa, con atto all'unanimità del Consiglio Europeo, ad altre sfere di criminalità grave e transnazionale, a partire da quelle di cui all'art. 83, par. 1 TFUE, che ad es. prevede già la "criminalità informatica" (oltre al terrorismo, allo sfruttamento di donne e minori, ecc.: cfr. *supra* nota 49).

in una prospettiva teorica più ampia, a questioni generali di teoria del reato, che attengono alla stessa definizione di nozioni basilari come quelle di "azione" e di "evento", nonché dell'eventuale nesso causale, penalmente rilevanti nel *Cyberspace*, da rileggere alla luce delle trasformazioni che hanno determinato l'*automazione*, la *dematerializzazione*, l'*interazione* e l'*interdipendenza* delle attività e dei servizi che vi si svolgono.

In particolare, il concetto basilare di "fatto" tipico, costitutivo di reato, la cui commissione fonda l'applicazione della sanzione penale ed, a monte, l'attivazione delle indagini e degli eventuali strumenti cautelari, non può prescindere da quelle "porzioni" sempre più rilevanti che si realizzano *tramite* i sistemi informatici ed in rete, in esecuzione di programmi basati su algoritmi sofisticati e complessi, concepiti ed attivati da soggetti che peraltro ne siano titolari o fruitori: fenomeni rispetto a cui occorre domandarsi in che misura siano anche giuridicamente imputabili alla "consapevole volontà" dell'uomo che li attiva o se ne serve. L'*autonomia* (seppur relativa) delle determinazioni e "scelte" operative dei sistemi informatici non sembra poterne escludere in linea di principio l'attribuzione (anche) alla sottostante "volontà" dei soggetti umani, da cui i sistemi stessi ed il loro *output* in ultima analisi necessariamente dipendono. Ma sono certamente da precisare i presupposti ed i limiti, in relazione ai quali può dirsi esercitato e mantenuto, ai fini della responsabilità penale, il "dominio" dell'uomo su tutti i risultati ed effetti che conseguono e permangono, spesso a grande distanza di tempo e di luogo.

Sulla base della definizione convenzionale di "sistema informatico" (cfr. *supra* § 2), e come si è visto anche nella soprastante analisi dei reati informatici in senso stretto ed, in particolare, nei casi paradigmatici dei delitti di frode informatica ed accesso abusivo (cfr. *supra* § 5.1.1), l'attività realizzata dal o se si vuole "tramite" il sistema stesso ha – già – una propria *specifica* rilevanza giuridica, tanto da essere espressamente sussunta nelle predette (come in altre) fattispecie penali sopra menzionate, con tutte le problematiche insorte per determinare anche il luogo ed il momento della consumazione.

Le evidenziate caratteristiche tecniche dell'*automazione*, che investe – oltre all'elaborazione – anche la circolazione, messa a disposizione, permanenza dei dati e dei contenuti nel *Cyberspace*, impongono dunque *in primis* di riconsiderare le condizioni della "consumazione" del reato, *ivi* in tutto o in parte commesso.

Non solo, infatti, si espandono nel tempo e nello spazio i suoi "effetti", come paradigmaticamente è emerso nel caso Google concernente il diritto all'oblio, affermato dalla citata sentenza della CGUE del 2014 (*supra* § 6.2), ma è lo stesso "fatto" tipico che, nella parte in cui si realizza *tramite* i sistemi informatici, si può ritenere che si protragga ed eventualmente "riproduca", in forza delle funzioni automatizzate di memorizzazione, trasmissione, messa a disposizione, condivi-

sione, circolazione, ricerca, ecc., peraltro non del tutto "dominabili" dai gestori e fruitori dei sistemi stessi.

In altri termini, non è corretto, nel contesto tecnologico descritto, ridurre la speciale "permanenza" del reato cibernetico ed espansione dei suoi effetti ad un mero *post factum* non punibile, penalmente irrilevante, perché il prolungamento *automatizzato* dell'azione o dell'evento *tipici* non è affatto separabile dagli altri elementi oggettivi e soggettivi costitutivi del "fatto" di reato, di cui sono parte essenziale, essendo questo che viene piuttosto ad assumere connotati specifici in ragione delle TIC, tramite cui l'autore lo ha (consapevolmente) posto in essere.

Si può piuttosto muovere dall'applicazione ed eventuale adattamento alla realtà cibernetica della tradizionale distinzione dogmatica fra momento di "perfezione formale" del reato, che si ha quando ne sono realizzati tutti gli elementi costitutivi essenziali, seppur nel loro contenuto minimo, e momento di "esaurimento" o "consumazione sostanziale", che si ha solo quando esso ha per l'appunto "esaurito" *definitivamente* il proprio specifico contenuto di offesa, avendo raggiunto il massimo grado di lesione del ben giuridico protetto[80].

Ebbene, il reato cibernetico non può dirsi "esaurito" nel periodo intermedio anche assai lungo che può intercorrere fra i due momenti, in cui "permane" e si approfondisce l'offesa. Tuttavia il fenomeno non pare riconducibile al paradigma del reato permanente in senso proprio (come è ad es. il sequestro di persona), che presuppone, alla stregua della fattispecie legale, la costante dipendenza della protrazione dell'offesa al bene giuridico (nell'esempio: la libertà personale della vittima) dalla diretta e contemporanea *condotta volontaria* del reo, il quale potrebbe in ogni momento farla cessare (tanto che si parla addirittura, da taluni, di un reato misto di commissione per la realizzazione iniziale e di omissione per il successivo mantenimento dello stato antigiuridico)[81]. Essendo l'automazione specifica delle TIC che determina la diffusione nel *Cyberspace* e la protrazione nel tempo dei suoi effetti ancora potenzialmente attivi, questi possono sfuggire al diretto controllo dell'azione del reo, che pur lo ha posto in essere loro tramite.

[80] Su tale distinzione, pacifica nella teoria generale del reato, quantomeno da CARRARA, *Momento consumativo del furto* (1870), in *Lineamenti di pratica legislativa penale*, Torino, 1874, 229 s., e recepita da tutta la manualistica, non solo italiana, ma anche straniera (cfr. per tutti JESCHECK, WEIGEND, *Lehrbuch des Strafrechts. Allgemeiner Teil*, 5. Aufl., Dunker & Humblot, Berlino, 1996, 517 s.), cfr. volendo anche PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993, 568 s.

[81] Sulle conseguenze della durata nel tempo caratteristiche del reato permanente ed altri reati di durata, cfr. per tutti ROMANO M., *Commentario sistematico del codice penale*, I, 3ª ed., Milano, 2004, Pre-Art. 39, § 118 s., 344 s.; sul *postfactum* basti il rinvio alla monografia di PROSDOCIMI, *Profili penali del postfatto*, Milano, 1982.

Neppure si attaglia perfettamente alle caratteristiche del reato cibernetico la nozione di reato "a consumazione prolungata", più recentemente sviluppata in giurisprudenza[82], in relazione a fattispecie (quali la corruzione o l'usura) che possono presentare momenti alternativi di consumazione, in quanto gli atti che le realizzano possono essere più d'uno, estendendosi ad abbracciare anche il od i pagamenti che seguono la promessa e l'accordo raggiunto fra le parti, con cui già formalmente si perfezionano, pur non esaurendone il contenuto offensivo, che si aggrava con i successivi versamenti. Infatti, anche tali atti successivi sono direttamente dipendenti da più azioni volontarie di accettazione da parte dell'autore dei pagamenti ulteriormente posti in essere dal soggetto passivo.

Si prospetta, quindi, l'esigenza di delineare una categoria dogmatica nuova, che abbracci la peculiare, sempre più diffusa e rilevante realtà che si manifesta nel *Cyberspace*, nella molteplicità di reati cibernetici configurabili, a partire da quelli di comunicazione e diffusione di un pensiero, nei quali non rileva un evento consumativo autonomamente verificabile nel mondo materiale, esterno cioè all'"infosfera" (quale può essere ad es. l'offesa al patrimonio altrui consumativa della frode informatica o dell'estorsione *on line*, che possono dirsi commesse nel tempo e luogo in cui si produce il danno altrui o si consegue l'ingiusto profitto, con tutte le problematiche che i moderni mezzi di pagamento on line però sotto altri aspetti sollevano). La diffamazione *on line*, la diffusione di pedopornografia, l'istigazione e propaganda di atti di odio e discriminazione razziale, la distribuzione o messa a disposizione di opere digitali in violazione dei diritti d'autore, le molteplici violazioni della riservatezza e della *privacy*, compresi gli accessi abusivi, e molti altri reati cibernetici si consumano interamente ed esclusivamente nel *Cyberspace*.

Il "fatto di reato" dunque presenta in questi casi una "consumazione protratta" che si estende oltre il momento della perfezione formale, fino a che non giunga al momento (difficile, ma non impossibile da verificare) dell'esaurimento sostanziale. In questo anche molto prolungato periodo di tempo, e nella corrispondente estensione nello spazio, non pare dogmaticamente corretto ravvisare gli elementi della *condotta* tipica, che deve sempre ricondursi al domino *attuale* della "volontà consapevole" dell'uomo, strettamente intesa.

Tuttavia è indubbio che l'offesa tipica, che ne è l'effetto, si produce in *conseguenza diretta* di siffatta condotta, volutamente e consapevolmente realizzata nel *Cyberspace*.

Sembra quindi delinearsi piuttosto una peculiare accezione di "evento", che pur se strutturalmente diversa dalla tradizionale nozione naturalistica, ne man-

[82] Per un quadro v. BRUNELLI, *Il reato portato a conseguenze ulteriori. Problemi di qualificazione giuridica*, Torino, 2000.

tiene molte caratteristiche equivalenti, sul piano degli effetti sulla vittima e dell'offesa agli interessi protetti: per sembra poter essere imputabile non solo "causalmente", ma anche "soggettivamente" all'autore, a titolo di dolo (quantomeno eventuale), oppure di colpa, se ne ricorrano gli estremi, rispettando naturalmente i limiti propri della responsabilità penale.

La scelta del mezzo tecnico utilizzato (TIC), che implica l'automazione del trattamento e della circolazione in rete, con tutte le caratteristiche e conseguenze sopra richiamate, comporta che siano conosciute o quantomeno conoscibili dall'autore che *vuole* "agire" loro tramite.

Ne consegue che il momento consumativo, alla cui stregua determinare la legge penale applicabile (*ex* art. 2 c.p.), dovrà includere tale fase ulteriore di "prolungamento" ed estensione dell'*evento* "cibernetico" (o *output* nel *Cyberspace*), fermo il divieto di retroattività della legge incriminatrice o sfavorevole rispetto al momento invece della condotta, in relazione alla quale soltanto può operare il contenuto precettivo della norma; mentre la decorrenza del termine di prescrizione dovrebbe essere posticipato tendenzialmente fino al momento dell'esaurimento o consumazione sostanziale, dato il protrarsi dell'interesse punitivo fino a detto momento, come del resto previsto per i reati permanenti ed a consumazione prolungata (art. 158, comma 1, c.p., nonché art. 644-*ter* c.p. per quanto concerne l'usura).

Il *luogo* di commissione del reato, che deve coincidere con il luogo della consumazione, sembra invece da riferire a quello della perfezione formale e, dunque, della *prima* manifestazione dell'evento, come del resto conferma la regola prevista per i reati di omicidio e permanenti (art. 8, commi 1, 2 e 3 c.p.p.), salvo che l'evento "cibernetico" assuma immediati caratteri di "ubiquità" e perciò, non essendo possibile determinarlo, sia necessariamente quello "dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione" (art. 9, comma 1, c.p.p.), con risultati in concreto non diversi da quelli collegati al menzionato criterio dell'"inizio della consumazione" previsto per il reato permanente (art. 8, comma 3, c.p.p.).

Ne consegue in ogni caso che dovrà riconoscersi, in conformità ai principi generali, la configurabilità della partecipazione concorsuale penalmente rilevante ex art. 110 c.p., in forma sia attiva sia omissiva, da parte di terzi – compresi gli ISP, in relazione al ruolo attivo o di condivisione di contenuti in rete concretamente svolto – fino all'avvenuto "esaurimento", sulla base dei relativi presupposti oggettivi e soggettivi[83].

[83] In tal senso si veda la sentenza della Corte di Cassazione 27.12.2016, n. 54946, nel c.d. caso Tavecchio, che ha confermato la condanna penale per concorso in diffamazione di un *blogger*, che aveva "mantenuto" il testo con le espressioni offensive sul proprio sito, nonostante fosse stato reso edotto del loro contenuto.

Evidenti sono le ricadute pratiche di tali conclusioni, nell'attribuzione di responsabilità penale agli operatori ed agli utenti della Rete, ad es. in un *social network* in cui si mantengano, inoltrino, approvino, facciano ulteriormente circolare *post*, messaggi, immagini penalmente lesive di diritti altrui, pur inizialmente trasmessi e prodotti da altri, che abbiano già "formalmente" consumato, ma non ancora "sostanzialmente" esaurito il reato commesso, per il protrarsi e diffondersi dell'evento od *output* nel *Cyberspace*.

I limiti di garanzia da riaffermare sono certamente rappresentati dal principio di stretta legalità, con l'inerente divieto di estensione analogica delle fattispecie penali, e dal principio di colpevolezza, che impone di circoscrivere comunque la responsabilità penale ai "fatti" *personalmente* imputabili: e dunque, rispetto all'evento od *output* "cibernetico", nei limiti (di spazio e di tempo), in cui esso sia riconducibile – al momento dell'azione – alla previsione e volontà dell'agente, nel caso di reato doloso, ovvero alla sua prevedibilità ed evitabilità, nel caso di reato colposo.

Un ampio campo ancora da esplorare, che investe questa ed altre nozioni basilari di teoria del reato – oltre a quelle di azione ed evento, anche quelle di causalità, di partecipazione criminosa, di tentativo, ecc.[84] – è dunque aperto alla riflessione ed elaborazione dogmatica del penalista, che per non venire meno al proprio compito di giurista deve saper adeguare i propri strumenti conoscitivi e le proprie categorie concettuali alla nuova realtà, ma senza mai abbandonare i principi fondamentali e le garanzie invalicabili del diritto penale, propri di un ordinamento democratico.

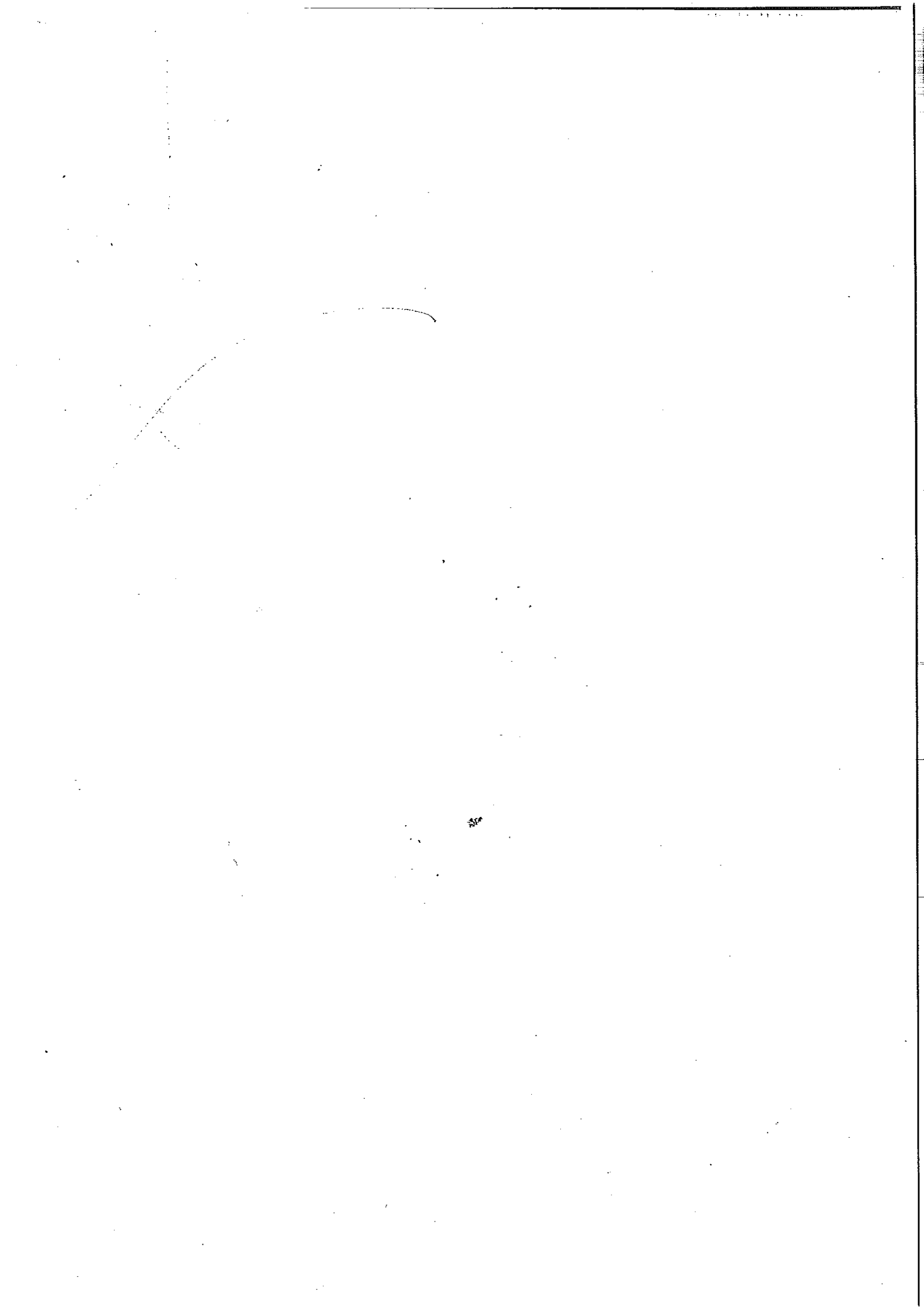
Bibliografia

Bertolisi, *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere*, in *www.penalecontemporaneo.it* (3.10.2017); Borruso-Buonomo-Corasaniti-D'Aietti, *Profili penali dell'informatica*, Milano, 1994; Mucciarelli-Picotti-Rinaldi-Ugoccioni, raccolti in *Legislazione pen.*, 1996, n. 1-2, 57 s.; Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, 1079 s., ora in *Scritti diritto penale*, II, Tomo I, Milano, 1997, 2289 s.; Brunelli, *Il reato portato a conseguenze ulteriori. Problemi di qualificazione giuridica*, Torino, 2000; Carrara, *Momento consumativo del furto* (1870), in *Lineamenti di pratica legislativa penale*, Torino, 1874, 229 s.; Cajani, *Profili penali del* phishing, in *Cass. pen.*, 2007, n. 6, 2294 s.;
Cajani, *Quella Casa nella Prateria: gli Internet Service Providers americani alla prova del caso Google Video*, in Picotti-Ruggieri (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 223 s.; Cajani-Costabile-

[84] Cfr. volendo già Picotti, *Internet e responsabilità penali*, in Pascuzzi G. (a cura di), *Diritto ed informatica*, Milano, 2002, 117 s.

MAZZARACO (a cura di), *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008; FLOR, Phishing, identity theft e identity abuse: *le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2007, 899 s.; FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online-Durchsuchung, in *Riv. trim. dir. pen. economia*, 2009, 695 s.; FLOR, *Tutela penale ed autotutela tecnologica de diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010; FLOR, *Verso una rivalutazione dell'art. 615* ter *c.p.?* in *www.penalecontemporaneo.it* (2.5.2012); FLOR, *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite*, in *Dir. pen. e processo*, 2015, 1296 s.; FLOR, *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere"?*, in *Dir. pen. e processo*, 2018, 506 s.; GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, 1984; INGRASSIA, *La Corte d'appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali*, in *www.penalecontemporaneo.it* (4.3.2013); INGRASSIA, *La sentenza della Cassazione sul caso Google*, in *www.penalecontemporaneo.it*, (6.2.2014); JESCHECK-WEIGEND, *Lehrbuch des Strafrechts. Allgemeiner Teil*, 5. Aufl., Dunker & Humblot, Berlino, 1996; KERR, *Computer Crime Law*, Thomson West, St. Paul MN, 2006; LESSIG, *Code and Other Laws of Cyberspace* (1999), 2ª ed., Basic Books, New York, 2006; LOTIERZO, *Il caso* Google-Vivi Down *quale emblema del difficile rapporto degli* Internet Providers *con il codice della* privacy, in *Cass. pen.*, 2010, n. 11, 3994 s.; LUPARIA (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 8 marzo 2008, n. 48)*, Milano, 2009; LUPARIA (a cura di), *Internet provider e giustizia penale*, Milano, 2012; MANNA, *Considerazioni sulla responsabilità penale dell'*internet provider *in tema di pedofilia*, in *Dir. informaz. e informatica*, 2001, 145 s.; MANNA, *I soggetti in posizione di garanzia*, in *Dir. informaz. e informatica*, 2010, 779 s.; PASCUZZI G. (a cura di), *Diritto ed informatica*, Milano, 2002; PATRONO, *Privacy e vita privata*, in *Enc. Dir.*, XXXV, Milano, 1985, 557 s.; PECORELLA, *Il diritto penale dell'informatica* (2000), 2^ ed., Milano, 2006; PETRINI, *La responsabilità penale per i reati via Internet*, Napoli, 2004; PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999; PICOTTI, *Problemi penalistici in tema di falsificazione di dati informatici*, in *Dir. informaz. e informatica*, 1985, 939 s.; PICOTTI, *Studi di diritto penale dell'informatica*, Verona, 1992; PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993; PICOTTI, *Tutela dei dati personali e tutela della persona*, in CAMMELLI-GUERRA (a cura di), *Informazione e funzione amministrativa*, Rimini, 1997, 297 s.; PICOTTI, *Fondamento e limiti della responsabilità penale dei Service-providers in* Internet, in *Dir. pen. e processo*, 1999, n. 3, 379 s.; PICOTTI, *La responsabilità penale dei* Service-providers *in Italia*, in *Dir. pen. e processo*, 1999, n. 4, 501 s.; PICOTTI, *Profili penali delle comunicazioni illecite via* Internet, in *Dir. informaz. e informatica*, 1999, n. 2, 283 s.; PICOTTI, voce *Reati informatici*, in *Enc. Giur.*, vol. agg. VIII, Roma, 2000; PICOTTI, *Internet e responsabilità penali*, in PASCUZZI G. (a cura di), *Diritto ed informatica*, Milano, 2002, 117 s.; PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Ib. (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 s.; PICOTTI, *Il campo di applicazione del mandato d'arresto europeo: i reati "in lista" e "fuori lista" e la disciplina della legge italiana di attuazione*, in BARGIS-SELVAGGI (a cura di), *Mandato d'arresto europeo. Dall'estradizione alle procedure di consegna*, Torino, 2005, 127 s.; PICOTTI, *Il mandato d'arresto europeo fra principio di legalità e doppia incriminazione*, in BARGIS-SELVAGGI (a cura di), *Mandato*

*d'arresto europeo. Dall'estradizione alle procedure di consegna*, Torino, 2005, 33 s.; PICOTTI, *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in BERTOLINO-FORTI (a cura di), *Scritti per Federico Stella*, Napoli, 2007, vol. II, 1267 s.; PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e processo*, 2008, n. 6, 700 s.; PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, 2008, 437 s.; PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. economia*, 2011, n. 4, 827 s.; PICOTTI, *Sicurezza, informatica e diritto penale*, in DONINI-PAVARINI (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, 217 s.; PICOTTI, *European Union's Directives in Substantive Criminal Law: What Discontinuity in Respect to the Pre-Lisbon Instruments?*, in AA.VV., *Toward Scientific Criminal Law Theories*, Beijing, 2015, 1248 s.; PICOTTI, *Quale diritto penale nella dimensione globale del* Cyberspace*?* in WENIN-FORNASARI (a cura di), *Diritto penale e modernità*, Trento, 2017, 309 s.; PICOTTI, *Terrorismo e sistema penale: realtà, prospettive, limiti* (Relazione di sintesi del VII corso di diritto e procedura penale "Giuliano Vassalli" per dottorandi e giovani penalisti – SII e Gruppo italiano AIDP, Noto, 11-13 novembre 2016), in *Riv. trim. dir. pen. contemporaneo*, 2017, 249 s.; PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004; PICOTTI-RUGGIERI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011; POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?* in *Dir. Un. Eu.*, 2014, n. 3, 601 s.; PROSDOCIMI, *Profili penali del postfatto*, Milano, 1982; RESTA, *Libertà della rete e protezione dei dati personali: ancora sul caso* Google-Vivi Down, in *Dir. informaz. e informatica*, 2013, 502 s.; RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; RODOTÀ, *Intervista su privacy e libertà*, Bari, 2005; RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014; ROMANO M., *Commentario sistematico del codice penale*, I, 3^ ed., Milano, 2004; RUGGIERI, *Profili processuali nelle indagini sui reati informatici*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova 2004, 153 s.; SALVADORI, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-*ter *c.p.*, in *Riv.trim.dir.pen.ec.*, 2012, 369 s.; SALVADORI, *L'adescamento di minori. Il contrasto al* child-grooming *tra incriminazione di atti preparatori ed esigenze di garanzia*, Torino, 2018; SARZANA DI SANT'IPPOLITO, *Informatica, Internet e diritto penale (*1994), 3 ed., Milano, 2008; SEMINARA, *La responsabilità penale degli operatori su Internet*, in *Dir. informaz. e informatica*, 1998, 745 s.; SIEBER (ed.), *Information Technology Crime. National Legislation and International Initiatives*, Carl Heymanns Verlag, Köln, Berlin, Bonn, München, 1994; SIEBER, *The International Handbook on Computer Crime. Computer-related Economic Crime and the Infringements of Privacy*, John Wiley & Sons, New York, Brisbane, Toronto, Singapore, 1986; SIEBER, *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag*, Verlag C.H. Beck, Munchen, 2012; TRONCONE, *Il caso* Google *(e non solo), il trattamento dei dati personali e i controversi requisiti di rilevanza penale del fatto*, in *Cass. pen.*, 2014, n. 6, 2060 s.; ZICCARDI, *Hacker. Il richiamo della libertà*, Milano, 2011; ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.



5 000002 315862

9 788859 818700