LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI GIURISPRUDENZA

CATTEDRA DI DIRITTO PENALE 2

IL *LOCUS COMMISSI DELICTI* NEI *CYBERCRIMES*

RELATORE

Chiar.mo Prof.
Antonino Gullo

CANDIDATA

Daniela Santonicola
Matr. 140413

CORRELATORE

Chiar.mo Prof.
Maurizio Bellacosa

ANNO ACCADEMICO 2019/2020

Ai miei genitori, custodi dei miei sogni.

A Rosa, Isabella, Ferdinando e Luca, punti fermi della mia vita.

Ad Armando, il mio faro nella tempesta.

INDICE

INTRODUZIONE 4

CAPITOLO I

IL *CYBERCRIME* E I *CYBERATTACKS*

1. La nascita e lo sviluppo del *cyberspace* 11
2. Il fenomeno dei *cyberattacks* e le tipologie di attacco 15
   2.1 Il *malware* 20
   2.2 Il *ransomware* 25
   2.3 Il *phishing* 30
   2.4 Il *pharming* 39
3. La criminalità informatica: rilievi introduttivi 41
4. Inquadramento normativo 48
   4.1 La legge n. 547/1993 56
   4.2 La Convenzione di Budapest, 23 Novembre 2001 72
   4.3 La legge di ratifica della Convenzione: legge n. 48/2008 78
5. La prevenzione come risposta alla criminalità informatica: la *cybersecurity* ... 85
6. Le caratteristiche principali del fenomeno: la desensibilizzazione e l'aterritorialità 90

CAPITOLO II

L'INDIVIDUAZIONE DEL *LOCUS COMMISSI DELICTI*

1. La consumazione del reato 94
2. Il *locus commissi delicti* 99
   2.1 Profili sostanziali 101
   2.2 Profili procedurali 108
3. I limiti del principio di territorialità nel *cyberspace* 111
   3.1 Il principio della personalità attiva e passiva: il modesto riconoscimento nel contesto nazionale 116

4. I problemi giuridici relativi ai reati informatici 119
5. Gli approdi giurisprudenziali 123
6. Le linee evolutive 128

CAPITOLO III

LE SINGOLE FATTISPECIE

1. L'accesso abusivo ad un sistema informatico o telematico: art. 615-*ter* 132
1.1. Criticità della sentenza della Corte di Cassazione S.U. n. 17325 del 2015 139
2. La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici art. 615-*quater* c.p 142
3. Interruzione illecita di comunicazioni informatiche o telematiche art. 617-*quater* c.p. 146
4. La diffamazione *online*: art. 595 comma 3 c.p. 149
5. La frode informatica: art. 640-*ter* c.p. 155
6. La truffa comune realizzata mediante l'utilizzo di strumenti tecnologici o la rete: art. 640 c.p. 160
7. Indebito utilizzo e falsificazione di carte di credito e di pagamento: art. 493-*ter* c.p. 163

CAPITOLO IV

LE PROSPETTIVE *DE IURE CONDENDO*

1. Considerazioni introduttive 168
2. Analisi *de iure condito* 170
3. Analisi delle prospettive *de iure condendo* 177
3.1 *(Segue).* L'esperienza in ambito europeo (cenni) 181
3.1.1 *(Segue).* L'esperienza spagnola 181
3.1.2 *(Segue).* L'esperienza francese 183
3.1.3 *(Segue).* L'esperienza tedesca 185
4. Considerazioni conclusive 187

CONCLUSIONI 190

INDICE BIBLIOGRAFICO 194

INDICE DELLA GIURISPRUDENZA 205

SITOGRAFIA 210

INTRODUZIONE

L'individuazione del luogo di commissione del reato si rivela un'operazione imprescindibile in vista della collocazione spaziale della fattispecie criminosa, che coinvolge sia profili di ordine sostanziale che processuale. Proprio a tal fine il presente elaborato si prefigge l'obiettivo di esaminare i profili che attengono alla tematica menzionata nel particolare contesto del *cyberspace*, in cui si prescinde dalla fisicità delle condotte intese nel senso consueto.

Il titolo della tesi ha l'intento di evidenziare, sin da subito, il punto dolente dell'annosa questione, vale a dire l'individuazione del *locus commissi delicti* nei *cybercrimes*, quei reati che si commettono o possono essere commessi mediante la rete.

La commissione *online* di determinate condotte illecite comporta il distanziamento delle stesse dagli accadimenti materiali esteriori comunemente intesi e rende ostico inquadrare le suddette azioni in un campo territorialmente limitato. Le azioni si esplicano nella nuova realtà cibernetica che consente la delocalizzazione delle risorse, la detemporalizzazione e deterritorializzazione delle operazioni poste in essere[1]: i soggetti pianificano condotte che si svolgeranno automaticamente, avendo la possibilità di collocarsi in più luoghi virtuali e venendo meno la necessità di un collegamento tra il soggetto agente e l'elaboratore informatico.

In proposito, è bene premettere che il dilagante sviluppo delle tecnologie informatiche ha prodotto permeanti mutamenti nelle dinamiche sociali e relazionali, tali da trasformare il modo di intendere dei concetti tradizionali. La classica concezione di nozioni basilari quali spazio, tempo, individuo, dovrà essere riconsiderata e adattata alla luce delle mutate esigenze dell'attuale contesto d'azione.

Si assiste ad un'incessante trasposizione del fulcro delle operazioni umane in una realtà che si allontana dalla classica percezione della fisicità e materialità, cui si è abituati a presenziare. La condotta umana si interfaccia con una serie di

[1] Cfr. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 143.

operazioni automatizzate, fino a sfumare in una serie di *bit* che si rinvengono nella dimensione dello spazio cibernetico: essa si tramuta in una forma di trasmissione, immissione e gestione di dati a mezzo di impulsi elettronici.

È nel solco di tale spazio che sorgono nuove esigenze di protezione, in virtù delle minacce che da esso scaturiscono: accanto alle innegabili innovazioni che il *cyberspace* ha introdotto nella quotidianità, si riscontra la presenza di nuove problematiche parametrate all'atteggiarsi di una nuova forma di criminalità, che ivi trova terreno fertile. Si tratta, pertanto, di condotte transnazionali, da cui sorge l'opportunità di armonizzare le legislazioni nazionali, in vista di sopire tale preoccupante fenomeno. Le condotte dei *cyber*criminali sono infatti connotate da ubiquità, per cui l'individuazione del *locus commissi delicti* si mostra come un'operazione non semplice, che involve la risoluzione di questioni con i principi tradizionali dell'ordinamento giuridico.

Si presenta il bisogno di indagare su tale argomento, dibattuto parimenti in dottrina e giurisprudenza, inglobato in un incessante divenire, alla luce dei continui mutamenti che coinvolgono la realtà digitale. L'intento del presente lavoro, pertanto, è quello di fare chiarezza sulla tematica del *locus commissi delicti*, tentando di fornire soluzioni sistematiche che si conformino alla realtà cibernetica.

L'elaborato si articola in quattro capitoli, nel tentativo di fornire un'analisi adeguata circa le criticità inerenti alla collocazione spazio-temporale delle azioni criminose concernenti la nuova frontiera della criminalità.

Il primo capitolo ha ad oggetto lo studio del *cybercrime* e dei *cyberattacks*. Verrà, innanzitutto, fornita una premessa di ordine generale sul contesto della realtà cibernetica, mediante un'analisi concernente la nascita e lo sviluppo del *cyberspace*, partendo dalle sue origini fino ad arrivare al ruolo che esso ricopre nella realtà odierna grazie alle sue peculiari caratteristiche, esaminando altresì le insidie che in esso si annidano. Si passerà poi ad analizzare il fenomeno delle minacce presenti nello spazio cibernetico, in virtù dell'espansione della Rete, che ha permesso ad un numero indefinito di utenti di accedervi, accentuando così la vulnerabilità dei sistemi presi di mira dai c.d. attaccanti della Rete. Ampio spazio sarà riservato alle diverse tipologie di attacco che si configurano nel *cyberspace*, data la diffusività che hanno acquisito nel corso dell'ultimo decennio, tenendo

conto delle molteplici modalità esistenti e delle gravi ripercussioni che si generano per la collettività. In particolare, saranno trattati i seguenti attacchi cibernetici: *malware*, *ransomware*, *phishing*, *pharming*, ognuno di essi si caratterizza quanto a struttura, tecniche di attacco, target e diramazione.

Nel prosieguo, si tratterà nel dettaglio degli esordi della criminalità informatica, ripercorrendone la storia evolutiva quale nuova frontiera della criminalità. Emergerà da questa analisi che il *cyber*spazio non può essere più considerato uno spazio franco dal diritto, per cui si sottolineerà l'esigenza di una delimitazione giuridica delle forme di aggressione che attentano ai diritti dei singoli, questione che, in un primo momento, è stata affrontata mediante interventi legislativi sporadici, volti a scongiurare possibili violazioni dei principi cardine dell'ordinamento giuridico, poi grazie a spinte sovranazionali, attraverso un provvedimento normativo *ad hoc*, che ha avuto il merito di aver introdotto nella legislazione italiana i reati informatici.

Si volgerà poi lo sguardo al mutato atteggiamento del legislatore, il quale da un'attitudine puramente repressiva progredisce verso un'ottica preventiva, mediante lo sviluppo di una strategia di *cybersecurity* in ambito nazionale, fondata sulla stretta cooperazione tra pubblico e privati. Da ultimo, l'attenzione sarà riservata alle caratteristiche principali del fenomeno, quali la desensibilizzazione e l'aterritorialità, che consentiranno di aprire la strada per la trattazione della seconda parte dell'elaborato.

Il secondo capitolo tratterà nello specifico il tema oggetto della tesi, vale a dire i problemi attinenti all'individuazione del *locus commissi delicti* nei *cybercrimes*. In particolare, l'attenzione si soffermerà dapprima sull'inquadramento dal punto di vista terminologico del concetto di consumazione del reato, al fine di comprendere cosa si intenda con questa locuzione. Si disquisirà, nel prosieguo, sui profili di ordine generale concernenti il luogo di consumazione del reato, sottolineandone l'importanza in virtù della determinazione della rilevanza penale della fattispecie in un luogo e dell'individuazione del giudice territorialmente competente.

Sarà ripercorso l'*iter* che ha portato il legislatore italiano ad accogliere il principio di territorialità nel codice Zanardelli e poi il successivo affermarsi del

principio di tendenziale universalità della legge penale italiana nel codice Rocco. Prima di addentrarsi nel dettaglio sugli aspetti concernenti i profili di ordine sostanziale e procedurale, si discuterà dell'adozione del criterio di ubiquità, per cui il reato si considera commesso tanto nel luogo in cui è avvenuta la condotta, anche solo in parte, tanto in quello in cui si è verificato l'evento.

Si passerà quindi allo studio dei profili sostanziali, partendo dall'esplicazione dei principi cardine dell'ordinamento penale concernenti l'applicazione della legge penale nello spazio per poi focalizzarsi su quelli adottati dal codice di procedura penale, che consentono di attuare un collegamento tra il reato e il luogo in cui esso è commesso, nell'ottica di stabilire il giudice territorialmente competente a giudicare una determinata condotta. Si affronterà, in seguito, la tematica concernente l'applicazione dei principi tradizionali nello spazio cibernetico, il quale travalica i confini spazio-temporali, limitando così la possibilità di individuare il punto esatto in cui viene commessa una condotta, e mal si concilia con la necessità degli ordinamenti giuridici di affermare la propria sovranità. In particolare, si volgerà lo sguardo ai principi di personalità attiva e passiva, interrogandosi sulla loro capacità di supplire al tradizionale principio di territorialità, senza trascurare le potenzialità relative ad un loro possibile accoglimento.

L'attenzione si focalizzerà, poi, sui problemi giuridici che si pongono in relazione all'individuazione del *locus commissi* delicti nei reati cibernetici, avuto riguardo del fatto che la questione concerne esclusivamente i reati a evento informatico, i reati di mera condotta commessi *online* ed i casi di tentativo di reati di evento realizzati *online*. Si affermerà la necessità di un diritto flessibile, al fine di plasmare i criteri di individuazione del *locus commissi delicti* al mutato contesto d'azione.

In ragione di tale obiettivo, ci si addentrerà in una disamina circa le pronunce rilevanti sul tema, partendo dal principio di diritto espresso dalla Corte di Cassazione a Sezioni Unite in riferimento al luogo di consumazione della fattispecie di accesso abusivo ad un sistema informatico o telematico, per poi approdare all'analisi di altre pronunce della Corte inerenti ad altre fattispecie, con l'intento di evidenziare l'importanza della tematica anche in ambito ermeneutico.

Il capitolo si concluderà con un breve esame circa le possibili interpretazioni evolutive, volte a conciliare due aspetti apparentemente incompatibili: le nuove tecniche di aggressione dei cybercriminali e i tradizionali principi dell'ordinamento penale.

All'esito di tale disamina, ci si concentrerà sulle singole fattispecie per cui maggiormente si pone la problematica di individuazione del *locus commissi delicti*, in quanto si è più volte esplicitata in dottrina la necessità di affrontare tale questione seguendo un metodo casistico. In particolare, nel terzo capitolo, si discorrerà sulla fattispecie che maggiormente ha scosso la giurisprudenza, fino a richiamare l'attenzione delle Sezioni Unite, vale a dire il delitto di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter*, del quale si esamineranno prima gli aspetti fondamentali e poi ci si concentrerà sulle criticità concernenti la suddetta sentenza.

Si tratterà, in seguito, della fattispecie di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, di cui all'art. 615-*quater*, a cui non risulta applicabile il principio di diritto precedentemente menzionato, per la peculiarità dell'azione posta in essere, la quale si sostanzia in un transito di informazioni che necessitano di giungere al destinatario. Si affronterà la tematica finanche in relazione al delitto di interruzione illecita di comunicazioni informatiche o telematiche, di cui all'art. 617-*quater* c.p. per cui si evincerà la possibilità di estendere le considerazioni a cui sono giunte le Sezioni Unite. Stesse questioni, ma con soluzioni differenti si porranno per la diffamazione a mezzo Internet, trattandosi di un reato di evento psicologico, che si consuma nel luogo in cui terzi percepiscono il messaggio diffamatorio e ciò evidenzierà come risulti sostanzialmente ostica l'individuazione del *locus commissi delicti.* Si volgerà lo sguardo alle truffe *online*, nel dettaglio alla frode informatica e alla truffa comune realizzata attraverso l'utilizzo di strumenti tecnologici o comunque mediante la rete, che individuano come momento e luogo della consumazione quello in cui si è prodotto il duplice evento, fermo restando che la determinazione del *locus commissi delicti* è strettamente legata alle modalità di manifestazione della condotta criminosa. Da ultimo, sarà trattata la fattispecie di indebito utilizzo e falsificazione di carte di credito e di pagamento, che riscontra un punto di contatto con il crimine

cibernetico quando la condotta viene posta in essere nel *dark web* ovvero per mezzo di servizi di *home banking,* rendendo così ostica l'individuazione del punto esatto in cui si consuma il reato.

In conclusione, nel quarto capitolo, l'attenzione sarà rivolta ad esaminare possibili prospettive *de iure condendo.* Difatti si evidenzierà come, in attesa di un intervento legislativo volto a sopire le problematiche sulla presente tematica, si riveli necessaria un'interpretazione evolutiva dei principi tradizionali per adattarli alla realtà cibernetica, ontologicamente aterritoriale e atemporale.

Dapprima si analizzeranno, dopo brevi considerazioni introduttive, le soluzioni *de iure condito* che si sostanzieranno in un'interpretazione evolutiva dei principi tradizionali, alla luce degli orientamenti dottrinali e giurisprudenziali. Successivamente si disquisirà sulle possibili soluzioni *de iure condendo,* con l'obiettivo di sollevare eventuali spunti di riflessione in merito ad un futuro intervento legislativo. In particolare, ci si chiederà se l'*input* per l'auspicato intervento normativo potrebbe avvenire avendo a mente l'esperienza nazionale nel settore della diffamazione commessa mediante trasmissioni radiofoniche o televisive di cui all'art. 30 comma 5 della legge del 6 agosto 1990 n. 223, la quale individua quale foro territorialmente competente il luogo di residenza della persona offesa; ovvero ancora volgendo lo sguardo al progetto di legge in tema di diffamazione *online*, che intende far chiarezza in merito all'individuazione del *locus* per tale fattispecie. Ebbene da tali esperienze è possibile trarre un criterio applicabile alle ipotesi in cui venga in considerazione un reato cibernetico, al fine di scongiurare i dubbi che lungamente hanno attanagliato dottrina e giurisprudenza.

Si verificherà poi se un altro spunto di riflessione rilevante, in attesa di un intervento legislativo, potrà emergere dalle esperienze dei paesi europei sulla medesima questione, per cui a tal fine sarà esaminata, sempre in un'ottica de *iure condendo,* dapprima l'esperienza spagnola, secondariamente quella francese e infine quella tedesca. L'analisi di questi ordinamenti permetterà di evidenziare come questa tematica riguardi tutti i paesi in questione, alla luce della natura transnazionale degli illeciti cibernetici, i quali con soluzioni differenti hanno cercato di porre fine al dibattito in merito, per cui ad essi si dedicherà l'attenzione, al fine di prospettare soluzioni valevoli nella legislazione nazionale.

Concludendo si sottolineerà come nel *cyber*, più di ogni altra materia, presente e futuro abbiano un confine labile, per cui è necessario adottare soluzioni flessibili al passo con l'evoluzione tecnologica.

CAPITOLO I

IL *CYBERCRIME* E I *CYBERATTACKS*

SOMMARIO: 1. La nascita e lo sviluppo del *cyberspace*. – 2. Il fenomeno dei *cyberattacks* e le tipologie di attacco. – 2.1 Il *malware*. – 2.2 *Il ransomware*. – 2.3 Il *phishing*. – 2.4 Il *pharming*. – 3. La criminalità informatica: rilievi introduttivi. – 4. Inquadramento normativo. – 4.1 La legge n. 547/1993. – 4.2 La Convenzione di Budapest, 23 Novembre 2001. – 4.3 La legge di ratifica della Convenzione: legge n. 48/2008. – 5. La prevenzione come risposta alla criminalità informatica: la *cybersecurity*. – 6. Le caratteristiche principali del fenomeno: la desensibilizzazione e l'aterritorialità.

1. La nascita e lo sviluppo del *cyberspace*

L'evoluzione tecnologica ha contribuito alla trasposizione del fulcro delle attività sociali, politiche ed economiche in una nuova dimensione, quella del cyberspazio.

Il termine *cyberspace* fu coniato dallo scrittore William Gibson nella prima metà degli anni Ottanta, in un racconto di fantascienza dal titolo *Burning Chrome* e successivamente utilizzato nel romanzo *Neuromancer*. Con tale espressione lo scrittore si riferiva ad un luogo immaginario di allucinazioni tecnologiche composto da dati, in cui uomini e computer si fondevano per creare un'unica realtà, che veniva contrapposta allo spazio reale[2]. Tale vocabolo ha acquisito differente accezione a partire dalla prima metà degli anni Novanta, con l'avvento di Internet, indicando un ambiente informatico volto allo scambio di informazioni attraverso sistemi interconnessi[3]. Lo spazio cibernetico non coincide con Internet, ossia con il sistema di reti di telecomunicazioni, ma si tratta di un ambiente virtuale di più ampio spettro. Sebbene non esista un'unica definizione comunemente accettata, esso viene

[2] Cfr. GIBSON, *Neuromante,* 1986 «*Cyber*spazio: un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...]». Il termine *cyber* deriva dal termine greco "kibermetikos", che significa navigatore e nel linguaggio corrente tale termine è utilizzato per indicare lo spazio in cui agiscono ed interagiscono programmi informatici e utenti.

[3] V. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del* cyber*spazio e i suoi effetti sulla politica internazionale,* in *Politica&Società*, 1/2018, 61 ss.

definito oggi quale insieme di infrastrutture informatiche tra loro connesse, costituito da *hardware*, *software*, dati ed utenti, nonché dalle relative relazioni intercorrenti tra gli stessi[4], come indicato dall'art. 2 del decreto del Presidente del Consiglio dei ministri n. 66/2013[5]. In altre parole, il *cyber*spazio comprende Internet e le reti di comunicazione, nonché i sistemi informatici in cui vengono elaborati dati.

Alcuni studiosi stratificano tale ambiente virtuale in quattro differenti livelli: uno fisico, composto da dispositivi materiali, che permettono il funzionamento della rete; un livello logico, in cui vi è l'assemblaggio delle diverse componenti, che offrono servizi agli utenti; un livello di informazione, in cui vi è la creazione e distribuzione dell'informazione e l'interazione tra gli utenti; un livello personale, riferito ai singoli individui che compiono operazioni *online*[6]. Diversamente altri studiosi, come Martin C. Libicki, rappresentano il *cyberspace* su tre livelli: fisico, sintattico, semantico. Il primo fa riferimento agli elementi materiali; il secondo si pone ad un livello superiore, contenente informazioni e istruzioni che i progettisti e gli utenti danno allo strumento informatico; e il terzo rielabora i dati contenuti nelle macchine[7]. Questo porta a considerare il cyberspazio quale nuova dimensione, al cui interno si esplicano le dinamiche relative ai singoli Stati, quale guerra e pace.

Tale dimensione è caratterizzata dal dinamismo, posto che è stata creata dall'uomo e può essere modificata dallo stesso, al passo con il progresso in campo scientifico e tecnologico e ciò la rende difficilmente identificabile e gestibile. Le peculiarità dello spazio cibernetico si ravvisano nella sua connotazione dematerializzata, deterritorializzata, atemporale, nonché nell'anonimato che viene garantito. Queste caratteristiche permettono di differenziare le condotte che si esplicano in rete da quelle tradizionalmente intese, in quanto un soggetto può facilmente svolgere un'operazione complessa, connettendosi in più luoghi virtuali,

---

[4] Si veda MENSI, *La sicurezza cibernetica*, in MENSI, FALLETTA, *Il diritto del web*, Padova, 2018, 281.

[5] V. *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale* adottata con d.p.c.m. 24 gennaio 2013, pubblicato nella Gazzetta Ufficiale 19 marzo 2013, n. 66.

[6] Così PANATTONI, Compliance, cybersecurity *e sicurezza dei dati personali*, Assago, 2020, 7 s.

[7] Sul punto MARTINO, *La quinta dimensione della conflittualità*, cit., 64 s.

anche nello stesso momento. Esso è un luogo privo di confini spaziali e ciò rende problematica l'applicazione di quei principi, tra cui quello di territorialità, che esigono l'individuazione di un luogo in cui viene realizzata la condotta, per cui si è parlato di anarchia del *cyber*spazio. L'utente, inoltre, può programmare un'attività anche in tempi diversi e svolgere la stessa attraverso operazioni automatizzate, che non necessitano di un contatto fra persona e sistema informatico[8].

Altro elemento caratterizzante è la pervasività, che permette di qualificare il *cyber*spazio come un'arena in cui si stabiliscono quotidianamente interconnessioni a livello globale, in cui si esplicano le fondamentali libertà di informazione, espressione e associazione del cittadino, che può accedervi con risorse minime. Gli individui usufruiscono dei vantaggi che il *cyberspace* offre, quale luogo imprescindibile per lo sviluppo economico, sociale e culturale, grazie alle *Information and Communication Technologies*, vale a dire quei metodi e tecniche che permettono agli utenti di creare, immagazzinare e scambiare informazioni. Oggi sono resi disponibili dispositivi sempre più sofisticati, in grado di operare ovunque, grazie alla copertura data dalle reti di comunicazione di dati, nonché dalle numerose tecniche di connessione garantite, che assicurano la presenza costante degli individui nel *cyberspace*. Sono presenti in rete i servizi più disparati, che consentono agli utenti di disporre in qualsiasi momento di notizie aggiornate, di accedere al *cloud*, acquistare o vendere qualsiasi merce o bene, nonché creare, progettare e realizzare iniziative, fino alla disponibilità di nuove valute c.d. virtuali, «tutto diviene *electronic* o *digital*, dall'*e-commerce*, alla *digital economy*, dall'*e-tourism*, all'*e-art*, e così via»[9]. Il sistema economico e sociale nel suo complesso è diventato dipendente dal *cyberspace*. Gli stessi servizi essenziali per il Paese, quali acqua, luce, gas, trasporto su strada, rotaia ed aereo, vengono erogati attraverso reti telematiche che garantiscono, grazie alla interconnessione, un elevato *standard* di qualità nella fornitura e nell'accesso ai servizi[10]. Si tratta delle cosiddette "infrastrutture critiche", ossia quelle infrastrutture essenziali per il

[8] Così FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 10/2015, 1297.

[9] V. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Cybercrime*, Torino, 2019, 39 s.

[10] In tal senso VULPIANI, *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in *Riv. di criminologia, vittimologia e sicurezza*, 2007, I(1), 46-54.

mantenimento delle funzioni vitali della società e della sicurezza, dalla cui distruzione o malfunzionamento deriverebbe un impatto rilevante per il Paese e che per l'interesse nazionale ricoperto, necessitano di adeguata protezione[11]. Difatti, sebbene tale spazio sia privo di confini, *ergo* di frontiere nazionali, gli Stati sono i principali attori nell'assicurare la sicurezza dello stesso, proteggendo reti ed infrastrutture e, proprio a tal fine, sorge la necessità del rispetto degli indirizzi strategici, varati dal singolo Stato, da parte di tutti gli attori coinvolti. Vanno riportati nello spazio cibernetico i valori e i diritti democratici, con l'esigenza di assicurare un adeguato bilanciamento tra questi e le esigenze di libertà che lo contraddistinguono. L'obiettivo è quello di arginare le minacce che provengono da questa dimensione, che implica vulnerabilità per la sicurezza.

Accanto agli aspetti positivi, quali la digitalizzazione e le interconnessioni tra utenti, che hanno facilitato le interazioni e hanno contribuito ad uno sviluppo economico delle attività produttive, il *cyber*spazio nasconde anche aspetti critici derivanti dalle sue stesse caratteristiche. Esso in sé non è minaccioso, ma tali criticità sembrerebbero ravvisarsi in nuove forme di aggressione commesse da singoli individui o da gruppi criminali e rivolte alle infrastrutture fisiche, ai diritti degli utenti, alle attività produttive e agli stessi Stati, che si traducono in minacce cibernetiche, vale a dire condotte che vengono realizzate nello spazio cibernetico, grazie ad esso ovvero in danno di quest'ultimo: si tratta di strumenti in grado di danneggiare capacità nazionali e non solo. Queste minacce, sebbene perpetrate in uno spazio intangibile, hanno conseguenze dirette nella realtà fisica e la caratteristica dell'anonimato rende difficoltoso perseguire simili condotte.

Le forme di aggressione che si manifestano sono mutevoli e caratterizzate da asimmetria, a causa del continuo sviluppo delle stesse, che mette a rischio tutti i sistemi informativi esistenti. L'asimmetria consiste nel fatto che le stesse possono colpire da grandi distanze, essendo sufficiente un accesso alla rete, possono attaccare sistemi sofisticati e con un'efficacia tale da non garantire un'adeguata

[11] Cfr. la Direttiva 2008/114/CE del Consiglio dell'Unione Europea relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, recepita dall'Italia con d.lgs. n. 61 dell'11 aprile 2011.

azione difensiva[12]. Tali minacce sfruttano le vulnerabilità tecniche e organizzative, che scaturiscono da una mancata implementazione della sicurezza. Proprio per tali motivi, è demandato agli Stati, in cooperazione con i privati, garantire stabilità e sicurezza per evitare la concretizzazione di simili minacce. L'individuazione preventiva e la mitigazione delle vulnerabilità e dei problemi di sicurezza presenti nella configurazione dei sistemi comporta una conseguente riduzione dei costi per l'implementazione dei controlli di sicurezza.

2. Il fenomeno dei *cyberattacks* e le tipologie di attacco

La digitalizzazione ha esteso l'utilizzo di dispositivi informatici e l'accesso alla rete ad un numero di utenti sempre maggiore. Questo ha permesso la creazione di nuove aree di vulnerabilità dei sistemi e dati informatici, che vede il moltiplicarsi di potenziali vittime e attori delle minacce. Se da un lato la tecnologia ha permesso un'adeguata gestione delle risorse, dall'altro presenta anche degli aspetti negativi da identificare nelle suddette aree di vulnerabilità. L'evoluzione progressiva delle *Information and Communication Technologies*, con il conseguente legame di dipendenza tra queste ultime e ogni settore economico e sociale, comporta infatti che un incidente in materia di sicurezza informatica possa coinvolgere ed interessare enti o organizzazioni di più Stati[13]. Proprio il continuo mutamento e sviluppo che caratterizza le modalità di aggressione utilizzate dai *cyber*-criminali, rende ardua l'esistenza di sistemi informativi completamente sicuri, quindi non vulnerabili.

Ai sensi dell'art. 2 n. 8 del Regolamento sulla *cyber*-sicurezza, per minaccia informatica si intende «qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone»[14].

L'attacco informatico è definito più specificamente come il tentativo di ottenere un accesso non autorizzato a servizi, risorse o informazioni di sistema o di

[12] V. Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, Dicembre 2013.

[13] Si veda FLOR, Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo:* dalla CIA-triad protection *ai più recenti sviluppi*, in *Riv. dir. Internet*, 3/2019, 443 ss.

[14] Art. 2 n. 8, Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, *Cybersecurity Act*.

comprometterne l'integrità, e in generale consiste nell'atto intenzionale di tentare di eludere uno o più servizi di sicurezza o controlli di un sistema informativo digitale[15].

Le minacce cibernetiche si possono distinguere in cinque macro-categorie, a seconda delle finalità: l'*hacktivismo,* che ha per lo più finalità dimostrative e mira a creare un danno di immagine e che si verifica in concomitanza di tensioni e crisi politiche; il crimine cibernetico o *cybercrime,* che colpisce principalmente il settore privato ed ha ad oggetto attività con finalità criminali, volte ad ottenere denaro o sottrarre informazioni allo scopo di trarne profitto; *cyber*-spionaggio, che ha come bersaglio obiettivi industriali e scientifici, al fine di carpire dati e informazioni sensibili; *cyber*-terrorismo, che colpisce organizzazioni, Stati e individui, con azioni ideologicamente motivate; guerra cibernetica, che consta di operazioni militari e l'organizzazione delle medesime attività, tramite il *cyberspace*[16]. Le minacce sono, pertanto, sempre più insidiose e difficili da contrastare.

Gli attacchi cibernetici si distinguono, sul piano della modalità di azione, a seconda che siano posti in essere tramite un'unica operazione – c.d. attacchi semplici – ovvero attraverso più operazioni tra loro collegate – c.d. attacchi complessi.

Essi possono essere catalogati in base all'oggetto dell'attacco, il quale può essere il sistema informatico o le infrastrutture fisiche o logiche, ovvero i dati e le informazioni. Nel primo caso, si parla di attacchi informatici attivi, diretti ad alterare o comunque danneggiare il sistema o le sue infrastrutture, compresi i *devices* collegati; nel secondo caso, si fa riferimento ad attacchi informatici passivi, diretti ad acquisire, utilizzare indebitamente, alterare o danneggiare dati o informazioni, senza coinvolgere sistemi o infrastrutture su cui sono archiviati.

Tali attacchi possono distinguersi, in base alle modalità di realizzazione, in attacchi fisici, sintattici, semantici. L'attacco fisico consta di attività dirette contro le infrastrutture fisiche, le parti *hardware,* come computer, *server*, dispositivi, cavi. L'attacco sintattico consiste in attività malevole rivolte verso le soluzioni *software*,

[15] La definizione è stata desunta dal *website "National Initiative for Cybersecurity Careers and Studies", www.niccs.us-cert.gov.*

[16] Sul punto GORI, *Le nuove minacce* cyber, in *Informazioni della Difesa*, Periodico dello Stato Maggiore della Difesa, Supplemento al n. 6/2014, 16.

essenziali per il funzionamento dei sistemi e delle reti. L'attacco semantico consta di attività malevole che incidono sulle interazioni tra l'utente e il computer, ossia nella modifica di informazioni corrette e nella diffusione di informazioni errate[17].

Altro elemento caratterizzante consiste nel fatto che gli stessi possono essere attuati con violenza, attraverso danneggiamento di sistemi informatici, dati, informazioni o *software*, ovvero possono essere realizzati tramite una condotta fraudolenta, in cui vi è la cooperazione artificiosa della vittima[18].

I *cyberattacks* possono indirizzarsi verso diversificati *target*, tra cui infrastrutture critiche, sistemi finanziari e di pagamento, privati. Sono tutti bersagli vulnerabili, che se attaccati possono paralizzare la struttura economico-sociale del Paese. Con riferimento alle infrastrutture critiche, si tratta di settori nevralgici per gli interessi del Paese e ciò che rileva è il carattere essenziale di queste rispetto al mantenimento delle funzioni vitali della società, quali la salute pubblica, la sicurezza pubblica e il benessere economico e sociale dei consociati.

A ben vedere, tali infrastrutture non costituiscono l'unico bersaglio dei *cyber*-criminali: oggi gli attacchi si rivolgono sempre più spesso verso privati e piccole aziende, che sono più vulnerabili, in quanto soggetti ignari e non completamente istruiti sulle molteplici quantità di attacchi esistenti, che possono essere sferrati anche con una semplice *mail*. I soggetti attaccanti utilizzano spesso tecniche di ingegneria sociale, che manipolano un determinato soggetto per reperire informazioni e dati. Attraverso tale tecnica, non si vanno a sfruttare dei *gap* tecnici dei sistemi di sicurezza, ma si sfrutta la risorsa umana, tramite la sua manipolazione. L'attaccante studia i comportamenti della vittima nell'utilizzo della rete, così da far leva sullo stato mentale della stessa ai fini dell'acquisizione di informazioni. Inoltre, occorre rilevare che il soggetto attaccante non va ad identificarsi esclusivamente con un unico individuo, ma sempre più spesso con sodalizi criminali, che sfruttano la rete per trarne profitto.

Gli attacchi che utilizzano tecniche di *social engineering* possono essere suddivisi in quattro fasi: la prima, quella del "*footprinting*", consta di un'attività preparativa di studio delle modalità più opportune con cui approcciarsi alla

[17] In tal senso PANATTONI, Compliance, cybersecurity *e sicurezza,* cit., 26.
[18] V. FLOR, Cybersecurity *ed il contrasto ai* cyber-attacks, cit., 454.

potenziale vittima e di recupero informazioni e può trattarsi di una fase anche molto lunga a seconda della complessità dell'attacco; la seconda fase è quella del "contatto", in cui l'attaccante inizia a stabilire un contatto con la vittima, cercandone la fiducia e complicità; la terza è quella della "manipolazione psicologica", in cui si sostanzia l'attacco, con cui l'ingegnere sociale cerca di carpire le informazioni tramite tecniche psicologiche con strumenti atti ad influenzare la vittima; l'ultima fase è quella della "fuga", in cui si termina l'attacco e si consolidano i risultati ottenuti, facendo perdere ogni traccia[19].

È importante quindi predisporre, a fini preventivi, delle contromisure come *antivirus*, *firewall*, nonché un'adeguata formazione e conoscenza di queste tecniche da parte dell'utente. Grazie all'installazione di un *software antivirus* è possibile limitare il rischio di propagazione di attacchi, in quanto esso isola il *software* malevolo prima che questo possa contaminare ulteriori dati, tramite la «scansione della memoria e delle unità a disco all'interno delle quali, se vengono rintracciate specifiche sequenze di *byte,* può affermarsi che il sistema è infetto e deve essere bonificato»[20]. Una volta individuato il *virus* malevolo si avvisa l'utente e si tenta di bonificare il sistema attraverso la sua neutralizzazione.

Accanto agli *antivirus*, un ruolo importante per la sicurezza delle infrastrutture è il *firewall*, che viene definito come «un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi»[21], in modo tale da evitare connessioni pericolose per il sistema. Esso opera come una specie di filtro, di cui esistono varie tipologie a seconda che l'attività di protezione sia destinata ad una piccola rete o ad una rete più ampia, come quella aziendale.

Ad ogni modo, le contromisure analizzate devono essere combinate con un'adeguata conoscenza e opportuna formazione da parte dell'utente dei rischi che si possono concretizzare: la prevenzione è possibile, infatti, solamente ove vi sia consapevolezza delle minacce, che possono derivare dal cyberspazio.

---

[19] Sul punto CAPONE, *Gli attacchi di ingegneria sociale*, in *www.cyberlaws.it,* 8 marzo 2018.

[20] Si veda CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, 2009, 125 s.

[21] Così definito da Cisco, in *www.cisco.com*.

I danni derivanti da un attacco informatico sono molteplici: vi è, innanzitutto, un rilevante impatto economico che si esplica direttamente con l'interruzione dell'attività causata dalla compromissione di determinati sistemi o dati, con il pagamento di un eventuale riscatto richiesto dall'attaccante e con la perdita di informazioni personali; altra fonte di danno si ravvisa nelle spese economiche da sostenere per implementare la sicurezza, *ergo* misure di protezione, per evitare la reiterazione di simili attacchi, in quanto all'incremento degli attacchi corrisponde un aumento dei costi per la sicurezza.

Accanto alle conseguenze summenzionate, di più diretta evidenza, si affiancano i danni reputazionali, legali e sanzionatori: gli attacchi informatici possono causare un danno di immagine, che deriva dal non aver adottato preventivamente adeguate misure di protezione, che può di conseguenza far sorgere forme di responsabilità nei confronti dei fruitori derivanti dalla perdita di dati, che può a sua volta determinare l'applicabilità di sanzioni, secondo il *framework* nazionale ed europeo[22].

Il fenomeno dei *cyberattacks* ha assunto una rilevanza sempre maggiore, dovuta alla rapida evoluzione delle modalità di attacco e dell'efficacia degli stessi: secondo il rapporto CLUSIT 2020, il 2019 è stato l'anno in cui vi è stata un'evoluzione delle minacce *cyber*, sia dal punto di vista qualitativo che quantitativo, osservando una crescita degli attacchi, della gravità e dei danni che ne conseguono. Dal punto di vista quantitativo, rispetto al 2014, la crescita degli attacchi gravi di pubblico dominio è stata del +91,2%[23]. Rilevano, principalmente, attacchi industrializzati su scala planetaria, che hanno bersagli molteplici, quali infrastrutture, reti, *server*, *client*, *devices* mobili, piattaforme social. Lo studio CLUSIT ha evidenziato che gli attacchi gravi di pubblico dominio nel 2019 sono stati 1.670, segnalando un aumento rispetto al 2018 (+7,6%), con una media di 139 attacchi gravi al mese[24]. Dal rapporto emerge che gli attacchi gravi sono compiuti maggiormente per finalità di "*cybercrime*", che resta la principale causa degli attacchi, con un aumento del +12,3% rispetto al 2018 e del +162%

[22] Sul punto PANATTONI, Compliance, cybersecurity *e sicurezza*, cit., 29.
[23] Dati ricavati dal Rapporto CLUSIT 2020.
[24] *Ivi*, 16.

rispetto al 2014[25]. Gli attacchi sono considerati gravi quando hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione e di diffusione di dati sensibili. Tra le tecniche di attacco maggiormente diffuse si segnalano la categoria dei "*malware"*, la categoria "*phishing/social engineering*" e la categoria "*Distributed Denial of Service* (DDoS)". Si evidenzia nel rapporto anche la presenza di attacchi eseguiti con tecniche sconosciute, rientranti nella categoria "*unknown*", che mette in luce come gli attacchi siano sempre più sofisticati, oggetto di costante sviluppo e mutamento, tale da non rendere conoscibili le stesse tecniche con cui vengono perpetrati.

Una delle principali problematiche, afferenti questo fenomeno, è la mancata denuncia degli attacchi che contribuisce alla creazione di cifre nere, che non ne permette uno studio completo. Ciò fa notare come al cuore della questione ci sia anche un problema culturale. Secondo il report IOCTA (*Internet Organized Crime Threat Assessment)*, elaborato all'interno di Europol, è necessario rafforzare le attività di contrasto, tramite un'efficace cooperazione pubblica e privata e attraverso risposte coordinate a tali attacchi[26].

2.1 Il *malware*

Il *malware* è considerato la tecnica di attacco maggiormente diffusa e costituisce uno degli aspetti negativi rilevanti della digitalizzazione, in quanto è in grado di colpire sistemi, dispositivi mobili e reti, senza il consenso dell'utente. Il termine *malware* deriva dall'espressione "*malicious software*", letteralmente *software* malintenzionato, vale a dire un *software* malevolo, progettato per accedere ad un sistema informatico per rubare dati personali, spiare le vittime e danneggiare i sistemi, *ergo* hanno la funzione di interferire con le normali operazioni svolte da un computer.

Esistono diverse tipologie di *malware*, le quali però possiedono un unico modello strutturale, basato su quattro fasi: infezione, quiescenza, propagazione e esecuzione. La prima fase è quella dell'infezione, in cui il *software* malevolo si introduce nel sistema, superando le eventuali misure di protezione predisposte, vi

[25] *Ivi*, 18.
[26] V. IOCTA 2019, *European Cybercrime Centre (EC3)*, Europol.

si installa e modifica le impostazioni del sistema in modo tale che resti occultato. Il *malware* si inserisce all'interno del sistema bersagliato tramite diversi canali, tra cui il trasferimento materiale del codice virale, che per mezzo di un supporto fisico di memorizzazione viene trasferito al sistema, prevedendo un accesso al computer. Tra i canali di trasmissione dell'attacco vi sono ancora la posta elettronica e il *web*: nel primo caso il *malware* si inserisce tramite allegati di posta elettronica, che grazie a tecniche di *social engineering* vengono aperti dall'utente bersaglio, circuito; nel secondo caso si trasmette il *software* malevolo attraverso un *download* dal *web*, la cui azione può essere svolta dalla stessa vittima, che inconsapevolmente scarica un determinato *file* apparentemente innocuo ovvero dall'attaccante che trasmette il *malware*, grazie alla semplice apertura di una pagina *web*[27]. Quest'ultimo è attualmente il canale maggiormente diffuso, accanto alla trasmissione tramite posta elettronica. La fase dell'infezione richiede l'attivazione del codice virale e spesso ciò avviene mediante la cooperazione della vittima, che inconsapevolmente apre *file*, attua *download* senza conoscerne la reale natura maligna.

La seconda fase è quella della quiescenza, che si protrae fino alla disattivazione del codice malevolo o fino alla eliminazione da parte di *software* di protezione e durante la quale il *software* resta silente fino alla sua attivazione, vale a dire una condizione che determini la sua attivazione. Una volta inserito il *software* risiede nella memoria del computer, pertanto gli attaccanti utilizzano tecniche di occultamento per confonderlo con gli altri programmi presenti in memoria, così da evitare che venga individuato dai *software* di protezione.

La terza fase è quella della propagazione o replicazione, che non è presente in tutte le tipologie di *malware* e si sostanzia nel replicarsi e propagarsi dello stesso ad altri sistemi, infettandoli.

La quarta fase è quella delle azioni malevole, ovverosia quel momento in cui il *software* esegue i suoi compiti ed avviene il danneggiamento del sistema e il furto di dati. Dopo quest'ultima fase, il *software* malevolo torna alla fase di quiescenza, sempre che il sistema non venga definitivamente compromesso[28].

[27] Cfr. MEZZALAMA, LIOY, METWALLEY, *Anatomia del malware*, in *Riv. Mondo Digitale*, 47/2013, settembre 2013, 3 ss.

[28] *Ivi*, 2 s.

Il *malware* è una macro-categoria in cui sono ricomprese varie tipologie, come *virus, worm, trojan horse, spyware, adware, keylogger, ransomware*.

Il *virus* infetta dei *file*, attaccandosi ad un programma ospite, in modo tale da danneggiare il sistema, cancellare dati, aprire *backdoor*, disattivare *software* di rilevazione *virus*, nonché rallentare in generale il computer. Questo entra in azione solo quando viene eseguito il programma che lo ospita e quest'ultimo, a sua volta contagia, altri *file*[29]. Un esempio di *virus* che nel 1999 colpì numerosi sistemi è "*Melissa*", che viaggiava attraverso posta elettronica come allegato *mail*. Una volta aperto l'allegato, infilandosi nella rubrica di *Microsoft Outlook*, il *virus* si rispediva ai primi cinquanta indirizzi mail, così diffondendosi su altri sistemi[30]. Si stima che abbia causato danni per circa un miliardo di dollari.

Il *worm* è un *software* dotato di autonomia, progettato per diffondersi su diversi computer mediante una rete e, a differenza del *virus*, non ha bisogno di un programma ospite in cui annidarsi. Lo scopo del *worm* è quello di infettare computer, saturandone le risorse, senza danneggiare i singoli *file*. Esso opera mediante lo sfruttamento delle vulnerabilità del sistema attaccato, selezionando poi gli indirizzi collegati alla rete, come pure la lista dei contatti di posta elettronica dell'utente, costituenti un ulteriore potenziale bersaglio, per auto propagarsi.

Uno degli attacchi *worm* più famosi è l'attacco "*I love you*", scoperto nel 2000, che ha colpito milioni di computer attraverso l'invio di un allegato *mail*, con testo "*I love you*" nell'oggetto. Il *worm* selezionava i destinatari tramite delle *mailing list*, pertanto i messaggi sembravano provenire da conoscenti: una volta aperto l'allegato, il *worm* si autoriproduceva, inviando una copia alla rubrica e con l'indirizzo dell'utente come mittente e causando il rallentamento del computer fino a renderlo inutilizzabile. Si stima che abbia causato danni in 10 miliardi di dollari[31].

Un altro esempio di attacco è "*Conficker"*, scoperto nel 2008. Esso si diffonde su piattaforme *Microsoft Windows*, sfruttando una falla di rete del sistema, ma può essere diffuso anche medianti ulteriori vettori, quali chiavette *usb* o ancora

---

[29] Sul punto CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 122.

[30] Sul punto DI GIORGIO, *Melissa, virus velenoso come un serpente a sonagli*, in *la Repubblica*, 29 marzo 1999.

[31] Cfr. LANA, I love You, *venti anni fa il primo virus informatico che ha messo il mondo in ginocchio*, in *www.corriere.it*, 4 maggio 2020.

hard-disk esterni. Tale *software* infetta sistemi operativi e attua il *download* di altri *malware* da pagine *web* indicate dall'attaccante. *Conficker* ha creato diversi danni e potrebbe aver infettato fino a nove milioni di *personal computer* in tutto il mondo[32].

Il *trojan horse* si introduce in maniera silente nel sistema, dato che si mostra come un programma utile, il quale cela però funzionalità dannose, eseguite all'insaputa della vittima. Esso è composto «generalmente da 2 *file*: il *file server*, che viene installato nella macchina vittima, ed un *file client*, usato dall'attaccante per inviare istruzioni che il *server* esegue»[33]. In tal modo l'attaccante riesce ad avere il totale controllo e il libero accesso al computer vittima fino ad arrivare alla captazione dei flussi di dati, all'attivazione del microfono per registrare l'audio ambientale e l'attivazione della videocamera per scattare foto. Il controllo viene di frequente assunto grazie a "*backdoor"*, che consentono a un soggetto esterno di prendere il controllo remoto di una macchina senza il consenso dell'utente. Questo *malware* non ha la capacità di auto propagarsi, pertanto deve essere inviato dal *cyber*criminale alla singola macchina che si ha intenzione di infettare.

Spesso i diversi *malware* agiscono congiuntamente, ad esempio tramite l'invio di un *worm* in rete volto ad installare *trojan* su diversi sistemi, anche per la creazione di una *botnet*, ossia una rete di computer assoggettati al controllo di un amministratore malevolo, i quali vengono utilizzati, a loro volta, per sferrare ulteriori attacchi. Tra i *trojan horse* recenti si annovera l'attacco "*Ginp il mobile banking trojan*", che ha sfruttato la sensibilità della popolazione, generata dall'emergenza sanitaria causata dal *virus SARS-CoV-2* (*Covid-19*). Tale forma di *trojan* garantisce, infatti, di visualizzare la posizione delle persone risultate positive al *Covid-19* nelle vicinanze, attraverso l'installazione di un'applicazione apparentemente utile che contiene il *trojan*, previa la richiesta di una somma di

[32] Così MARKOFF, *Worm Infects Millions of Computers Worldwide*, in *The New York Times*, 22 gennaio 2009: "*Experts say it is the worst infection since the Slammer worm exploded through the Internet in January 2003, and it may have infected as many as nine million personal computers around the world*".

[33] Così SILVETTI, *I crimini informatici più frequenti degli ultimi anni: tabella riepilogativa e profili giuridici*, in *Quot. giur.*, 4 ottobre 2019.

denaro, che poi non verrà sottratta. L'obiettivo dell'attaccante è quello di entrare in possesso delle credenziali della carta di credito[34].

Tra i *malware* di tipo *trojan* spicca il captatore informatico o "*trojan* di stato", che può essere utilizzato dagli inquirenti a fini di attività investigativa in ambito penale per determinate classi di reati. Grazie al d.lgs. 216/2017 art. 4, con cui è stata attuata la delega contenuta nella legge n. 103/2017 (c.d. legge Orlando), è stata introdotta la disciplina delle "intercettazioni mediante inserimento di captatore informatico", con cui vengono dettate le condizioni di ammissibilità e i limiti di detto strumento, che può essere utilizzato solamente in riferimento a particolari delitti, come delitti di criminalità organizzata ovvero delitti contro la pubblica amministrazione, data l'invasività del mezzo per i delitti fondamentali costituzionalmente tutelati.

Lo *spyware* è un *software* che minaccia gravemente la sicurezza della *privacy*, in quanto ha lo scopo di sottrarre dati sensibili dal sistema su cui è occultamente installato, al fine di trarne profitto. Tale attacco sfrutta le vulnerabilità dei sistemi e la scarsa consapevolezza da parte dell'utente vittima, i cui i dati sottratti vengono inviati, generalmente, ad un *server* remoto al fine di generare pubblicità mirata, sulla base delle preferenze dedotte dalle suddette informazioni.

Lo *spyware* viene pianificato utilizzando tecniche di ingegneria sociale, le quali monitorano le abitudini degli utenti mediante il tracciamento della cronologia della navigazione. Tra i principali vettori di trasmissione di tale *malware* si annoverano i *cookies*, vale a dire i dati di navigazione che i siti *web* memorizzano sui computer dei *client*, i *link* contenenti codici malevoli, la pubblicità ingannevole, che è volta a presentare il software malevolo come utile e infine può essere veicolato tramite altri *malware*[35].

L'*adware* è un *software* che proietta annunci pubblicitari non richiesti, reindirizza l'utente verso siti *web* diversi da quello indicizzato e raccoglie i dati, al fine di profitto, essendo progettato per scopi prettamente commerciali.

---

[34] Sul punto TARSITANO, *Ginp, il* trojan Android *che finge di segnalare i contagiati da Coronavirus*, in *www.cybersecurity360.it*, 25 marzo 2020.

[35] Si veda LOMBARDO, Spyware*: cosa sono, come si diffondono e come eliminarli*, in *www.cybersecurity360.it*, 16 maggio 2019.

Il *keylogger* è in grado di memorizzare tutto ciò che un utente digita su una tastiera, quindi informazioni fondamentali, quali *password* e credenziali utente. Esistono due tipologie di *keylogger*: la tipologia *hardware* necessita dell'inserimento di un dispositivo elettronico all'interno della tastiera o comunque tramite un dispositivo collegato, vale a dire che richiede un contatto tra il soggetto e il computer; la tipologia *software*, invece, consta di un programma informatico, in grado di carpire tutti gli *input*[36].

Tra i *malware* che hanno causato maggiori danni va citato "*Stuxnet"*, scoperto nel 2010 e famoso per aver rallentato notevolmente il programma nucleare in Iran e per aver colpito sistemi industriali, in quanto ha alterato la velocità delle centrifughe dell'impianto per l'arricchimento dell'uranio, portando alla sostituzione forzata di molte macchine. La novità di questo attacco è che esso non mirava semplicemente a carpire informazioni e violare i sistemi, ma era concepito in modo tale da sabotare le infrastrutture fisiche le quali, sebbene non connesse alla rete, venivano attaccate utilizzando come vettore una chiavetta *usb*. Venivano colpiti quei sistemi dotati di particolari configurazioni, restando dormiente su tutti gli altri e creando su questi solamente dei malfunzionamenti non rilevanti. *Stuxnet* era un *software* complesso, che si propagava a tutti i sistemi connessi al programma nucleare iraniano, fino a diffondersi e colpire sistemi diffusi in tutto il globo. Si componeva di tre moduli: un *worm* che permetteva al *software* di auto-replicarsi su altre macchine, un collegamento che permetteva l'esecuzione delle copie e un sistema che occultava lo stesso, redendolo non individuabile. Esso sfruttava quattro vulnerabilità di un *software* che non sono ancora note a nessuno, se non all'attaccante. Si ritiene che tale *malware* sia stato sviluppato da un progetto statale ed è per questo che si parla con riferimento ad esso di arma digitale con scopi offensivi[37].

2.2 Il *ransomware*

Il *ransomware* è un tipo di *malware* estorsivo, che infetta un computer, rendendo inaccessibile il sistema e bloccandone l'utilizzo ovvero criptando i *file* di

[36] Cfr. RIJTANO, Keylogger*: cos'è, come eliminarlo, i migliori per Windows, Mac e cellulare*, 24 maggio 2018, in *www.cybersecurity360.it.*

[37] Si veda FREDIANI, *Guerre di rete*, Bari, 2017, 9 ss.

particolare rilevanza e per il cui ripristino l'attaccante richiede una somma da pagare, vale a dire un riscatto, "*ransom*" appunto, da versare il più delle volte sotto forma di criptovalute. Si è dinnanzi ad una condotta bifasica costituita da una prima fase di attacco ed una seconda fase di minaccia con richiesta di riscatto[38]: una volta inoculatosi e compromesso il funzionamento del sistema ovvero criptati i *file,* sullo schermo appare un messaggio con cui si avvisa dell'infezione e si richiede un riscatto da versare in termini perentori per recuperare detti dati. Come anticipato, la somma da pagare viene versata sotto forma di criptovaluta, la più nota delle quali è il *bitcoin,* che vanta transazioni rapide e permette di non tracciare il *cyber*criminale, in quanto si tratta di una valuta nascosta, che è visibile solamente a colui il quale conosce la chiave di accesso, mentre la transazione risulterà sempre visibile nel sistema *blockchain,* da intendersi come una sorta di libro mastro che conserva permanentemente la storia delle transazioni[39]. Dopo aver effettuato il pagamento, la vittima riceverà una *mail* attraverso cui potrà effettuare il *download* del programma di decriptazione, sebbene possa accadere che il *malware* abbia cancellato definitivamente i dati o reso completamente inservibile il sistema, tale che il pagamento sia risultato futile.

I beni messi in pericolo mediante tale tipologia di *malware* sono la riservatezza e la sicurezza informatiche, la libertà e la confidenzialità dei dati, nonché la *privacy*, in quanto il *cyber*criminale entra in possesso di tutti i dati criptandoli e rendendoli inservibili per l'utilizzatore, il quale è indotto così a pagare una somma di denaro per entrarne nuovamente in possesso nel più breve tempo possibile. L'importo richiesto si aggira, il più delle volte, attorno a poche centinaia di euro, così da prospettare al soggetto vittima un danno ridotto a fronte dell'ingente danno minacciato costituito della perdita di dati.

Il *ransomware* irrompe nel sistema grazie a vulnerabilità presenti nel servizio di rete o mediante *download* da Internet, nonché tramite posta elettronica, come allegato *e-mail*, che resta la tecnica più diffusa: una volta effettuato il *download* e aperto l'allegato il *ransomware* si attiva. Simili tecniche puntano ad

[38] Sul punto LUBERTO, *"*Sex-Torsion*" via* web *e minaccia a mezzo* ransomware*: la nuova frontiera del delitto di estorsione*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Cybercrime*, Torino, 2019, 729.

[39] V. CONSOB, *Le criptovalute: che cosa sono e quali rischi si corrono,* in *www.consob.it.*

ingannare l'utente, che è portato ad aprire gli allegati *mail*, in quanto risultanti provenienti da indirizzi conosciuti.

Il primo attacco *ransomware* documentato risale al 1989 e si trasmetteva attraverso *floppy disk* infetti, i quali venivano lasciati presso studi medici e cliniche. Una volta inserito il disco nel sistema, questo criptava i *file*, rendendoli indisponibili, poi veniva pubblicata sulla schermata una richiesta di riscatto, da pagare in contanti da indirizzare a una casella postale a Panama. Solamente dopo aver ricevuto il denaro, veniva inviato un programma di decriptazione per consentire all'utente di tornare nella disponibilità dei dati[40]. Questo attacco ebbe una diffusione limitata, in quanto poche persone all'epoca utilizzavano il computer.

Gli attacchi sono stati implementati dalla pervasività della tecnologia e della crittografia che hanno concesso ai *cyber*criminali nuove tecniche con cui perpetrare condotte simili, sempre più efficaci. Oggi il *ransomware* rappresenta la tipologia di *malware* più diffusa: basta pensare che secondo il rapporto CLUSIT 2020, nel 2019 sono stati quasi la metà del totale degli attacchi di tipo *malware*[41]. Esistono numerose famiglie di *ransomware*, la cui varietà rende spesso complicato per gli apparati di protezione riconoscerli e proteggersi da essi. Nel 2013 viene individuato per la prima volta il *software* malevolo "*CryptoLocker*", che è stato poi affinato nel 2017. Esso ha infettato i sistemi operativi *Microsoft Windows*, diffondendosi mediante allegato di posta elettronica ovvero attraverso un computer assoggettato ad una *botnet*, vale a dire una rete di computer controllabili da un amministratore malevolo, che utilizza la stessa per lanciare attacchi simultanei. Dopo aver eseguito il *software* che si presenta come un *file zip* con estensione "*pdf*", sebbene non lo sia, questo si connette ad un *server* di controllo, difficilmente rintracciabile, che genererà una chiave di tipo "*RSA*"[42], la quale permette di cifrare i dati, rendendoli inaccessibili all'utente. Una volta cifrati i dati, appare una schermata con cui viene

[40] Cfr. PANADA, UNTERBRINK (a cura di), Ransomware*: un flagello che prende di mira privati e aziende*, in *Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia*, 2017, 205, in *www.clusit.it*.

[41] V. *Analisi delle principali categorie di malware*, in *Rapporto CLUSIT 2020*, 2020, 29, in *www.clusit.it*.

[42] Per un approfondimento si veda BONAVOGLIA, *Cifrari a chiave pubblica*, in *www.crittologia.eu*: egli spiega che la chiave di tipo *RSA* funziona tramite due chiavi distinte, usate per cifrare e decifrare, anche per questo dette cifrari asimmetrici. Si tratta di chiavi diverse tra loro dipendenti, ma dall'una non è possibile risalire all'altra, ergo sebbene sia possibile conoscere la chiave di cifratura non è possibile risalire a quella di decifratura, che resterà privata.

presentata una richiesta di riscatto per decifrare i dati da effettuare entro un certo termine. Se il pagamento non avviene entro il termine, l'attaccante cancella la chiave privata che permette di decifrare i dati e questi non potranno essere più recuperati, ma il più delle volte, anche qualora il riscatto venga pagato, il soggetto non entra più in possesso dei suoi dati.

Tra gli attacchi maggiormente dannosi, si annovera anche "*WannaCry*", che nella primavera del 2017 ha colpito oltre duecentomila sistemi informatici, collocati in varie parti del globo, causando perdite per diversi miliardi di dollari. Esso opera come un *crypto-ransomware*, vale a dire un tipo di attacco che rende inaccessibili i dati dell'utente che risultano codificati e ne promette il ripristino, previo pagamento di un riscatto da versare in *Bitcoin.* Nel caso di specie, *"WannaCry"* si è diffuso per mezzo di finte *mail* e di un *exploit* chiamato *EternalBlue*, sviluppato dall'agenzia di sicurezza nazionale statunitense, su computer non aggiornati connessi alla rete con sistema operativo *Microsoft Windows*, sfruttando la vulnerabilità del protocollo di condivisione di file di rete "*SMB*", *Server Message Block:* trattasi di un protocollo che consente di condividere, creare e aggiornare *file* nel *server* remoto. Dopo aver infettato un computer con tale falla, senza intervento da parte dell'utente, il *ransomware* si propaga a tutti gli altri sistemi, che usufruiscono delle condivisioni di rete "*SMB*". Una volta infettato un sistema, il *ransomware* cripta i file, mediante crittografia *RSA,* e presenta una richiesta di riscatto per poter decifrare i dati[43]. Il pagamento del riscatto, tuttavia, non assicura il ripristino dei dati. Ad essere stati infettati sono stati, soprattutto, ospedali ed enti pubblici, più lenti nell'aggiornamento dei sistemi, in quanto *WannaCry* ha attaccato sistemi non aggiornati. Un aggiornamento gratuito del sistema *Windows* garantiva, infatti, la protezione da questo tipo di attacco, che avrebbe reso immune il sistema[44]. L'attacco non ha comportato guadagni cospicui per gli attaccanti, ma ha avuto piuttosto una valenza simbolica, visto il numero dei sistemi infettati.

Accanto a simile attacco perpetrato nel 2017, va menzionato anche il *software* malevolo "*NotPetya*", il quale ha sfruttato ancora una volta l'*exploit*

[43] Cfr. RIJTANO, SBARAGLIA, WannaCry*, cos'è, come funziona e come difendersi dal ransomware che ha fatto piangere il mondo*, 28 giugno 2018, in *www.cybersecurity360.it.*

[44] V. DAL CHECCO, *Il* ransomware Wannacry *infetta PC non aggiornati: ospedali ed enti pubblici a rischio*, 12 maggio 2017, in *www.ransomware.it.*

EternalBlue, tramite protocollo "*SMB*" per la diffusione nelle reti aziendali, colpendo i *file* e richiedendo un riscatto per il ripristino. Esso non solo ha cifrato i dati, ma ha scaricato anche le credenziali dalla memoria del computer, rubando dati. A differenza del *software WannaCry*, questo si è diffuso anche "lateralmente" su sistemi non vulnerabili della stessa rete, permettendo così una diffusione capillare[45].

Contrastare simili attacchi è un'operazione complicata, che deve partire da un'analisi del rischio per individuare i *softwares* esposti a pericolo e in prosieguo adottare le misure di prevenzione ritenute opportune, vale a dire *best practices* da seguire per prevenire gli attacchi. La prima attività da porre in essere è quella di sensibilizzazione e formazione degli utenti, i quali sono invitati a non visualizzare allegati di posta elettronica che non siano attesi, anche se provenienti *prima facie* da enti noti. È necessario dotare il proprio sistema di un *antivirus* aggiornato, nonché aggiornare i sistemi operativi per ridurre le vulnerabilità presenti di *default*. Importante è effettuare un *backup* frequente dei dati, che permetterà di non subire danno alcuno, anche qualora un *ransomware* colpisse il sistema, in quanto i dati risulterebbero recuperabili da altro supporto, previo controllo dell'integrità del *backup* e previa bonifica della macchina intaccata. Altra tecnica è quella di consentire l'opzione "mostra estensioni *file*", che permetterà di individuare *software* potenzialmente maligni.

Queste sono solo alcune delle tecniche di prevenzione e difesa da adottare contro tali attacchi. È proprio la proliferazione di questi che ha portato alla creazione, da parte dei produttori di *antivirus*, di programmi "*decryptor*" gratuiti, in grado di sbloccare e recuperare tutti i *file* criptati. Si tratta di una procedura complessa, che vacilla di fronte agli attacchi sempre più recenti e sofisticati. A tal fine, risulta rilevante citare il progetto internazionale "*No more ransom*", intrapreso dal *National High Tech Crime Unit* della polizia olandese, dall' *European Cybercrime Centre* dell'*Europol*, dal *Kaspersky* e *McAfee*, frutto di una cooperazione tra settore pubblico e privato, in lotta contro il *cybercrime*, che ha l'intento di educare gli utenti alla prevenzione di tali attacchi e all'adozione di

[45] Sul punto FREDIANI, *10 cose da sapere dell'infezione* NotPetya, *e perché è più insidiosa di* Wannacry, 28 giugno 2017, in *www.lastampa.it*.

contromisure per contrastarli, tramite la condivisione delle conoscenze. Esso ha lo scopo di guidare le vittime nel recupero autonomo dei propri dati criptati, non sempre possibile, evitando così il pagamento di un riscatto ai *cyber*criminali, mostrando dei mezzi di recupero alternativi ad esso[46]. Il pagamento del riscatto è sempre sconsigliato per evitare di contribuire alla tenuta in vita delle minacce *ransomware,* inoltre, esso non garantisce la restituzione dei file e non rende esenti da ulteriori attacchi, che potrebbero nuovamente sfruttare la vulnerabilità del sistema ancora presente.

2.3 Il *phishing*

Il *phishing* è una complessa tecnica fraudolenta volta a carpire dati e informazioni riservate di un utente, per realizzare furti di identità e utilizzi non autorizzati di quelle informazioni, che determinano il fulcro offensivo dell'attacco. Nasce come tecnica di *social engineering* che, tramite condotte ingannevoli, raggira la vittima al fine di ottenere informazioni, cedute inconsapevolmente. L'etimologia del termine *phishing* è incerta: si ritiene derivi dall'unione di termini inglesi "*phreaking*" e "*fishing*" – il primo riferito all'uso di frequenze per manipolare un sistema telefonico e il secondo riferito al verbo "pescare" – alludendo alla pesca dei dati dell'utente via *web* ovvero dall'unione delle parole "*password*" e "*fishing*", riferendosi appunto alla pesca di *password*[47]. L'obiettivo del *phisher* è portare l'utente a fornire i propri dati, riguardanti in particolare le credenziali di autenticazione per accedere a servizi bancari *online,* il numero di carta di credito, finanche il numero di carta d'identità, al fine di accedere ad aree esclusive per rubarne l'identità digitale. Lo scopo può essere conseguito mediante l'invio di messaggi di posta elettronica ingannevoli ad un elevato numero di destinatari sconosciuti, contenente messaggi apparentemente provenienti da istituzioni realmente esistenti, con il fine di influenzare il soggetto e indurlo a connettersi a pagine *web prima facie* appartenenti alle suddette istituzioni ed inserire le sue

[46] Cfr. il sito web dedicato al progetto: *www.nomoreransom.org*; si veda anche SANTORO, *Il progetto internazionale "*No more ransom*" alla luce dell'attacco WannaCry,* in *Web&Tech Sicurezza informatica,* 1° giugno 2017.

[47] FLOR, Phishing, identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen*., 2007, 903 s.

credenziali. I messaggi formulati *ad hoc* contengono, solitamente, notizie allarmanti relative a presunti problemi tecnici, piuttosto che segnalazioni di aggiornamenti ovvero di accessi sospetti, che hanno l'intento di indurre il soggetto a cliccare su *link* allegati che conducono a siti fittizi approntati dall'attaccante, apparentemente identici per quanto attiene la grafica al sito reale, e in prosieguo di convincerlo a fornire le credenziali di accesso riservate per porre fine a tali problemi. L'acquisizione di tali informazioni costituisce l'obiettivo del *phisher,* che si realizzerà solo nel momento in cui l'utente fornisce i dati ovvero questi vengano prelevati in via autonoma per mezzo di programmi quali *keylogger* e *web trojan*.

Il numero degli attacchi *phishing* si è progressivamente evoluto nel corso degli anni, al punto che si annoverano ulteriori tecniche con cui propagare l'attacco in rete sempre più sofisticate, come l'utilizzo di software malevoli *malware*, *trojan* o *spyware*. Il *phishing* perpetrato mediante *malware* comporta l'esecuzione di un *software* malevolo sul computer dell'utente, che può essere diffuso sfruttando *bug* del sistema di sicurezza ovvero utilizzando tecniche di ingegneria sociale. Un'ulteriore specializzazione del *phishing* può essere considerato l'attacco mirato definito "*whaling*"[48], che si sostanzia in un attacco in cui il *phisher*, fingendosi dirigente di un'azienda, istituisce un contatto con un dipendente della stessa, al fine di indurre tale soggetto ad effettuare un pagamento a suo favore.

Gli attacchi di questo genere sono una *res* in crescita, tale da non consentire una disciplina giuridica *ad hoc* che consideri unitariamente il fenomeno in questione, esistendo, *a contrario*, diverse norme giuridiche nelle quali sussumere le fasi che lo caratterizzano.

Secondo parte della dottrina, i *phishing attacks* sono composti da sei fasi distinte: la prima fase è chiamata "*planning*", in cui il *phisher* individua il soggetto vittima da colpire, cosa rubare, le tecniche da utilizzare, nonché gli obiettivi da perseguire tramite detto attacco; la seconda fase è quella di "*setup*", in cui il soggetto attaccante si adopera per predisporre e creare gli strumenti e i meccanismi, occorrenti all'attacco da sferrare, procacciandosi poi i contatti e le informazioni delle potenziali vittime; inizia così la terza fase che è quella di dell'attacco vero e

[48] Cfr. Rapporto CLUSIT 2020: gli attacchi mirati vengono definiti *spear phishing*, vale a dire attacchi mirati nei confronti di strutture apicali di istituzioni pubbliche o privati.

proprio, detta appunto "*attack"*, in cui l'attaccante instaura un contatto con la vittima, mediante *e-mail, chat, website, malware*: tale fase è finalizzata a indurre la vittima a porre in essere operazioni che sono volte all'acquisizione delle informazioni personali riservate, quali le credenziali, che lo collega alla quarta fase, vale a dire quella della "*collection*", in cui l'attaccante sottrae le credenziali delle vittime per mezzo di *e-mail*, *web form,* telefono con cui si chiede al soggetto attaccato di inserirle materialmente; la quinta fase è quella della "*fraud*", in cui il *phisher* utilizza direttamente le informazioni raccolte o le credenziali per acquistare beni, rubare denaro dal conto *online* della vittima accedendovi fraudolentemente, operare un furto di identità, riciclare denaro ovvero le commercia o vende per ulteriori scopi illeciti, realizzando un profitto; la sesta ed ultima fase è quella del "*post attack*", in cui l'attaccante, una volta raggiunto i propri scopi fraudolenti, disattiva i meccanismi, copre le tracce, controlla le reazioni dei soggetti e il successo dell'attacco, che serve a programmarne di nuovi[49].

Nell'ordinamento italiano sussistono diverse fattispecie giuridiche nel cui alveo è possibile ricondurre le diverse condotte di *phishing*, poste in essere per compiere le singole fasi. Per quanto concerne le prime fasi, la formazione della falsa *e-mail* e l'invio della stessa, con cui il *phisher* si attribuisce un falso nome o un falso stato ovvero falsa qualità, potrebbe integrare la fattispecie di sostituzione di persona di cui all'art. 494 c.p., in quanto l'attaccante così facendo tenta di indurre in errore le vittime prescelte, per sottrarre loro informazioni rilevanti, procurandosi così un vantaggio con altrui danno. La Corte di Cassazione ha riconosciuto la configurabilità di tale delitto anche qualora perpetrato in Rete, integrando la condotta colui che utilizzi un account di posta elettronica attribuendosi i dati di un soggetto terzo, inducendo in errore gli "utenti della rete", arrecando un danno allo stesso[50]. A ben vedere però, tale fattispecie criminosa risulta configurabile solo ove il *phisher* si attribuisca gli estremi identificativi di una persona reale. Ciò è dovuto al fatto che il delitto di cui all'art. 494 c.p. si configura solo in riferimento alla sostituzione di persona fisica, come nel caso in cui la *mail* contenga dei riferimenti alla persona fisica come la firma in calce, per cui qualora la stessa sia, *a contrario,*

[49] CAJANI, COSTABILE, MAZZARACO, *Phishing e furto d'identità digitale: indagini informatiche e sicurezza bancaria*, Milano, 2008, 15 s.

[50] Cfr. Cass. pen., Sez. V, 14.12.2007, n. 46674, in *www.pluris-cedam.utetgiuridica.it.*

caratterizzata dalla presenza di segni distintivi di un ente non è possibile integrare simile delitto. Non risulta configurabile il delitto nell'ipotesi in cui i dati forniti dalle vittime, *ergo* i profili identitari delle vittime, vengano utilizzati su siti *web*, non risultando integrato l'elemento oggettivo del reato, poiché l'attaccante non si attribuisce in tal guisa un falso nome, un falso stato o una falsa qualità, non realizzandosi una materiale sostituzione di persona in quanto le credenziali non permettono di identificare il soggetto persona fisica, potendosi così integrare al più un accesso abusivo a sistema informatico, ai sensi dell'art. 615-*ter* c.p.; in più non vi è l'induzione in errore, che non risulta compatibile con l'esecuzione automatizzata delle richieste da parte del sistema informatico, che esegue le istruzioni impartite dal fruitore del sistema, equiparabile al soggetto legittimato proprio per l'utilizzo delle credenziali identitarie[51].

Qualora la condotta volta a procacciare informazioni sia posta in essere mediante la diffusione di un *malware*, da collocare all'interno del sistema vittima, potrà ritenersi astrattamente sussistente la fattispecie di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, di cui all'art. 615-*quinquies* c.p.: il programma in questione ha lo scopo di carpire automaticamente le informazioni del soggetto, alterando così il funzionamento del sistema informatico, che integrerebbe la fattispecie[52]. Si tratta di un reato di pericolo, volto a salvaguardare l'integrità dei sistemi informatici dalle condotte pericolose di diffusione di programmi *virus*, che potrebbero ledere il bene protetto.

Il messaggio di posta elettronica che l'utente riceve solitamente contiene un *link* che collega ad una pagina *web* di un sito fittizio, apparentemente identico nella grafica e nei contenuti al sito reale, che viene approntato dal *phisher* per ingannarlo. Il sito clone suscita nella vittima una falsa rappresentazione della realtà, che lo induce ad agire, effettuando l'accesso al sito con le proprie credenziali, compiendo poi un atto di disposizione patrimoniale, che determina una depauperazione del patrimonio: in tal modo l'attaccante si appropria dei dati dell'utente, ottenendo un ingiusto profitto. Questo è lo schema tipico della truffa comune di cui all'art. 640 c.p., che nella condotta descritta sarebbe astrattamente

[51] FLOR, *Phishing, identity theft e identity abuse*, cit., 909.
[52] CAJANI, COSTABILE, MAZZARACO, *Phishing e furto d'identità digitale*, cit., 119.

configurabile. La condotta del *phisher* fa credere al soggetto di interagire con un ente di fiducia mediante l'invio di una *mail* contenente i dati di quell'ente e un messaggio che lo induce ad agire fornendo i propri dati personali relativi all'accesso a determinati servizi e ciò integra l'elemento modale del delitto *de quo* costituito dagli "artifici e raggiri", da cui scaturirà l'evento. Gli artifici e raggiri si ritengono posti in essere da chi utilizza le caratteristiche proprie dell'ente esistente.[53] In tal modo la vittima indotta in errore realizzerà l'atto di disposizione patrimoniale per effetto degli artici e raggiri, da cui avrà luogo l'ingiusto profitto per l'attaccante e il conseguente danno patrimoniale per la medesima che subisce una *deminutio patrimonii*. Si tratta di un delitto a necessaria cooperazione della vittima, la cui disposizione patrimoniale è essenziale ai fini della realizzazione del profitto ingiusto con altrui danno, eventi consumativi del reato.

Secondo parte della dottrina il delitto in questione non trova spazio qualora il *phisher* acceda autonomamente ai servizi finanziari della vittima, eseguendo operazioni finanziarie a suo favore, in quanto difetterebbe il requisito dell'atto di disposizione patrimoniale effettuato dalla vittima, requisito implicito ma essenziale della disposizione[54]. Diversamente vi è chi ritiene che alla configurazione del delitto non osti il fatto che l'atto di disposizione patrimoniale sia posto in essere autonomamente dal reo e non dalla vittima, in quanto la norma di cui all'art. 640 c.p. dispone che il soggetto agente debba procurare a sé o ad altri un ingiusto profitto, a nulla rilevando che la condotta di disposizione patrimoniale sia posta in essere dallo stesso *phisher*[55]. Il reato di truffa comune di cui all'art. 640 c.p. potrebbe concorrere con il reato di cui all'art. 494 c.p., in quanto le due norme tutelano due beni giuridici eterogenei e in aggiunta la sostituzione di persona non costituisce un elemento costitutivo della truffa comune[56].

Nella condotta del *phisher* che si procuri i dati idonei all'accesso ad un sistema protetto da misure di sicurezza potrebbero astrattamente ravvisarsi gli estremi del delitto di "detenzione abusiva di codici di accesso a sistemi informatici"

---

[53] Cfr. nota a sentenza di AGNINO, Computer crime *e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*, in *Corr. merito*, 3/2009, 290.

[54] Sul punto FLOR, *Phishing, identity theft e identity abuse*, cit., 916.

[55] Trib. Milano 19.10.2008, in *Corr. merito*, 3/2009, 285 ss., con nota di Agnino, *Computer crime e fattispecie penali tradizionali: quando il phishing integra il delitto di truffa*.

[56] Trib. Milano 19.10.2008, in *Corr. merito*, cit., 288.

di cui all'art. 615-*quater* c.p., qualora la condotta stessa sia sorretta dall'elemento soggettivo idoneo ad integrare la fattispecie di reato, vale a dire dal dolo specifico di procurare a sé od altri un ingiusto profitto o di arrecare un danno ad altri. Dopo aver carpito fraudolentemente i dati della vittima, il reo è abilitato all'accesso ai servizi online: accedendo all'*account* della vittima abusivamente, senza diritto, eludendo così le misure di protezione, come l'autenticazione, poste per tutelare il diritto del soggetto all'accesso esclusivo, si realizza un accesso abusivo in un sistema informatico o telematico, di cui all'art. 615-*ter* c.p. L'acquisizione delle credenziali con il successivo utilizzo per l'accesso abusivo comporterà la sola applicazione dell'art. 615-*ter*, norma più grave che tutela il medesimo oggetto giuridico, rendendo la precedente condotta di detenzione abusiva un antefatto non punibile[57]. Si ritiene configurabile il concorso tra la truffa comune di cui all'art. 640 c.p., che si consuma con il conseguimento dell'ingiusto profitto e altrui danno, e l'accesso abusivo a sistema informatico o telematico di cui all'art. 615-*ter* c.p., vista l'eterogeneità dei beni tutelati.

La condotta del *phisher* potrebbe altresì configurare il delitto di frode informatica di cui all'art. 640-*ter* c.p., qualora posto in essere mediante le condotte tipiche di alterazione del funzionamento del sistema informatico o telematico ovvero di intervento senza diritto su dati, informazioni o programmi contenuti nello stesso, che determina l'ingiusto profitto con altrui danno.

Il reato di frode informatica si differenzia dalla truffa comune in quanto non si richiede che il reo operi mediante artifici o raggiri e non si richiede l'induzione in errore della vittima: la condotta fraudolenta è volta a manipolare il sistema informatico o telematico e ad esso si rivolge. Potrebbe integrare il delitto la condotta del soggetto agente che acceda abusivamente all'*account* relativo a servizi finanziari o bancari *online* della vittima, intervenendo nel sistema informatico senza diritto, ed effettui operazioni finanziarie di trasferimento illecite, che dipendono da un elaboratore tramite un'operazione automatica[58]. Il disvalore della condotta è

[57] In argomento PECORELLA, *Diritto penale dell'informatica*, Ristampa con aggiornamento, Padova, 2006, 374.

[58] Cfr. SCARCELLA, *Il* phishing *è punibile come frode informatica*, in commento alla sentenza Cass. pen., Sez. II, 24.10.2018, n. 48553, *in Quot. Giur*., 13 novembre 2018*;* in tal senso anche Cass. pen., Sez. II, 13.10.2015 n. 50140, che ha statuito che «[...] l'abusivo utilizzo di codici

peraltro accresciuto qualora il fatto sia commesso con furto o indebito utilizzo dell'identità digitale, rendendola meritevole di una sanzione più elevata.

Sembrerebbe escludersi il concorso tra la truffa *ex* art. 640 c.p. e la frode informatica *ex* art. 640-*ter* c.p. Si ritiene sia ammissibile, invece, il concorso tra la fattispecie di accesso abusivo a sistema informatico o telematico e frode informatica, data la diversità che sussiste tra le stesse che attiene agli elementi costitutivi e ai beni giuridici tutelati dalle rispettive norme[59]: l'una richiede quale elemento essenziale la presenza di un sistema informatico o telematico dotato di misure di protezione ed è volta a tutelare il domicilio informatico e in senso più ampio lo *jus excludendi alios*; l'altra richiede ai fini della consumazione la manipolazione del sistema, non richiesta per l'accesso abusivo e intende tutelare l'integrità del patrimonio e secondo parte della dottrina e della giurisprudenza anche il regolare funzionamento dei sistemi informatici e telematici e della riservatezza dei dati in esso gestiti, nonché la speditezza del traffico giuridico[60].

Con il tempo si sono sviluppate nuove modalità di attacco, definite "miste", che rendono partecipi soggetti terzi nell'azione criminosa. Fuori dai casi di concorso, nella condotta del soggetto terzo, reclutato dall'attaccante, c.d. *financial manager* o prestaconto, il quale mette a disposizione un conto corrente su cui il *phisher* possa trasferire il denaro e possa così ostacolarne la provenienza delittuosa, potrebbero astrattamente ravvisarsi gli estremi del delitto di riciclaggio di cui all'art. 648-*bis* c.p.[61]. È necessario, ai fini della sussistenza del delitto, che il *financial manager* si sia rappresentato la possibilità della fonte criminosa delle somme e ciononostante abbia agito ugualmente, previo corrispettivo. La consapevolezza da parte del soggetto prestaconto della fonte criminosa del denaro

informatici di terzi [...] è idoneo ad integrare la fattispecie di cui all'art. 640ter c.p. ove quei codici siano utilizzati per intervenire senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico, al fine di procurare a sé od altri un ingiusto profitto», *ivi*; diversamente in dottrina CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit., 120, ritiene che le condotte di cui all'art.640-*ter* siano insussistenti.

[59] Così CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit., 123; si veda inoltre Cass. pen., Sez. VI, 04.10.1999, n. 3067 in *Cass. pen.*, 11/2000, 2990 ss., con note di ATERNO e CUOMO.

[60] In tal senso ANTOLISEI, *Manuale di diritto penale. Parte speciale*, Vol. I, Milano, 2016, 499; NERI, *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, 97 s.; si veda anche Cass. pen., Sez. II, 15.04.2011, n. 17748, in *www.pluris-cedam.utetgiuridica.it.*

[61] In argomento DI PAOLO, Cyebr crime. *Il* phishing*: prospettive di un delitto*, in *Arch. Pen.*, 2/2017, 18 maggio 2017, 14 ss., in *Arch. pen. web*.

rappresenta il disvalore del delitto in questione. Il soggetto terzo si presta a ricevere le somme derivanti dalla condotta dal *phisher* e ne ostacola in tal modo la provenienza delittuosa, servendosi poi di società di *money transfer* per il trasferimento, che interrompe la traccia dei flussi monetari.

La stessa Corte di Cassazione ha affermato che la condotta del prestaconto volta ad ostacolare la provenienza delittuosa delle somme trasferite sul conto corrente predisposto *ad hoc*, a seguito di attacco *phishing*, integra il reato di cui all'art. 648-*bis* c.p.[62]. Qualora si sia limitato a ricevere dette somme, essendo consapevole della provenienza criminosa, senza poi trasferirle, potrebbe rispondere del delitto di ricettazione, *ex* art. 648 c.p. Si tratta di condotte che assicurano i proventi delittuosi e determinano la riuscita dell'attacco.

Dopo aver effettuato una disamina delle figure delittuose che astrattamente rilevano, è importante precisare che l'uso di metodologie sempre più ingegnose e artificiose permette di considerare il *phishing* un fenomeno perennemente nuovo e in continua evoluzione, venendone così in rilievo diverse tipologie, tra cui il "*vishing*", lo "*smishing*" e il "*twishing*".

Il termine *vishing* deriva dalla crasi tra il *VoIP* (*Voice over Internet Protocol*) ed il *phishing*. Definito anche *phishing* vocale, il *vishing* è un tipo di attacco che sfrutta la sensibilità del destinatario, il quale riceve comunicazioni che simulano avvisi urgenti spesso inerenti al proprio conto corrente da parte di un istituto di fiducia, che segnala le problematiche più variegate e lo invita a comporre un determinato numero telefonico ai fini della risoluzione degli stessi. Una volta composto il numero telefonico, l'utente ignaro contatterà un *call center*, in *prima facie* in grado di porre fine ai problemi prospettati, che lo indurrà a comunicare i propri dati, in particolare il numero del conto corrente o carta di credito[63]. Solitamente tale attacco si sostanzia in un sistema di chiamata automatico, volto a contattare diversi soggetti ed invitarli, con una registrazione vocale automatica, a comporre il numero di un dato *call center* e fornire informazioni inerenti al proprio

[62] V. DI VIZIO, Phishing*: le operazioni del prestaconto possono integrare il delitto di riciclaggio*, in *Quot. Giur. Web & Tech* Phishing, 27 marzo 2017, che richiama Cass. pen., Sez. II, 1.03.2017, n. 10060, in *www.pluris-cedam.utetgiuridica.it*.

[63] Sul punto TRUNFIO, CRISAFI, *Il phishing*, in CENDON (diretto da), *Trattato breve dei nuovi danni. Figure emergenti di responsabilità*, Vol. 3, Padova, 2014, 531 ss.

conto corrente, mediante inserimento dei dati personali. Tale meccanismo è svolto mediante l'attivazione di un *VoIP*, vale a dire una tecnologia che consente di avere un numero telefonico, in cui la voce viene veicolata tramite *Internet Protocol*, ossia un sistema di comunicazione sfruttato dalla rete internet[64].

Lo *smishing*, termine derivante dalla crasi tra le parole *Short Message Service* (*sms*) e *phishing*, è un attacco di tipo *phishing* che è volto a carpire informazioni personali, quali dati finanziari, tramite *sms*. Lo *smisher* invia un messaggio *sms* al soggetto vittima prescelto, nel quale lo induce a collegarsi a determinate piattaforme *web*, sulla base di presunte offerte vantaggiose, invitando così la vittima a fornire i propri dati personali[65].

Di recente si è sviluppata un'altra tecnica avente la medesima finalità, vale a dire quella di carpire i dati sensibili degli utenti malcapitati, che viene definita "*twishing*", crasi tra *Twitter* e *phishing*. Tale tipologia di attacco sfrutta un *social network*, mediante l'invio di un messaggio alla vittima, con cui lo si indirizza verso il *login* per l'accesso, previa registrazione, ad un sito *web*, permettendo al *twisher* di conoscere informazioni sensibili[66].

Tra i fattori di successo del *phishing* si annoverano le tecniche di *social engineering*, le falle nei sistemi di sicurezza, la transnazionalità e la dematerializzazione del denaro e dei rapporti, che garantiscono così l'anonimato[67]. Si ritiene che il modo migliore per evitare di restare vittime di tali attacchi è quello di effettuare controlli capillari prima di cliccare su *link* annessi ad ogni tipo di comunicazione, usare connessioni sicure ed evitare di condividere i propri dati sensibili. Si evince come questo sia un fenomeno sempre più sofisticato, lesivo di diversi beni giuridici, la cui continua evoluzione rende difficoltosa una repressione repentina e il cui contrasto dovrebbe basarsi non solo su misure a carattere normativo, ma principalmente sulla sensibilizzazione sociale, vale a dire su una buona cultura informatica e su un aggiornamento costante in merito alle tecniche di attacco maggiormente perpetrate.

---

[64] Cfr. PERRI, *Lo* smishing *e il* vishing*, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. Internet*, 3/2008, 266.

[65] V. TRUNFIO, CRISAFI, *Il phishing*, cit., 532.

[66] *Ivi*, 533.

[67] Sul punto D'AGOSTINI, D'ANGELO, VIOLINO, ATTANASIO, *Diritto Penale dell'Informatica: dai* Computer Crimes *alla* Digital Forensic, Forlì, 2007, 79.

2.4 Il *pharming*

Il *pharming* è un fenomeno volto ad acquisire illecitamente informazioni riservate. Costituisce un'evoluzione del *phishing*, con cui condivide l'obiettivo di acquisizione abusiva di dati sensibili, realizzato con un diverso *modus operandi*, che consta di una manipolazione del sistema DNS (*Domain Name System*).

Per comprendere tale tecnica di attacco, è importante soffermarsi sul funzionamento del servizio di rete, che permette ai cibernauti di navigarvi facilmente. Quando l'utente digita l'indirizzo alfanumerico di una pagina *web*, i *server* DNS traducono lo stesso in un indirizzo IP numerico, che permette il collegamento con il *server web* corrispondente a quel dominio. Il DNS può essere equiparato ad un *database* distribuito, contenente i nomi dominio delle pagine *web* e l'associazione ai relativi indirizzi IP. Esistono vari DNS nella catena di connessione, tra cui il "*resolver*" generalmente intermediario tra la rete *client* ed il *server* dei nomi DNS, e quello *dell'Internet Service Provider*, che opera quando nel DNS locale non risiedono le informazioni necessarie[68]. L'attaccante può scegliere di assumere il controllo di un qualsiasi DNS della catena di connessione, sia del DNS di un pc locale, sia del *server* DNS su larga scala dell'*Internet Service Provider*, da cui ricava l'indirizzo IP corrispondente al nome dominio digitato dall'utente e crea successivamente un sito clone, simile a quello reale, su cui dirotta la vittima, incidendo sul sistema. Nel caso in cui l'attaccante operi nei confronti dei server DNS *dell'Internet Service Provider*, questo va ad alterare gli abbinamenti tra il dominio e l'indirizzo IP: precisamente si va a modificare la corrispondenza numerica del dominio digitato dall'utente, compromettendo i *server* DNS che decodifica un indirizzo IP diverso da quello reale, che conduce la vittima al sito *web* del tutto simile a quello reale, creato *ad hoc* dal soggetto attaccante. Nel caso in cui, invece, il *pharmer* operi direttamente nei confronti del *personal computer* della vittima, egli attua una variazione al suo interno dei *file hosts*[69] ovvero del

[68] Cfr. LOMBARDO, Pharming*: cos'è, come funziona e i consigli per difendersi dalla truffa dei "siti-trappola"*, 28 gennaio 2020, in *www.cybersecurity360.it.*

[69] I file *hosts* possono essere qualificati come un elenco di indirizzi alfanumerici risolti in indirizzi IP, i quali sono memorizzati sul computer locale ed utilizzati dal *personal computer* per gli accessi successivi, senza dover interrogare i *server* DNS per effettuare il collegamento. Questo

registro di sistema dei DNS predefiniti, mediante l'ausilio di programmi *trojan* o attraverso ulteriori modalità di accesso, sfruttando le vulnerabilità del sistema[70]. L'utente difficilmente si renderà conto dell'attacco, dato che avrà digitato un indirizzo URL corretto nel proprio *browser*. L'attaccante con il *pharming* punta quindi a reindirizzare l'utente inconsapevole verso un *server web* clone allestito appositamente, lasciando credere allo stesso di navigare sul sito corretto di modo che effettui l'accesso per carpirne le informazioni, che è necessario ai fini della concretizzazione dell'attacco.

Come il *phishing*, il *pharming* può essere inquadrato tra gli attacchi complessi, in quanto l'*iter criminis* consta di svariate azioni, commesse in tempi diversi. Il *pharmer* compie un'alterazione del funzionamento dei sistemi informatici o telematici, dato che agisce abusivamente sul sistema DNS, integrando astrattamente la fattispecie di frode informatica, di cui all'art. 640-*ter*, il cui evento è costituito dal rilascio delle informazioni personali da parte della vittima ignara. La successiva condotta di accesso all'*account* dell'utente può configurare la fattispecie di accesso abusivo a sistema informatico o telematico, di cui all'art. 615-*ter*.

Il *pharming* è un tipo di attacco maggiormente pericoloso e raffinato rispetto al *phishing*, in quanto non occorre adescare l'utente mediante *e-mail* provenienti da istituti apparentemente reali per indurlo a connettersi a siti fittizi ed inoltre il computer della vittima non viene generalmente intaccato e la prova delle azioni commesse può essere facilmente occultata ripristinando le tabelle di DNS[71]. Proprio per queste sue caratteristiche esso può essere considerato un fenomeno in crescita. La diffusione di tale tipologia di attacco scaturisce anche dal fatto che vengono utilizzate, per la sua realizzazione, tecniche di *rootkit*[72], ossia un tipo di *malware*

indica che una modifica dei file archiviati può reindirizzare il traffico di rete verso un sito web clone: vd. LOMBARDO, Pharming, cit., *www.cybersecurity360.it*

[70] Così DEL NINNO, *Il furto di identità*, in CENDON (diretto da), *Trattato breve dei nuovi danni. Figure emergenti di responsabilità*, Vol. 3, Padova, 2014, 545.

[71] Sul punto CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit., 39.

[72] I *rootkit* «sono dei kit, ovvero strumenti o insiemi di strumenti, come sequenze di macro o veri e propri software, atti ad ottenere sul computer bersaglio i permessi di *root*, senza ovviamente che il proprietario del sistema oggetto dell'attacco ne sia a conoscenza. [...] *root* è l'utente con pieni poteri sul sistema , quindi può compiere qualunque operazione»: da LEANDRO, Rootkit*: cosa sono, come individuarli e come rimuoverli*, in *www.cybersecurity360.it,* 10 luglio 2019.

che consente di controllare a distanza un personal computer, facilitando così l'azione del *pharmer* che può manipolare il sistema dei *server* DNS.

3. La criminalità informatica: rilievi introduttivi

Lo sviluppo delle Tecnologie dell'Informazione e della Comunicazione ha determinato un cambiamento epocale nel sistema delle comunicazioni e delle relazioni interpersonali, il che ha favorito l'evoluzione di una nuova realtà delinquenziale. Si è passati da una dimensione "privata" del *personal computer* ad una dimensione "pubblica" dei sistemi, sorta con l'avvento di Internet, quale "Rete delle reti". Questo è stato concepito negli anni Sessanta del secolo scorso a scopi difensivi in ambito statunitense[73] e successivamente ha abbandonato tali finalità, imponendosi come mezzo di comunicazione di massa con l'estensione dell'accesso alla rete a qualsiasi utente, che ha permesso la creazione di un ambiente virtuale in cui si producono e diffondono contenuti, si svolgono interazioni umane e si facilitano le operazioni quotidiane.

Accanto agli aspetti positivi dati dalla rivoluzione cibernetica appena citati nonché, tra gli altri, la possibilità di creare svariate forme di aggregazione, condivisione e comunicazione che generano un rilevante impatto sui rapporti sociali, economici e culturali, scaturiscono altresì aspetti negativi, generandosi nuove forme di aggressione a beni giuridici inediti da affiancare a quelli tradizionali. La criminalità si è infatti adattata ai mutamenti storici, dando luogo ad una vera e propria rivoluzione del crimine, che trova terreno fertile in una realtà come il *cyberspace*, dotato di caratteristiche peculiari quali la dematerializzazione delle risorse, l'aterritorialità, l'atemporalità e l'anonimato.

Tale rivoluzione incide sul diritto vigente, fino a toccare talvolta il nucleo principale, sottoponendolo ad un adeguamento costante, affinché possa continuare ad operare con la propria capacità regolatrice. Nasce, dunque, una nuova frontiera

[73] «La storia di I. ha inizio con quella dell'ente che più di ogni altro ha contribuito alla sua nascita: l'ARPA (*Advanced Research Project Agency*), creata nel 1957 (ha cambiato nome nel 1971, premettendo il termine *Defense*, e diventando così la DARPA) dal dipartimento della Difesa statunitense per finanziare i progetti di ricerca suscettibili di applicazioni militari. Qui nel 1967 L. Roberts, del *Massachusetts Institute of Technology*, pubblicò un piano per *ARPANet*, una rete per l'interconnessione e l'interlavoro di calcolatori di tipo diverso, distribuiti su distanze geografiche anche considerevoli». Voce "*Internet*", in *Enc. onl. Treccani*, in *www.treccani.it*.

della criminalità, la criminalità informatica, la cui espressione – sebbene non rientrante in una categoria giuridicamente definita – indica l'insieme delle condotte antigiuridiche legate all'utilizzo delle nuove forme di tecnologia[74], che minacciano gravemente i diritti di persone e gruppi, che necessitano di adeguata protezione giuridica.

I primi riferimenti alla pirateria informatica sono avvenuti al "*Massachusetts Institute of Technology*" di Cambridge (c.d. M.I.T.) alla fine degli anni Cinquanta, quando iniziava a radicarsi, tra docenti e studenti interessati al mondo dell'informatica, il fenomeno dell'*hacking*, che aveva l'obiettivo di elevare il livello di conoscenze scientifiche[75]. Gli *hacker* accademici si identificavano in soggetti che si rapportavano con gli elaboratori elettronici al fine di superare i limiti imposti dagli stessi, per dimostrare capacità tecnica e innovazione, ed il cui lavoro si basava sulla sperimentazione pratica. Questi violavano i sistemi informatici per verificarne la sicurezza, senza però alterare il funzionamento degli stessi, eccettuata la modifica necessaria delle informazioni per consentire gli accessi. L'etica degli *hacker* si fondava sull'assunto che l'accesso ai computer dovesse essere libero ed illimitato, così come l'accesso a tutte le informazioni, fonte di insegnamento[76]. Il termine ha successivamente acquisito una valenza negativa con la diffusione di Internet, quando le tecniche di *hacking* hanno iniziato ad essere usate per scopi criminosi, come quello di danneggiare, sabotare ovvero alterare il funzionamento del sistema informatico o telematico. Oggi le tecniche di *hacking* sono alquanto variegate e sofisticate: esse si sostanziano in tutti quegli attacchi, precedentemente analizzati (vedi *supra* Cap. I § 2 e ss.), idonei a riportare danni gravi non solo ai singoli, ma all'intera comunità virtuale. Le capacità di contrastare tali fenomeni sono complesse, vista la capacità dei soggetti agenti di eliminare le proprie tracce, nonché cambiare identità.

Le prime manifestazioni di criminalità informatica moderna si annoverano all'inizio degli anni Settanta, riconducibili a quelle condotte antigiuridiche, definite *computer crimes*, poste in essere mediante abuso degli elaboratori. I *computer*

[74] Così BALLONI, BISI, SETTE, *Principi di criminologia applicata. Criminalità, controllo, sicurezza*, Padova, 2015, 254.

[75] Sul punto CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 10 s.

[76] Cfr. LEVY, Hackers*: Gli eroi della rivoluzione informatica*, Milano, 1996.

crimes si riferiscono a condotte aventi ad oggetto un sistema informatico o telematico connesso solo eventualmente in reti telematiche ristrette o comunque parte di un sistema di rete più articolato, ma non aperto al pubblico[77]. Sovente si fa riferimento ad essi come "*computer-related crime*", per indicare che il *computer* è lo strumento usato dal criminale per commettere il reato.

L'accesso pubblico alla Rete ha permesso l'incremento degli utenti, i quali hanno sfruttato le potenzialità della stessa e le sue funzioni – tra cui l'utilizzo ai fini commerciali, come sistema comunicativo e di diffusione dei dati – che sono state adoperate per la commissione di diversi tipi di illeciti. Negli anni Novanta, con l'apertura di Internet al pubblico, si è infatti passati da un concetto di criminalità informatica legato alla lesione del sistema informatico ad uno più ampio, comprensivo di condotte delittuose che non possono prescindere dalla connessione in Rete ai fini della loro commissione, riferendosi a qualsiasi condotta criminale che ha a che fare con la rete e i *computer*: questi illeciti sono riconducibili al concetto di *cybercrime.*

Si può operare una classificazione sistematica degli illeciti riconducibili a fattispecie criminose perpetrabili nel *cyberspace*, che prende le mosse dai reati informatici c.d. "in senso stretto" per estendersi ad altre nozioni di più ampio raggio. I reati informatici in senso stretto comprendono tutte quelle fattispecie legali costruite, sul piano della formulazione, con elementi di tipizzazione legati a procedimenti automatizzati di dati e informazioni o comunque attività ovvero modalità di operazione avente carattere tecnologico[78], vale a dire tutte quelle fattispecie che contengono un elemento che rievoca le Tecnologie dell'Informazione e della Comunicazione, il quale deve essere necessariamente integrato ai fini della sussistenza della stessa.

Diversamente sono riconducibili ai reati informatici c.d. "in senso ampio" tutte quelle fattispecie che possono essere commesse anche mediante strumenti informatici ovvero con modalità di azione che ricadono su oggetti tecnologici. In tal caso la formulazione della fattispecie non sempre contiene riferimenti alle TIC, ma sono ricavabili riferimenti in via ermeneutica.

---

[77] V. PICOTTI, *Diritto penale e tecnologie informatiche*, cit., 47.

[78] In argomento FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet,* in *Dir. pen. cont.*, 20 settembre 2012, 4.

Altre volte gli elementi di tipizzazione tipici dei reati informatici sono presenti nella fattispecie come possibile modalità di condotta o oggetto della stessa[79]. Ci si riferisce, pertanto, a tutte quelle fattispecie "comuni" che, pur non facendo espresso riferimento a tali elementi caratterizzanti, possono essere applicate a quelle condotte commesse nel *cyberspace* o per mezzo della tecnologia. Si tratta di una categoria soggetta ad ampliamento, date le numerose condotte che oggi possono essere commesse via *web*.

Come anticipato, si è progressivamente passati, nel corso degli anni, dai *computer crimes* ai *cybercrimes*, ossia quei reati che si commettono ovvero si possono commettere in rete, nel *cyberspace*. Anche in questa categoria si possono distinguere i reati cibernetici "in senso stretto" ed i reati cibernetici "in senso ampio": nei primi l'elemento specializzante è costituito dalla commissione del fatto in rete o della fruibilità del *cyberspace*, che è essenziale ai fini della configurabilità della fattispecie, per cui è un requisito espressamente previsto dal legislatore; nei reati cibernetici in senso lato, l'esplicito riferimento alla rete compare solo in via eventuale, per cui è possibile ricondurre il fatto a tale categoria anche in via interpretativa, dato che sono formulati in termini elastici che ne permettono la realizzazione in concreto in rete e sono concepibili anche a prescindere dalla stessa. I reati cibernetici "in senso stretto" sono anche reati informatici "in senso stretto", in quanto la commissione in rete del fatto comporta necessariamente un riferimento espresso alle TIC. Per converso non tutti i reati informatici "in senso stretto" sono parimenti reati cibernetici "in senso stretto", visto che non si richiede obbligatoriamente per i primi che il fatto sia commesso in rete, ben potendo il requisito caratterizzante – le TIC – non necessitare della commissione in rete del fatto[80].

I reati informatici e i reati cibernetici differiscono rispetto a quelli tradizionali non solo per il modo in cui sono realizzati, il che consente all'attaccante di eliminare ogni traccia del suo comportamento deviante tale da rendere difficoltoso l'accertamento del fatto, ma anche per la percezione che la dinamica criminosa prospetta nel singolo. In questo senso, le tecnologie influenzano l'*iter*

[79] Sul punto PICOTTI, *Diritto penale e tecnologie informatiche*, cit., 76.
[80] *Ivi*, 78.

criminoso, conferendo sicurezza al reo per il presunto anonimato della rete, nonché per la bassa percezione del rischio che la condotta posta in essere venga scoperta e sanzionata, rafforzando l'idea di impunità, così da sfumare i confini tra ciò che è percepito come lecito e ciò che invece è illecito[81].

Proprio per le caratteristiche tipiche della realtà informatica, la criminalità nel *cyberspace* non può essere circoscritta ad un limitato numero di reati, dato che ricomprende un'ampia categoria di illeciti, con *modus operandi* sempre nuovi in grado di offendere i diritti altrui. Alla espansione delle modalità con cui vengono perpetrati gli illeciti corrisponde una diversificazione e ampliamento dei beni giuridici meritevoli di tutela penale.

La pirateria informatica lede beni giuridici diversi, come il patrimonio, la fede pubblica, l'ordine pubblico, il domicilio, la riservatezza dei dati e informazioni, colpendo i settori più disparati[82]. Tra questi si nota come alcuni possano essere annoverati a "nuovi" beni giuridici, poiché inesistenti prima dell'avvento dell'informatica, basti pensare alla riservatezza informatica, la quale è da intendersi come diritto della persona ad uno spazio esclusivo, in cui esplicare la propria personalità, che deve essere lasciato libero da intrusioni illegittime di terzi; ancora va richiamato lo specifico diritto alla tutela dei dati personali in rete, che necessitano di adeguate discipline di tutela che ne permettano il controllo da parte dell'utente cui si riferiscono, nonché la contrapposta esigenza di accessibilità a soggetti terzi, a condizioni determinate; altro bene giuridico "nuovo" che esige tutela contro eventuali attacchi configurabili nello spazio cibernetico è la sicurezza informatica, strumentale alla protezione dei diritti precedentemente citati, che svolge una funzione di tutela preventiva rispetto agli altri che vengono in considerazione[83]. Richiedono opportuna protezione anche i beni giuridici tradizionali, oggetto di aggressioni sempre nuove, maggiormente penetranti qualora commesse in rete.

Da questo breve esame emerge un'evoluzione del diritto penale dell'informatica, cui è devoluta la tutela di beni giuridici considerati essenziali, che

[81] Così BALLONI, BISI, SETTE, *Principi di criminologia applicata*, cit., 271 s.
[82] Sul punto CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 3.
[83] In argomento PICOTTI, *Diritto penale e tecnologie informatiche*, cit., 52 s.

si rinviene non solo nel codice penale, ma anche nella legislazione speciale e che sono caratterizzati da indubbie peculiarità, riflettendo così la diversa struttura che assumono le interazioni nel *cyberspace*.

Con l'avvento della criminalità informatica, il concetto di azione penalmente rilevante muta il suo significato nella realtà virtuale, dato che non è più intesa come un'azione di un soggetto dagli effetti tangibili nella realtà materiale esterna, ma si esprime in forme di trasmissione, immissione e gestione di dati a mezzo di impulsi elettronici. Il soggetto agente interagisce con il sistema per cui ogni suo gesto corrisponde ad un impulso elettronico, che fa compiere al *computer* una serie di operazioni. La condotta si rivolge infatti a strumenti tecnologici automatizzati e viene realizzata mediante una connessione tra sistemi distanti tra loro, per cui accade che gli effetti di una condotta si esplichino in un luogo diverso rispetto a quello in cui la stessa è stata compiuta. Il reo con il proprio comportamento deviante sembrerebbe in grado di produrre conseguenze dannose simultaneamente ed in luoghi differenti e ciò rende più ostico l'accertamento della responsabilità. È importante considerare che la possibilità di produrre eventi avversi in luoghi disparati – anche lontano dal luogo in cui si è posta in essere la condotta – rende complessa l'individuazione dell'autorità giudiziaria territorialmente competente ai fini dell'accertamento dell'illecito[84].

Gli oggetti su cui tali azioni ricadono sono il sistema informatico ovvero il sistema telematico. Il primo allude ad una nozione di computer molto ampia per evitare vuoti di tutela e la cui definizione è stata fornita dall'art. 1 della Convenzione di Budapest, che lo individua in «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dei dati»[85]. Essenziale è che il sistema informatico sia in grado di elaborare un numero consistete di dati in formato digitale e sia in grado di elaborare automaticamente le informazioni per mezzo di elaboratori. Il sistema informatico è composto da *hardware* e *software*: con il primo termine si richiama la struttura fisica del sistema, ossia le componenti materiali

[84] Sul punto AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, Padova, 2010, 15 s.

[85] V. CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 4 ss.

come l'unità centrale; con il secondo si rinvia ai programmi di base, vale a dire le componenti logiche del sistema.

Per sistema telematico, invece, si intende un complesso organico idoneo alla elaborazione e trasmissione a distanza di dati e di informazioni, mediante l'impiego di tecnologie legate alle telecomunicazioni[86].

I reati informatici sono generalmente reati comuni, per cui possono essere commessi da chiunque. Accade sovente che la complessità dell'azione da porre in essere per integrare la fattispecie richieda la competenza specifica del soggetto agente, per cui alcune fattispecie attribuiscono un maggiore disvalore al comportamento deviante qualora il soggetto rivesta determinate qualifiche o abbia particolari conoscenze tecniche. Tra questi spicca la qualifica di operatore di sistema, che si identifica in colui che è preposto alle operazioni di *input* ed *output*, di avvio e arresto del sistema, che scrittura le operazioni che il *computer* è tenuto ad effettuare, nonché nel soggetto che studia le evoluzioni del sistema ai fini dell'ottimizzazione dello stesso e che sviluppa algoritmi per soddisfare specifiche esigenze[87]. La qualifica viene attribuita non al soggetto che professionalmente si trovi ad interagire con il sistema informatico, ma anche a colui che di fatto si trovi ad intervenire sui dati o programmi dell'elaboratore, pertanto non si rende necessaria la relazione di proprietà con il sistema. Occorre considerare come tale soggetto si trovi in una posizione di vantaggio nel compimento dell'azione criminosa, dato che ha la possibilità di accedere ad aree riservate del sistema e controllare le operazioni che ivi vengono effettuate. Proprio per tale motivo il maggior disvalore si rinviene nel rapporto che sussiste tra il soggetto agente e il bene tutelato, il che giustificherebbe un più grave trattamento sanzionatorio.

Altro soggetto qualificato è il *provider* che è colui, persona fisica o ente collettivo, che permette ai terzi di accedere alla Rete. Generalmente le trasmissioni digitali all'interno delle reti telematiche non avvengono in modo diretto, dato che

[86] Per un'accurata analisi si veda CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 8, il quale statuisce che «il collegamento tra più sistemi informatici deve soddisfare alcuni requisiti essenziali: a) la connessione deve avere carattere stabile (attraverso canali di comunicazione televisivi, satellitari, telefonici, via etere) o permanente (LAN o rete collegata via cavo); b) lo scambio di informazioni e la connessione tra elaboratori distanti deve essere il mezzo necessario per conseguire le finalità operative del sistema».

[87] Così CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 21.

intervengono una serie di figure intermedie, *provider*, che si interpongono tra colui che immette l'informazione e l'utente finale, affinché i dati possano essere resi accessibili al pubblico. Senza entrare nel merito, si consideri solamente che il *provider* gestisce la rete su cui transitano le informazioni, per cui qualora si renda responsabile di comportamenti devianti, la sua condotta assume maggior disvalore proprio per la posizione privilegiata che lo stesso ricopre[88].

L'evoluzione continua delle minacce cibernetiche, sempre più sofisticate, ha portato ad interrogarsi sui problemi che pone la commissione del reato in Rete, i quali sono legati non solo all'inadeguatezza delle figure classiche di reato a ricomprendere le nuove modalità di aggressione criminosa, ma sono riconducibili anche alla difficoltà di accertamento del fatto, nonché di individuazione del responsabile[89]. La diffusione capillare del *cyberspace* ha infatti condotto a considerare in modo inedito finanche i concetti di spazio e azione penalmente rilevanti, tale da rendere inapplicabile in alcuni casi le regole tradizionali, per cui verrebbe in luce la necessità di un intervento del legislatore per reprimere determinate condotte criminose per mezzo del diritto penale.

4. Inquadramento normativo

La Rete non può oramai essere inquadrata come uno spazio franco dal diritto e ciò è reso evidente dalle nuove insidie che in esso si ravvisano, quali le nuove forme di aggressione che attentano ai diritti dei singoli e che richiedono protezione. Per un'efficace tutela di tali diritti sorge l'esigenza di sistemi armonizzati, per assicurare un'effettiva prevenzione e repressione, ove occorrente, di fatti criminosi perpetrati nel *cyberspace*. A tal fine si rende necessaria una delimitazione giuridica dei comportamenti illeciti nel cyberspazio, il cui criterio basilare è «ciò che è illecito *off line* non può essere lecito *on line,* anche se si presenta in nuove ed inimmaginate modalità e forme»[90].

La realtà giuridica deve aggiornarsi di pari passo al fenomeno della criminalità informatica, nonché prevenirlo affinché i beni giuridici non vengano

[88] V. AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 17 s.
[89] PECORELLA, *Diritto penale dell'informatica*, cit., 33 ss.
[90] V. PICOTTI, *Diritto penale e tecnologie informatiche*, cit., 42.

intaccati, mediante un quadro giuridico che si adatti ad esso, riscrivendo le regole generali e tenendo conto delle caratteristiche peculiari che le nozioni basilari assumono nel *cyberspace*. Si rileva, pertanto, l'esigenza di una regolazione e tutela giuridica.

La criminalità informatica non è una categoria giuridicamente definita, sebbene compaia in molteplici fonti europee. I primi riferimenti giuridici inerenti al fenomeno si rinvengono alla fine degli anni Settanta, quando il legislatore italiano è intervenuto in modo disomogeneo e casistico per reprimere forme di aggressione inedite verso beni giuridici protetti, mediante interventi sporadici, volti a contrastare specifici eventi, basta ricordare la legge del 18 maggio 1978, n. 191 introduttiva dell'art. 420 c.p., contro l'attentato ad impianti di elaborazione dati, o la legge 1 aprile 1981, n. 121 a garanzia e tutela dei dati archiviati in un sistema informatico ovvero normative più specifiche riguardanti l'antiriciclaggio di denaro, attraverso l'introduzione della legge n. 197 del 1991, con cui si puniva l'indebito utilizzo di carte di credito e l'introduzione della legge n. 518 del 1992, con cui si consentiva l'applicazione della disciplina a tutela del diritto d'autore al programma per elaboratore, essendo quest'ultimo equiparato alle opere per l'ingegno, così si incriminavano i reati di pirateria informatica al fine di garantire una più efficace tutela in ambito informatico[91]. Tali interventi si giustificarono a causa dell'obiettiva insuperabilità dei limiti imposti dal principio di tassatività, che richiamavano l'attenzione del legislatore sui primi avvenimenti rilevanti, riguardanti la criminalità informatica e che necessitavano di adeguato intervento legislativo, volto ad arginarli.

Dottrina e giurisprudenza tentavano di ricondurre, per limitare i vuoti di tutela, le nuove figure criminose a fattispecie tradizionali esistenti. Ciò era prospettabile con riferimento a condotte criminose perpetrate avverso le parti fisiche del sistema informatico – *hardware* – la cui condotta poteva astrattamente integrare le ipotesi classiche del danneggiamento o furto. Il problema si poneva in riferimento alle condotte di frode, attuata per il tramite dell'elaboratore, e le

[91] In argomento TESTAGUZZA, Digital forensic. *Informatica giuridica e processo penale*, Padova, 2014, 19.

condotte avverso dati e informazioni, nonché avverso le parti c.d. logiche del sistema[92].

Sempre più frequenti diventavano le truffe connesse all'elaborazione di dati avverso i sistemi bancari, che non integravano gli estremi del delitto di truffa di cui all'art. 640 c.p. per la mancanza di elementi costitutivi del reato, quali gli artifici o raggiri, non andando così ad indurre in errore il soggetto passivo, piuttosto si alterava il funzionamento dell'elaboratore. Problemi analoghi si ponevano per le condotte di accesso abusivo ad un sistema informatico, che si riteneva potessero essere assimilate – erroneamente – alla fattispecie di violazione di domicilio di cui all'art. 614 c.p., attuando un'analogia in *malam partem*, vietata. L'assenza di un presidio penalistico per condotte fino ad allora non conosciute ai più e in continua crescita faceva quindi sorgere la necessità di un'opportuna tutela, che consentisse di dare una risposta sanzionatoria adeguata ed evitasse vuoti di tutela.

Dalle più volte richiamate esigenze di protezione nacque un dibattito in merito ai *computer crimes*, che aveva ad oggetto, tra l'altro, il bisogno dei soggetti di servirsi delle nuove tecnologie per il soddisfacimento delle proprie esigenze, così come il diritto ad essere tutelati nell'esercitare tale libertà[93]. Il dibattito sorgeva dal fatto che si trattava di un campo nuovo in cui si potevano esplicare illeciti, che si portava con sé dilemmi di carattere sostanziale e processuale, che qualora non assistito da adeguata legislazione avrebbe condotto alla creazione di paradisi informatici.

Anche in ambito europeo si ravvisava la necessità di un quadro normativo armonizzato che permettesse di disciplinare un fenomeno sempre più diramato. Un primo contributo in tal senso è stato dato dall'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), che ha svolto uno studio sulla criminalità informatica a metà degli anni Ottanta. Dapprima nel 1983, l'organizzazione ha condotto uno studio sulla possibilità di applicare leggi penali a livello internazionale volte a contrastare i reati informatici, al fine di armonizzare la disciplina in materia. Successivamente nel 1986, l'OCSE ha pubblicato la relazione "*Computer-Related Crime: Analysis of Legal Policy*", in riferimento ai principali

[92] *Ivi*, 19.
[93] Sul punto FARINA, *Elementi di diritto dell'informatica*, Padova, 2019, 242.

orientamenti normativi dei Paesi partecipanti, analizzando la normativa esistente e le relative proposte di riforma, sottolineando l'importanza del diritto penale nel contrasto alla nuova criminalità[94]. Lo studio dell'OCSE ha rinunciato a fornire una definizione univoca del fenomeno, constatato che sarebbe stato difficile, nonché poco produttivo adottarne una comune che riscuotesse il consenso dei diversi paesi; piuttosto si considerava opportuno far riferimento ad una tipologia di abusi precisa, affinché vi fosse uno sviluppo uniforme in ambito europeo[95].

Il 13 settembre 1989 il Comitato dei Ministri del Consiglio d'Europa adotta la Raccomandazione "*sur la criminalitè en relation avec l'ordinateur*" n. R (89) 9, divenuta punto di riferimento internazionale. La Raccomandazione sulla criminalità informatica riconosce l'importanza di una risposta repentina ed adeguata al nuovo fenomeno criminoso, considerando il carattere transfrontaliero dello stesso. Essa non fornisce una definizione del fenomeno in questione, ma richiama l'attenzione dei legislatori coinvolti a far fronte allo stesso, visti i danni che la criminalità informatica è in grado di realizzare e l'incidenza della stessa sui rapporti economici e giuridici, nonché per offrire una tutela alle vulnerabilità dei sistemi informatici. Nella Raccomandazione le diverse condotte antisociali vengono ripartite in due gruppi – la lista "minima" e la lista "facoltativa" – a seconda che le condotte debbano essere represse in sede penale, invitando gli Stati ad intervenire finanche con interventi legislativi *ad hoc*, ovvero venga lasciata la scelta dello strumento punitivo alla discrezione dei singoli Stati, i quali possono intervenire anche con sanzioni di tipo amministrativo[96]. Rientrano nella c.d. lista minima tutte le condotte che, in virtù della loro gravità e diffusione, devono necessariamente essere represse, quali la frode informatica ossia «l'introduzione, alterazione, cancellazione o soppressione di dati o programmi o in qualsiasi altra ingerenza in un procedimento di elaborazione di dati che, influenzandone il risultato, cagioni ad altri un pregiudizio economico o materiale, al fine di procurare a sé o ad altri un ingiusto profitto»; il falso in documenti informatici, che si concretizza nella «introduzione,

[94] Così FLOR, Cyber-criminality*: le fonti internazionali ed europee*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Cybercrime*, Torino, 2019, 99.

[95] V. PECORELLA, *Diritto penale dell'informatica*., cit., 2.

[96] In argomento si veda PECORELLA, *Diritto penale dell'informatica*, cit., 7; NERI, *Criminologia e reati informatici*, cit., 33.

l'alterazione, la cancellazione o la soppressione di dati o programmi informatici o con qualsiasi altra ingerenza in un procedimento di elaborazione di dati, in maniera o in condizione tale che, in base al diritto nazionale, sarebbe integrato un reato di falso se l'azione avesse riguardato un oggetto tradizionale»; il danneggiamento di dati o programmi, realizzato con «la cancellazione, alterazione, deterioramento o soppressione senza diritto»; il sabotaggio informatico, che si sostanzia nella «introduzione, alterazione, cancellazione o soppressione di dati o programmi, ovvero nell'ingerenza in un sistema informatico, avendo l'intenzione di ostacolare il funzionamento di un sistema informatico o di un sistema di telecomunicazione»; l'accesso non autorizzato «ad un sistema informatico o ad una rete informatica, violando delle misure di sicurezza»; l'intercettazione non autorizzata «con l'impiego di mezzi tecnici, di comunicazioni destinate a, provenienti da, o nell'ambito di, un sistema o una rete informatici»; la riproduzione non autorizzata di un programma protetto, da intendersi anche come «diffusione o comunicazione al pubblico»; la riproduzione non autorizzata di una topografia «protetta dalla legge, di un prodotto a semiconduttori, ovvero allo sfruttamento commerciale o all'importazione a tal fine di una topografia o di un prodotto a semiconduttori, fabbricato usando quella topografia»[97]. La c.d. lista facoltativa ricomprende, invece, tutte quelle condotte da incriminare solo eventualmente con strumenti penali, lasciando così discrezionalità ai singoli Stati, a cui è consentito intervenire anche con tecniche sanzionatorie differenti. La ragione della presenza nella Raccomandazione del secondo gruppo di condotte è da ravvisarsi nel fatto che non è stato segnalato un consenso univoco sul tipo di tecnica sanzionatoria più adatto a reprimere tali comportamenti devianti, ma se ne raccomandava ugualmente l'incriminazione al fine di ottenere un sistema armonizzato. In tale lista rientrano l'alterazione di dati o di programmi informatici non autorizzata, quando la condotta non rientra nelle ipotesi di danneggiamento di dati e programmi; lo spionaggio informatico, che si sostanzia nel «conseguire attraverso mezzi illeciti ovvero nel divulgare, trasferire o utilizzare senza averne diritto e senza alcuna giusta causa un segreto commerciale o industriale, avendo l'intenzione di cagionare un pregiudizio economico al titolare del segreto o di ottenere per sé o per altri un ingiusto profitto»;

[97] Cfr. PECORELLA, *Diritto penale dell'informatica*, cit., 8.

l'utilizzazione non autorizzata di un elaboratore o di una rete informatica, qualora il soggetto «accetti un rischio non indifferente di cagionare un pregiudizio al legittimo utente del sistema o di danneggiare il sistema o il suo funzionamento, oppure abbia l'intenzione di cagionare un pregiudizio al legittimo utente del sistema o di danneggiare il sistema o il suo funzionamento, oppure cagioni di fatto un pregiudizio al legittimo utente del sistema o danneggi il sistema o il suo funzionamento»; l'utilizzazione non autorizzata di un programma informatico protetto, abusivamente riprodotto con l'intenzione di acquisire un profitto ingiusto per sé o per altri o di cagionare un pregiudizio al titolare dei diritti sul programma[98]. La raccomandazione invitava gli Stati ad adottare disposizione apposite per attuare un efficace contrasto del fenomeno, mediante interventi uniformi.

Tra gli interventi di rilievo va segnalata anche la Risoluzione finale approvata dal Congresso dell'AIDP – *Association Internationale de Droit Pénal* – nel 1994, la quale sollecita un ampliamento dei tipi di abuso dell'informatica meritevoli di sanzione. L'associazione ha posto tra i temi oggetto di studio, del XV Congresso, la criminalità informatica, suggerendo di rivalutare le indicazioni contenute nella Raccomandazione del Consiglio d'Europa alla luce delle nuove evoluzioni criminali. Non solo si ravvisava la necessità di reprimere con lo strumento penale, dato il diffuso consenso sorto nel corso degli anni, anche le condotte devianti contenute nella c.d. lista facoltativa, ma si riteneva necessario valutare la possibilità di ricorrere a tale tecnica sanzionatoria anche per la prevenzione di fatti colposi, considerazione non presente nella Raccomandazione[99]. Nel Congresso dell'AIDP si invitava a ricomprendere, tra le condotte penalmente rilevanti, anche il commercio di codici d'accesso e la diffusione di virus o programmi simili, per apprestare una protezione adeguata alle esigenze affiorate a causa degli attacchi perpetrati avverso i sistemi informatici. Tali indicazioni sono state poi accolte dal legislatore italiano con la legge del 23 dicembre 1993 n. 547.

Rilevante si rivela altresì la Raccomandazione (95) 13, approvata l'11 settembre 1995, in ambito procedurale, con cui il Consiglio d'Europa ha fornito una prima risposta ai crimini informatici commessi nell'ambito dell'*Information*

[98] *Ivi*, 8 s.
[99] *Ivi*, 10 s.

Technology (IT), considerando come tali sistemi possano essere usati per commettere reati; essa ha, inoltre, palesato la necessità di apprestare adeguate garanzie nella ricerca e raccolta delle prove elettroniche, sempre più importanti nel corso delle investigazioni aventi ad oggetto comportamenti devianti commessi nell'ambito delle IT; si suggerisce poi di predisporre specifici obblighi per i *service providers* affinché forniscano le misure necessarie per permettere l'intercettazione di comunicazioni e la possibilità di identificare gli utenti da parte delle autorità investigative[100].

Nel 1997 viene creato il Comitato di esperti sulla Criminalità nel Ciberspazio – *PC-CY*: *Committee of Experts on Crime in Cyberspace* – in seno al Consiglio d'Europa, a cui è stato assegnato il compito di stilare una bozza di convenzione internazionale, per combattere e reprimere la criminalità informatica nel nuovo spazio virtuale privo di confini territoriali e temporali, con l'obiettivo di facilitare la cooperazione in ambito internazionale nelle attività investigative e di accertamento di questi comportamenti antisociali, che richiedono una disciplina armonizzata date le peculiari caratteristiche[101]. Il mandato del Comitato consisteva, in particolare, nell'esaminare, alla luce delle recenti Raccomandazioni, le questioni riguardanti le infrazioni commesse nello spazio cibernetico, perpetrate attraverso reti di comunicazione e Internet; le questioni attinenti alla necessità di prevedere un sistema armonizzato in materia penale con riferimento alle definizioni, sanzioni e responsabilità delle parti interessate; la risoluzione dei problemi inerenti al ricorso di poteri coercitivi; le questioni riguardanti la competenza nei confronti di condotte criminose avvenute nel *cyberspace*, dato il carattere transnazionale degli illeciti che rende difficoltoso determinare il luogo in cui sono avvenuti e fa sorgere problemi inerenti alla risoluzione dei conflitti di competenza[102].

Il compito assegnato al Comitato è stato assolto quattro anni dopo, con l'adozione della Convenzione sulla criminalità informatica il 23 novembre 2001, che costituisce uno degli strumenti internazionali fondamentali nella lotta alla

[100] Sul punto FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 100 s.
[101] *Ivi*, 101.
[102] Per un approfondimento si veda SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale.* (3. Riv., corretta ampliata ed.), Milano, 2010, 587 ss.

criminalità informatica, elaborata anche con la partecipazione di Stati extraeuropei, quali Stati Uniti, Canada, Giappone e Sud Africa (v. *infra* § 4.2).

Assume rilievo altresì la Decisione Quadro 2005/222/GAI relativa agli attacchi contro i sistemi di informazione, con l'obiettivo di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti all'applicazione della legge degli Stati membri, mediante un ravvicinamento delle legislazioni, in suddetta materia, dati i crescenti attacchi ai danni di tali sistemi e il timore per la possibilità di realizzazione di attacchi terroristici avverso i sistemi di informazione facenti parte di una infrastruttura critica degli Stati membri. Tale Decisione disponeva agli stati membri di criminalizzare determinati comportamenti, come l'accesso illecito a sistemi di informazione; l'interferenza illecita per quanto riguarda i sistemi; l'interferenza illecita per quanto riguarda i dati; l'utilizzazione, il favoreggiamento nonché la complicità ed il tentativo; la responsabilità delle persone giuridiche. Si noti che, a differenza della Convenzione di Budapest, essa non si riferiva a tutti i reati commessi mediante le tecnologie informatiche, ma solamente agli attacchi informatici[103].

La Decisione Quadro 2005/222/GAI è stata sostituita dalla Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione. Tale direttiva stabilisce norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione, con l'obiettivo di prevenire la commissione di questi reati e incrementare la cooperazione tra le autorità giudiziarie e le autorità competenti dei Paesi membri. L'intervento della Direttiva si giustifica sull'assunto che il buon funzionamento e la sicurezza dei sistemi all'interno dell'Unione Europea siano fondamentali per lo sviluppo del mercato interno e di un'economia innovativa[104]. La Direttiva ripercorre la linea di intervento della sostituita Decisione quadro, salvo talune differenze che si rinvengono nell'obbligo per gli Stati di incriminare la condotta di intercettazione illecita di comunicazioni informatiche o telematiche e la previsione di una sanzione minima per le condotte di fabbricazione, vendita, uso,

[103] In argomento SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 627 s.

[104] Cfr. Considerando 2 della Direttiva 2013/40/UE.

messa a disposizione di *software* e *password,* al fine di commettere uno dei reati previsti dalla direttiva[105].

L'evoluzione normativa segue il passo della criminalità informatica, al fine di contrastarla mediante l'armonizzazione delle legislazioni nazionali e la cooperazione tra le autorità giudiziarie e competenti dei Paesi coinvolti.

4.1 La legge n. 547/1993

La sempre maggiore diffusione dell'informatizzazione ha determinato nuove esigenze di protezione, che consentissero di arginare e reprimere il fenomeno della criminalità informatica. Dopo i primi interventi frammentari – precedentemente richiamati – e i tentativi di ricondurre le nuove forme di aggressione alle fattispecie tradizionali, è seguita la Raccomandazione sulla criminalità informatica che diede origine alla legge n. 547 del 1993, recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica", che ha fatto fronte all'esigenza di apprestare un'adeguata tutela contro le nuove forme di aggressione inerenti alle tecnologie informatiche, introducendo i reati informatici nel codice penale. L'adozione di questa legge ha permesso di scongiurare le continue violazioni del principio di tassatività, dovute all'applicazione delle fattispecie tradizionali a fatti integranti condotte devianti inerenti ai sistemi informatici e ha consentito di adeguare la normativa interna ai dettami sovranazionali. La Raccomandazione invitava, infatti, gli stati a reprimere le condotte contenute nella lista "minima" con lo strumento penale e solo a discrezione le condotte contenute nella lista "facoltativa".

Tra i primi problemi affrontati durante l'*iter* legislativo vi era quello relativo alla scelta di modificare il codice penale o promuovere una legge speciale *ad hoc*: è stato doveroso stabilire se relegare le nuove figure criminose in un apposito titolo da destinare esclusivamente ai delitti in materia informatica e telematica ovvero ricondurre i nuovi reati alle figure esistenti che presentassero somiglianze con

[105] V. CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione, Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. pen. cont.*, 30 ottobre 2013.

essi[106]. La commissione ministeriale ha optato per la seconda scelta, nella convinzione che la particolarità della materia non fosse una ragione sufficiente per la configurazione di un titolo apposito, considerato che le nuove figure criminose si sono esplicate quale nuove forme di aggressione, caratterizzate dal mezzo utilizzato o dall'oggetto materiale, a beni giuridici già oggetto di tutela in altre parti del codice, anche per arginare la tendenza alla decodificazione[107]. Il legislatore ha preferito così novellare il codice penale, differentemente dalle scelte adottate in altri Paesi europei, quali Portogallo e Francia, dei quali il primo introdusse i *computer crimes* con una legge *ad hoc*, mentre il secondo introdusse un apposito titolo all'interno del codice penale[108]. La scelta italiana si avvicina a quella adottata dal legislatore tedesco, che ha introdotto le nuove fattispecie criminose laddove vi erano le corrispondenti fattispecie tradizionali, che sarebbero state applicabili qualora non fosse stato usato lo strumento informatico.

L'introduzione dei *computer crimes* si è tradotta nella previsione di nuove figure criminose all'interno del codice, vicine alle fattispecie tradizionali relative protettive dei medesimi beni giuridici, ovvero nell'aggiornamento delle tradizionali fattispecie di reato, con riferimenti al mondo delle tecnologie. Il legislatore ha, infatti, verificato quali tra le condotte rientranti nella nuova criminalità fossero già caratterizzate da rilevanza penale in base alle norme vigenti, operando in tal caso solo tramite un aggiornamento delle stesse. Doveroso è stato individuare, pertanto, il bene giuridico, che rappresenta il punto di contatto tra la realtà e l'astrazione normativa, che consente di ricostruire e incriminare esclusivamente le condotte lesive di un determinato bene tutelato, in conformità al principio di offensività, che

[106] Così D'AGOSTINI, D'ANGELO, VIOLINO, *Diritto penale dell'informatica: dai computer crimes alla digital forensic*, cit., 9.

[107] Presentazione da parte del Ministro di Grazia e Giustizia (G. Conso) del Disegno di legge n. 2773, Camera dei Deputati, XI Legislatura.

Tale scelta è stata condivisa anche da parte della dottrina, che denunzia con preoccupazione il dilagante aumento della legislazione penale speciale che ha causato un'indecifrabilità del sistema, come evidenziato da BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. Pen.*, 9/1995, 2329; di contro MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ*., 1992, 364 ss., che sottolinea come la materia avrebbe necessitato di un trattamento autonomo in base al riconoscimento di nuovi beni giuridici ovvero in base al riconoscimento di una nuova realtà che vede modificare le nozioni relative a norme tradizionali.

[108] In argomento FARINA, *Elementi di diritto dell'informatica*, cit., 244.

permette di escludere i comportamenti devianti compatibili con la lettera della legge, ma non offensivi del bene[109].

Il sistema penale italiano è ispirato al modello garantistico liberale del diritto penale del fatto, per cui il reato deve presentarsi quale forma di offesa ad un bene giuridico, a cui far ricorso quale ultima *ratio*, conformemente al principio di sussidiarietà, comportando una valutazione sulla meritevolezza della sanzione penale in base all'interesse da tutelare e al grado dell'offesa, nel rispetto del principio di proporzione. Ciò evidenzia come l'operazione più delicata sia stata quella di individuare i comportamenti ai quali attribuire rilevanza penale.

La legge ha implementato le disposizioni codicistiche, introducendo nuove fattispecie di reato e aggiornando quelle esistenti. Essa è intervenuta in settori eterogenei, aventi quale minimo comune denominatore l'utilizzo delle tecnologie informatiche nella commissione del fatto. Tali settori possono diversi in quattro macro-categorie: frodi informatiche, perpetrate avverso lo strumento informatico; falsificazione, riguardanti documenti predisposti da un sistema informatico e telematico; integrità dei dati e dei sistemi informatici; riservatezza dei dati e delle comunicazioni informatiche[110].

Il primo settore di intervento è quello delle frodi informatiche, che si caratterizzano poiché vengono realizzate servendosi di strumenti informatici e di conseguenza per l'assenza dell'induzione in errore del soggetto umano: la condotta criminosa consta della manipolazione di dati, con cui si produce l'ingiusto arricchimento, interferendo con l'elaborazione di dati e informazioni rilevanti[111]. Per garantire la repressione di simili condotte, che non potevano essere trattati alla stregua del delitto di truffa comune, è stata introdotta nel Capo II (Dei delitti contro il patrimonio mediante frode) del Titolo XII del codice penale la fattispecie di frode informatica all'art. 640-*ter*, la cui *ratio* è da ravvisarsi proprio nell'assunto di combattere il dilagante fenomeno di abuso delle tecnologie informatiche, la cui

[109] *Ivi*, 245, nt. 10: l'autore richiama sull'argomento MARINUCCI, DOLCINI, *Costituzione e politica dei beni giuridici*, in *Riv. it. dir. proc. pen*., 2/1994, 333-373, i quali sottolineano come la scelta della Costituzione sia ispirata a favore del modello del reato come offesa ai beni giuridici, che fa discendere delle conseguenze sia in capo al legislatore sia in capo all'interprete.

[110] Così NERI*, Criminologia e reati informatici. Profili di diritto penale dell'economia*, cit., 40.

[111] Sul punto PECORELLA, *Diritto penale dell'informatica*, cit., 13.

principale forma di manifestazione si esplica mediante la manipolazione di dati, volta a conseguire l'illecito arricchimento. La norma punisce «chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno». Il delitto ricalca la stessa struttura della truffa comune di cui all'art. 640 c.p., consumandosi nel momento in cui l'agente consegue l'ingiusto profitto, con conseguente danno per la vittima; da essa differisce però poiché l'attività fraudolenta non è rivolta verso la persona fisica, ma verso l'elaboratore, il cui funzionamento viene alterato o vi si interviene senza diritto[112]. Il bene giuridico tutelato, data la sua collocazione, è il patrimonio, anche se in dottrina vi è chi ritiene che ad esso vadano affiancati il regolare funzionamento dei sistemi informatici e della riservatezza che ne deve accompagnare l'utilizzazione, nonché secondo altri la salvaguardia della libertà negoziale[113].

La norma prevede due diverse modalità di condotta che si possono realizzare in qualsiasi modo: l'alterazione del funzionamento, che consiste nel creare anomalie nei sistemi presi di mira, agendo o sulla componente *hardware* o sulla componente *software*, incidendo sul regolare svolgimento del processo di elaborazione o trasmissione di dati; l'intervento illegittimo, posto in essere con qualsiasi modalità su dati, informazioni e programmi, che indica qualsiasi azione che produca una modifica nei processi dell'elaboratore. Con l'espressione "senza diritto", si vanno a circoscrivere le condotte di colui che non ha il consenso del titolare del sistema, ma anche di chi pone in essere condotte vietate dall'ordinamento giuridico. Il legislatore ha previsto una sanzione più elevata nel caso in cui il fatto sia commesso a danno dello Stato o di altro ente pubblico o col

[112] Sul punto si è recentemente pronunciata la Cass. pen., Sez. II, 05.02.2020, n. 10354, che ha statuito che «Il reato di frode informatica ha la medesima struttura e, quindi, i medesimi elementi costitutivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. Anche la frode informatica si consuma, pertanto, nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui».

[113] V. ANTOLISEI, *Manuale di diritto penale. Parte speciale*, cit., 499; si veda anche Cass. pen., Sez II, 15.04.2011, n. 17748, in *www.pluris-cedam.utetgiuridica.it.*

pretesto di far esonerare taluno dal servizio militare, nonché qualora il fatto sia commesso con abuso della qualità di operatore di sistema[114].

Il secondo settore di intervento si riferisce alle ipotesi di abuso della tecnologia manifestatosi con la condotta di falsificazione del documento informatico, che non poteva essere ricondotta alle classiche figure di falso documentale per la mancanza della forma scritta, per l'impossibilità della sottoscrizione – problema oggi risolto con l'introduzione della firma digitale – e per l'assenza di elementi che consentissero di individuarne la provenienza. Per "documento informatico in senso stretto" si indica, infatti, il documento redatto in forma elettronica, magnetica o ottica, che differisce dal "documento informatico in senso lato", vale a dire quel documento soltanto predisposto attraverso un sistema informatico ma contenuto su supporto tradizionale[115].

Proprio per le difficoltà di sussunzione della tutela del documento informatico nella sfera di tutela delle fattispecie tradizionali sui falsi, il legislatore è intervenuto con la legge 547/1993, introducendo al Capo III (Delle falsità in atti) del Titolo VII (Dei delitti contro la fede pubblica) l'art. 491-*bis*, inteso a tutelare la fiducia e la sicurezza dei dati informatici nelle relazioni giuridiche, quando rappresentativi di situazioni rilevanti. Con tale norma, il legislatore ha esteso la tutela prevista per le falsità in atti, alle ipotesi in cui oggetto di falsificazione sia un documento informatico, equiparando le falsità documentali al falso informatico, di modo che non fossero necessarie nuove figure di reato incentrate esclusivamente sulla falsificazione del documento informatico, nella convinzione che la tecnologia ha permesso solo nuove forme di aggressione a beni già tutelati dal codice, rendendo applicabili per estensione le fattispecie esistenti al nuovo tipo di documento, che si caratterizza in ragione della natura informatica del supporto[116].

---

[114] Per una compiuta analisi si veda "Codice penale commentato sub *art. 640-ter*", in *www.pluris-cedam.utetgiuridica.it.*

[115] Così PECORELLA, Diritto penale dell'informatica, cit., 126.

[116] *Ivi*, 140 ss.; si noti come questo aspetto sia stato sottolineato dalla Presentazione da parte del Ministro di Grazia e Giustizia (G. Conso) del Disegno di legge n. 2773, Camera dei Deputati, XI Legislatura: «In tal modo si raggiunge un duplice obiettivo: quello di non mutare la struttura delle fattispecie in funzione della sola diversità dell'oggetto materiale e quello di sottoporre ad identico regime sanzionatorio fatti criminosi che non si differenziano sul piano dell'oggettività giuridica ovvero della natura dell'interesse violato».

Oggetto del reato è il documento informatico pubblico o privato, che la norma del 1993 definisce come «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli», venendo in rilievo unicamente quelle registrazioni non direttamente visibili all'occhio umano, memorizzate su un dispositivo sui quali possono essere fissati i dati, al fine di consentirne un impiego o riproduzione su altro supporto, ad esempio attraverso la visualizzazione sullo schermo di un elaboratore. La tutela è riservata ai documenti informatici aventi efficacia probatoria, limitando così l'efficacia punitiva a quelle falsificazioni che sarebbero penalmente rilevanti se fossero state realizzate su documenti di tipo tradizionale. Da notare è che il legislatore ha definito il documento informatico quale supporto, restando così ancorato ad una definizione tradizionale di documento, che è stata poi superata dapprima con la "legge Bassanini" del 1997 e poi con l'entrata in vigore del "Codice dell'amministrazione digitale", che individua il documento informatico nella rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, a prescindere dal supporto materiale[117].

Rientra nel medesimo settore di intervento – falso informatico – la falsificazione del contenuto di comunicazioni informatiche, per cui è stato introdotto il nuovo reato di falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche, di cui all'art. 617-*sexies*, all'interno della Sezione V (Dei delitto contro l'inviolabilità dei segreti), Capo III (Dei delitti contro la libertà individuale), Titolo XII (Dei delitti contro la persona). La norma riproduce la disciplina che l'art. 617-*ter* riserva alle telecomunicazioni telefoniche o telegrafiche, richiamando le diverse condotte di formazione, alterazione e soppressione: la prima condotta consiste nel formare falsamente una comunicazione informatica mai avvenuta; l'alterazione consta nella modifica della comunicazione; la soppressione consiste nella distruzione della comunicazione o comunque nell'impedimento per il destinatario di apprenderne il contenuto[118]. Essa mira a tutelare la sicurezza, la genuinità e la veridicità del contenuto delle nuove

[117] V. D'AGOSTINI, D'ANGELO, VIOLINO, ATTANASIO, *Diritto Penale Dell'Informatica*, cit., 15.

[118] Cfr. "Codice penale commentato sub art. 617-*ter* c.p.", in *www.pluris-cedam.utetgiuridica.it*.

forme di comunicazione e reprime non già la mera falsificazione del contenuto di una comunicazione, ma l'uso che si faccia o si lasci ad altri fare, occorrendo pertanto l'utilizzo in concreto del falso contenuto e replicando la struttura del reato di falsità in scrittura privata di cui all'art. 485 c.p.[119]. La fattispecie penale richiede il dolo specifico, in quanto l'agente deve agire avendo di mira l'intento di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno.

Un ulteriore ambito di intervento della legge Conso è rappresentato dalle aggressioni all'integrità dei dati e dei sistemi informatici. Si tratta di condotte illecite aventi ad oggetto beni informatici, a cui si riconduce ogni forma di danneggiamento di un sistema tanto nelle componenti *software*, tanto in quelle *hardware*. Le ipotesi di danneggiamento riconducibili al supporto fisico non creavano particolari problematiche, stante la riconducibilità alla nozione di cosa di cui all'art. 635 c.p. Diversamente vi era difficoltà di ricondurre le ipotesi di danneggiamento delle parti c.d. logiche alle fattispecie esistenti, vale a dire la difficoltà di ricondurre dati e programmi alla nozione di cosa, tipica della fattispecie di danneggiamento tradizionale di cui all'art. 635 c.p., richiedendo così l'intervento del legislatore.

L'intervento è stato effettuato con la legge del 1993, recependo le sollecitazioni poste dalla Raccomandazione del Consiglio d'Europa del 1989, mediante integrazione della tutela apprestata dalle fattispecie tradizionali e mediante l'inserimento di nuove fattispecie criminose, considerando non solo le ipotesi di danneggiamento alle componenti immateriali, ma anche quelle ipotesi di sabotaggio informatico aventi ad oggetto sistemi informatici, il cui funzionamento è di vitale interesse per la collettività, e dando specifica risposta alle ipotesi di diffusione di programmi *virus*. Con tale novella legislativa si è introdotta, al Capo I (Dei delitti contro il patrimonio mediante violenza alle cose o alle persone) del Titolo XIII, la fattispecie di danneggiamento di sistemi informatici e telematici di cui all'art. 635-*bis*, con cui il legislatore ha inteso reprimere le diverse forme di aggressione, sia alle componenti fisiche che logiche, dei sistemi informatici e telematici, ponendo fine ai dibattiti circa l'applicabilità dell'art. 635 c.p. e sostituendosi a questo nelle ipotesi di aggressione ai sistemi nel loro complesso.

[119] Così PECORELLA, *Diritto penale dell'informatica,* cit., 163 ss.

Tale norma sanziona, infatti, la condotta di chi distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui. In tal modo si va a ricomprendere, nella fattispecie in esame, oltre le ipotesi di danneggiamento logico – riferendosi a dati, informazioni o programmi – il danneggiamento dell'*hardware*, che comporta una lesione rivolta alle componenti fisiche del sistema. Ai fini dell'applicazione della stessa si richiede il requisito dell'altruità, richiedendo che tra il soggetto attivo e l'oggetto del reato non incorra una relazione di proprietà.

La distruzione di dati o programmi si realizza mediante la eliminazione definitiva degli stessi; il deterioramento indica una diminuzione apprezzabile del valore o della utilizzabilità del sistema; l'inservibilità comprende in sé tutte le ipotesi non riconducibili alla distruzione o deterioramento[120]. La fattispecie contiene con una clausola di sussidiarietà espressa – «salvo che il fatto costituisca più grave reato» – che è volta a circoscriverne l'ambito applicativo a fronte di più gravi presidi, come ad esempio quello previsto all'art. 420 c.p., vale a dire l'aggressione ad un sistema informatico di pubblica utilità.

Tra le innovazioni rientranti in tale settore, si rileva come all'art. 392 c.p., rubricato "Esercizio arbitrario delle proprie ragioni con violenza sulle cose", sia stato aggiunto un terzo comma, con cui si estende agli effetti della legge penale la nozione di "violenza sulle cose" ad alcuni comportamenti ricadenti su programmi informatici o telematici ovvero sul funzionamento di un sistema informatico o telematico. L'integrazione di tale fattispecie normativa, collocata nel Capo III (tutela arbitraria delle proprie ragioni) del Titolo III (Dei delitti contro l'amministrazione della giustizia), ha permesso di adattare la fattispecie tradizionale all'entità immateriale propria dei programmi informatici, che in quanto tali non erano assimilabili alla *res* corporea, cui la norma si riferiva[121]. La *ratio* va, infatti, ricercata nella necessità di evitare che comportamenti devianti, apparentemente riconducibili alle ipotesi di danneggiamento o mutamento di destinazione, andassero esenti da sanzione. Il soggetto agente, nell'ipotesi di cui al terzo comma, facendosi arbitrariamente ragione da sé, non coinvolge il supporto

[120] Cfr. D'AGOSTINI, D'ANGELO, VIOLINO, ATTANASIO, *Diritto Penale Dell'Informatica*, cit., 33 ss.

[121] *Ivi*, 11 s.

fisico, ma la sua condotta di alterazione, modificazione, cancellazione, impedito funzionamento coinvolge la parte immateriale, c.d. logica. Le modalità di aggressione sembrano richiamare la fattispecie di danneggiamento di sistema informatico o telematico, di cui all'art. 635-*bis* c.p.: la distinzione è da ravvisare nella presenza o meno di un preteso diritto da far valere, al momento della condotta.

Sempre nel medesimo settore, l'art. 420 c.p., "Attentato a impianti di pubblica utilità", è stato integralmente sostituito dalla legge 547/1993, al fine di apprestare la tutela prevista dalla norma ai casi in cui oggetto della condotta illecita siano sistemi informatici o telematici, ovvero i dati, le informazioni o i programmi in essi contenuti.

La norma, collocata nel Libro II, Titolo V (Dei delitti contro l'ordine pubblico), prevede al primo comma la reclusione da uno a quattro anni, per l'ipotesi in cui il soggetto commetta un'azione diretta a danneggiare o distruggere impianti di pubblica utilità. La medesima pena viene applicata, nel secondo comma, nel caso in cui tale azione sia diretta avverso un sistema informatico o telematico, ovvero dati, informazioni o programmi in essi contenuti, fermo restando il requisito della pubblica utilità. La legge ha previsto anche un aggravamento di pena nel caso in cui dal fatto derivi la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema.

Il requisito della pubblica utilità, che caratterizza l'oggetto materiale, va inteso nel senso di ricomprendere tutti i sistemi che in concreto svolgano una funzione pubblica, a prescindere dall'appartenenza ad un soggetto pubblico o privato. La novella legislativa non ha inciso sulla struttura del reato, costruito come delitto di attentato ovvero a consumazione anticipata, il cui momento consumativo coincide con il porre in essere la condotta diretta a danneggiare o distruggere. Si è mantenuta tale struttura per la rilevanza di tali sistemi, il cui attentato ad essi può essere fonte di pericolo per l'ordine pubblico[122].

Al fine di proteggere l'integrità dei dati e dei sistemi informatici e per combattere il dilagante fenomeno di diffusione dei programmi *virus*, è stata

[122] *Ivi*, 12 s.; si veda altresì SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 193 ss.

introdotta una nuova figura delittuosa nella Sezione IV (Dei delitti contro l'inviolabilità del domicilio), Capo III (Dei delitti contro la libertà individuale), del Titolo XII, all'art. 615-*quinquies* rubricata "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico". Il reato in esame mira a sanzionare la condotta ci chi diffonde, comunica, consegna un programma informatico malevolo avente per scopo o effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Si può notare come tale fattispecie attribuisca rilevanza penale a condotte prodromiche al danneggiamento, che potrebbe anche non verificarsi, qualificandosi così come un antecedente rispetto ai reati di evento di cui agli artt. 635-*bis*, 615-*ter* e 640-*ter*. L'oggetto materiale deve quindi essere un programma infetto, che va a ricomprendere i programmi *malware* idonei a danneggiare il sistema ovvero i dati e i programmi in esso contenuti.

La condotta di diffusione implica la messa in circolazione di programmi malevoli presso un numero indeterminato di persone, attuata mediante un sistema di reti ovvero mediante inserimento materiale degli stessi in un sistema informatico; la consegna implica la consegna del programma mediante cessione del supporto fisico su cui è registrato, con conseguente disponibilità altrui; la comunicazione comporta la cessione del programma malevolo per via telematica[123]. Tali condotte assumono rilevanza solo a condizione che siano oggettivamente idonee a creare una situazione di pericolo per i sistemi altrui.

Il legislatore del '93 è intervenuto anche a tutela della riservatezza dei dati e delle comunicazioni informatiche. Sempre più frequentemente si verificavano episodi di indebita acquisizione di dati e programmi riservati: condotte che rientrano nel c.d. "spionaggio informatico", in grado di creare non solo un pregiudizio economico, ma anche di mettere a rischio la riservatezza e l'integrità dei dati e dei programmi, contenuti nel sistema informatico. Proprio per questo il legislatore si è adoperato per incriminare le condotte – sconosciute prima dell'avvento della tecnologia informatica – di accesso a sistemi informatici altrui

[123] In argomento PECORELLA, *Diritto penale dell'informatica*, cit., 249 ss.

volte ad ottenere dati o programmi riservati e ha innovato la disciplina esistente dedicata ai delitti contro l'inviolabilità dei segreti.

Con la novella Conso, il legislatore ha accolto le indicazioni sovranazionali, inserendo una nuova disposizione nel codice penale, collocato nella Sezione IV (Dei delitti contro l'inviolabilità del domicilio), Capo III, Titolo XII, all'art. 615-*ter*, volta a reprimere l'accesso abusivo ad un sistema informatico o telematico. La nuova fattispecie ricalca i contorni del tradizionale reato di violazione di domicilio, di cui all'art. 614 c.p., in quanto volta a incriminare l'indebita intrusione in un sistema informatico altrui, realizzata con qualsiasi mezzo. Il sistema informatico è, infatti, considerato alla stregua di un'espansione ideale del domicilio tradizionale, pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione[124]. L'indebito accesso si connota di rilevanza penale, allorché sia rivolto avverso sistemi protetti da misure di sicurezza, vale a dire tutti quei dispositivi di tipo sia fisico che logico, volti ad impedire l'accesso ai soggetti non autorizzati. Per accesso abusivo si intende quella attività con cui un soggetto, connettendosi ad un sistema, ha la possibilità di prendere cognizione di dati, informazioni e programmi, ivi rinvenuti. La norma reprime altresì la condotta del soggetto che acceda al sistema in modo legittimo e vi si mantenga contro la volontà espressa o tacita del titolare dello *ius excludendi alios*.

Oggetto materiale del reato è un sistema informatico o telematico: con il primo ci si riferisce ad un complesso di elaboratori e di programmi per acquisire ed elaborare le informazioni in modo automatico; con sistema telematico si intende, invece, un mezzo per collegare gli elaboratori mediante una rete di telecomunicazioni[125].

L'individuazione del bene giuridico che la norma mira proteggere è controversa, per cui si sono prospettate tre differenti teorie: la prima indica l'oggetto di tutela nel domicilio informatico, date le affinità presentate tra l'art.615-*ter* e l'art. 614 c.p.; la seconda ipotesi riconduce l'oggetto giuridico all'integrità del sistema o dei dati, nonostante la sua collocazione sistematica; la terza individua l'oggetto di tutela nella riservatezza dei dati.

[124] In tal modo viene considerato nella presentazione da parte del Ministro di Grazia e Giustizia (G. Conso) del Disegno di legge n. 2773, Camera dei Deputati, XI Legislatura.

[125] Così definiti da ANTOLISEI, *Manuale di diritto penale.*, cit., 279.

La prima tesi è criticata da chi ritiene che in tal modo si estenderebbe impropriamente la sfera della riservatezza personale, dato che il delitto si applica anche nel caso di intrusione in sistemi appartenenti al settore pubblico, non legati alla nozione di domicilio e proiezione spaziale della persona.

La seconda tesi fa leva sulla previsione di un aumento di pena qualora dal fatto derivi la distruzione o il danneggiamento del sistema o dei dati o programmi in esso contenuti, ad evidenziare l'effettiva lesione del bene giuridico: tale tesi non può tuttavia essere accolta, in quanto così facendo la norma in esame andrebbe a prevenire una conseguenza dell'accesso abusivo, deviando l'obiettivo principale, costituito dalla tutela dell'acquisizione di informazioni riservate[126].

La terza tesi pone in evidenza il fatto che la riservatezza dei dati e dei programmi contenuti in un sistema informatico risulta messa in pericolo dalle intrusioni di terzi non autorizzati; tuttavia, se fosse così inteso, resterebbero privi di tutela i sistemi che non contengono dati o programmi ovvero contengono dati o programmi di pubblico dominio, essendo la condotta in tal senso inoffensiva per il bene protetto[127].

La giurisprudenza ha abbracciato la prima tesi, identificando il domicilio informatico in uno spazio ideale, ma anche fisico in cui sono contenuti i dati informatici di pertinenza del soggetto, che devono essere salvaguardati da qualsivoglia intrusione; ha sottolineato però come l'oggetto di tutela sia più ampio, concretandosi nello "*ius excludendi alios*" ed estendendo così la tutela non solo alla riservatezza informatica, ma anche agli aspetti economico-patrimoniali dei dati contenuti nel sistema[128].

Ai fini dell'integrazione della fattispecie è richiesto il dolo generico, che si sostanzia nella coscienza e volontà di accedere o mantenersi in un sistema informatico e nella consapevolezza dell'abusività del proprio comportamento, nonché l'altruità del sistema.

---

[126] In tal senso PECORELLA, *Diritto penale dell'informatica*, cit., 319 ss.; D'AGOSTINI, D'ANGELO, VIOLINO, ATTANASIO, *Diritto penale dell'informatica*, cit., 44.

[127] La giurisprudenza di legittimità pone in luce come l'articolo in esame non si limiti a tutelare i contenuti personali dei dati raccolti, ma offra una tutela più ampia: v. Cass. pen., Sez. VI, 04.10.1999, n. 3067, in *Cass. pen.*, 11/2000.

[128] V. Cass. pen., Sez. VI, 04.10.1999, n. 3067, in *Cass. pen.*, 11/2000.

La norma prevede al secondo comma una pena aggravata qualora il fatto sia commesso da un pubblico ufficiale o un incaricato di pubblico servizio, con abuso dei poteri o violazione dei doveri inerenti alla funzione o al servizio o da chi esercita anche abusivamente la professione di investigatore privato o con abuso della qualità di operatore di sistema; è aggravata altresì qualora il colpevole per commettere il fatto utilizzi violenza sulle cose o persone, o sia armato – ricalcando quanto previsto per la violazione di domicilio – nonché se dal fatto derivi la distruzione o il danneggiamento o l'interruzione del funzionamento del sistema o dei dati o programmi in esso contenuti. È prevista, al terzo comma, un'ulteriore aggravante per l'ipotesi in cui i fatti previsti dal primo e dal secondo comma riguardino sistemi di interesse militare o di interesse pubblico, considerando in tal modo la delicatezza dei dati che ivi possono essere contenuti.

Per la tutela della riservatezza dei dati e delle comunicazioni informatiche, è stata introdotta la norma incriminatrice della detenzione e diffusione abusiva di codici d'accesso, collocata nella Sezione VI, Capo III, Titolo XII, all'art. 615-*quater* del codice penale, rispondendo così alle sollecitazioni sovranazionali volte ad incriminare anche il commercio di codici ottenuti illecitamente per realizzare un accesso abusivo[129]. L'intento del legislatore era quello di prevenire condotte volte all'uso non autorizzato di quei mezzi che consentono un accesso abusivo, reprimendo condotte prodromiche alla realizzazione dello stesso.

Con tale previsione si punisce chiunque si procura, riproduce, diffonde, comunica o consegna abusivamente codici o comunque mezzi idonei a consentire l'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o ancora fornisce indicazioni utili a tale scopo, andando a reprimere ogni forma di condotta volta al conseguimento di tale scopo, che spazia dalla condotta di chi contribuisce a tale scopo, a quella di chi acquisisce la disponibilità di tali mezzi.

A dispetto del *nomen* della disciplina, non è esplicitamente menzionata la mera detenzione di codici di accesso da parte di chi non è autorizzato a utilizzarne, né si ritiene configurabile in tal caso un'ipotesi di tentativo, data la difficoltà di configurazione di quest'ultimo; ciononostante tale ipotesi viene ugualmente ricondotta alla fattispecie in esame, in quanto sarebbe prova di una condotta di

[129] Cfr. PECORELLA, *Diritto penale dell'informatica*, cit., 356 ss.

procacciamento degli stessi o comunque di autonoma elaborazione, facendola rientrare nella nozione di "procurarsi"[130]. Le condotte assumono rilevanza penale solo ove realizzate abusivamente, vale a dire da parte di colui che non sia autorizzato dal titolare del sistema. La norma richiede il dolo specifico di procurare a sé o ad altri un profitto o di arrecare ad altri un danno.

È prevista un'aggravante nel caso di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico, ovvero qualora il fatto sia commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore di sistema.

A tutela dell'inviolabilità dei segreti riguardanti documenti informatici è intervenuto il legislatore con l'introduzione di un secondo comma all'art. 621 c.p., rubricato "Rivelazione del contenuto di documenti segreti". La legge 547/1993 ha esteso la tutela, ampliando il concetto di documento, agli effetti della disposizione di cui al comma primo, comprensiva ora di tutti i supporti informatici contenenti dati, informazioni o programmi[131]. L'articolo punisce, se dal fatto derivi nocumento, la condotta di colui che essendo venuto abusivamente a conoscenza di un contenuto che debba rimanere segreto, lo rivela senza giusta causa ovvero lo impiega a proprio profitto.

Sempre a tutela dell'inviolabilità dei segreti, con la modifica dell'art. 623-*bis* – "Altre comunicazioni e conversazioni" – il legislatore ha aggiunto le modalità di comunicazione "informatica e telematica" e ha eliminato il riferimento allo strumento tecnologico del mezzo di trasmissione effettuato su filo, così stabilendo che «le disposizioni sulla tutela dell'inviolabilità dei segreti relative alle comunicazioni e conversazioni telegrafiche, telefoniche e informatiche si applicano si applicano a qualunque altra trasmissione a distanza di suoni, immagini o dati»[132].

---

[130] *Ivi*, 371 s.; diversamente ATERNO, *Aspetti problematici dell'art. 615-quater c.p.*, in *Cass. Pen.*, 4/2000, 870 ss., il quale ritiene che «[...] l'elencazione delle condotte sia tassativa e, di conseguenza, nel rispetto del principio di stretta legalità dovrebbe escludersi la rilevanza penale della mera detenzione e ciò al fine di evitare un'ulteriore ed eccessiva anticipazione della soglia di punibilità, difficilmente giustificabile sul piano della adeguatezza e della meritevolezza della pena, anche alla luce del richiesto dolo specifico che difficilmente potrebbe qualificare una condotta di mera detenzione».

[131] Presentazione da parte del Ministro di Grazia e Giustizia (G. Conso) del Disegno di legge n. 2773, Camera dei Deputati, XI Legislatura, 11.

[132] *Ibidem*.

Con l'inserimento dell'ultimo comma dell'art. 616 c.p. – rubricato "Violazione, sottrazione e soppressione di corrispondenza" e collocato nella Sezione V "Dei delitti contro la inviolabilità dei segreti", del Capo III, Titolo XII – il legislatore ha voluto estendere la tutela già prevista per le forme di corrispondenza tradizionale alle nuove tecnologie, tutelando in tal modo le comunicazioni informatiche o telematiche, vale a dire quelle comunicazioni realizzate mediante la tecnologia informatica, sia dal punto di vista statico, corrispondenza contenuta in supporti informatici, che dinamico ossia trasmessa per mezzo di un sistema informatico o telematico.

Il bene giuridico tutelato è la segretezza della corrispondenza. Per corrispondenza informatica si intende quella corrispondenza destinata ad essere inoltrata o comunque ricevuta per mezzo di un sistema informatico, memorizzata su un supporto di memoria, comprendendo così un'ampia gamma di ipotesi. Rientra nelle ipotesi *de quo* solamente la corrispondenza di cui il destinatario non ha preso visione, poiché in caso contrario troverebbero applicazione altre ipotesi di reato.

Per quanto attiene l'elemento soggettivo è stato previsto il dolo generico nei casi di pressa cognizione della corrispondenza chiusa, di distruzione e di soppressione e il dolo specifico per le ipotesi di sottrazione e distrazione, in quanto si richiede la finalità di prendere o farne prendere cognizione da parte di soggetti terzi.

Il legislatore è intervenuto, ancora nell'ambito dell'inviolabilità dei segreti, anche per assicurare tutela alle comunicazioni in atto, per cui si è ritenuto necessario introdurre nuove figure di reato, volte a reprimere l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche all'art. 617-*quater* c.p. e l'installazione di apparecchiature atte ad effettuarne l'intercettazione, l'impedimento o l'interruzione all'art. 617-*quinquies,* per tutelare la libertà e la riservatezza di tali comunicazioni.

L'art. 617-*quater* sanziona al primo comma l'intercettazione fraudolenta, ossia la conoscenza occulta o illegittima della comunicazione, l'impedimento, che indica una parziale impossibilità della comunicazione, e l'interruzione, che dà luogo ad un'impossibilità totale; al secondo comma, viene incriminata con la medesima pena la condotta di colui che divulga, mediante qualsiasi mezzo di

informazione al pubblico, il contenuto delle comunicazioni intercettate[133]. La fattispecie mira a proteggere le comunicazioni informatiche riservate in fase di trasmissione – profilo dinamico – che include sia le comunicazioni tra sistemi informatici, sia comunicazioni tra apparecchi[134].

Il delitto è aggravato qualora il fatto sia commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici ovvero quando il soggetto agente rivesta una particolare qualifica. Le medesime aggravanti si applicano anche per la successiva ipotesi di reato, di cui all'art. 617-*quinquies*.

Tale nuova figura criminosa è strettamente connessa alla precedente, in quanto incrimina condotte ad essa prodromiche. Viene punita, anticipando la tutela, l'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche. Ai fini della sussistenza del reato non è necessario utilizzare l'apparecchiatura installata, ma bisogna accertare l'idoneità in concreto della stessa a provocare l'evento dannoso, vale a dire ad intercettare, impedire o interrompere la comunicazione.

Accanto alle innovazioni e contestuali modifiche inerenti alla parte sostanziale, il legislatore è intervenuto anche ad integrare le norme processuali in tema di intercettazioni, introducendo l'art. 266-*bis* c.p.p., che ammette tra i mezzi di ricerca della prova l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi per i procedimenti relativi ai reati indicati nell'art. 266 c.p.p. e ai reati commessi tramite tecnologie informatiche o telematiche; consentendo di effettuare, ai sensi dell'art. 268 c.p.p., tali intercettazioni mediante impianti appartenenti a privati, allorché vi sia la necessità di disporre di particolari strutture o apparecchiature; integrando l'art. 25-*ter* del decreto legge n.306 del 1992, convertito con modificazioni dalla legge n.356 del 1992, disciplinante le intercettazioni preventive, estendendo tale forma di intercettazione anche alle comunicazioni relative a sistemi informatici o

[133] In tal senso D'AGOSTINI, D'ANGELO, VIOLINO, ATTANASIO, *Diritto Penale Dell'Informatica,* cit., 28.

[134] Così PECORELLA, *Diritto penale dell'informatica,* cit., 303.

telematici[135], che possono essere utilizzate qualora necessarie per l'attività di prevenzione relativa ai delitti di cui all'art. 51 comma 3-*bis* c.p.p.

La legge 547/1993 ha avuto il merito di aver introdotto nell'ordinamento italiano i *computer crimes*, ma è stata anche oggetto di critiche per lo più dovute alla formulazione delle singole fattispecie e alla mancata considerazione degli effetti che avrebbe sortito la criminalizzazione di certe condotte.

4.2 La Convenzione di Budapest, 23 Novembre 2001

La presa di consapevolezza della rilevanza internazionale del fenomeno della criminalità informatica ha ottenuto pieno riconoscimento con l'adozione da parte del Consiglio d'Europa della c.d. Convenzione sulla criminalità informatica, firmata a Budapest in data 23 novembre 2001, dopo un *iter* durato quattro anni, grazie alla quale gli Stati partecipanti si sono impegnati a disciplinare uniformemente un settore nato con lo sviluppo della tecnologia informatica. Entrata in vigore il 1° luglio del 2004, essa rappresenta uno dei più importanti strumenti sovranazionali in tale ambito ed è un punto di riferimento per la cooperazione internazionale, nonché un modello per chiunque voglia legiferare con l'obiettivo di arginare la criminalità nello spazio virtuale, caratterizzata dall'assenza di confini geografici. La Convenzione è stata sottoscritta da sessantasette paesi, tra cui anche paesi extraeuropei, e per la cui entrata in vigore l'art. 36 della stessa richiede che sia ratificata da cinque Stati, tre dei quali appartenenti al Consiglio. Essa è composta da 48 articoli, divisi in quattro capitoli, comprendenti le definizioni rilevanti, le misure da adottare in ambito nazionale in tema di diritto sostanziale e procedurale, la cooperazione internazionale e le clausole finali.

Gli scopi della convenzione sono quelli di armonizzare le infrazioni presenti nel diritto penale nazionale e le disposizioni comuni; consentire la perseguibilità dei delitti perpetrati mediante un sistema informatico, con il conferimento dei poteri necessari agli organi investigativi dei singoli Stati; assicurare la cooperazione

[135] Presentazione da parte del Ministro di Grazia e Giustizia (G. Conso) del Disegno di legge n. 2773, Camera dei Deputati, XI Legislatura, 12.

internazionale, mediante una strategia comune di contrasto a questi illeciti, data la natura transnazionale degli stessi[136].

La Convenzione – conscia del carattere globalizzante delle reti informatiche e quindi della necessità di perseguire tale fenomeno con una politica comune finalizzata alla protezione della società – si apre con l'indicazione di alcune definizioni terminologiche rilevanti, in grado di assicurare nozioni armonizzate negli Stati partecipanti, in riferimento al "sistema informatico", "dati informatici", "fornitori di servizi" e "dati relativi al traffico". In particolare, per sistema informatico si intende qualsiasi apparecchiatura o un gruppo di apparecchi interconnessi o collegati, di cui uno o più dei quali compie un'elaborazione automatica dei dati, grazie ad un programma; per dati informatici si indica qualsiasi rappresentazione di fatti, informazioni o concetti idonei ad essere utilizzati da parte di un programma o di un sistema informatico, ai fini dello svolgimento di una funzione; prestatore di servizi si identifica in un qualsiasi soggetto pubblico o privato che fornisce agli utenti dei propri servizi la possibilità di comunicare mediante un sistema informatico, nonché una qualsiasi entità che elabori o archivi dati per conto di un prestatore di servizi; per dati relativi al traffico si indicano i dati relativi ad una comunicazione realizzata mediante un sistema informatico e prodotta dallo stesso[137].

La Convenzione prevede, agli articoli successivi, alcune misure normative di diritto penale sostanziale da adottare a livello nazionale, che rappresentano il fulcro della stessa: trattasi di misure legislative atte a sanzionare le tipiche condotte di aggressione ai sistemi informatici, quali le fattispecie di accesso abusivo, di cui all'art. 2 della Convenzione, in cui si prevede che ogni Parte debba adottare misure necessarie per sanzionare le condotte di accesso illegale ai sistemi, senza autorizzazione, e che si possa richiedere che, ai fini dell'integrazione, il reato sia commesso violando le misure di sicurezza e con intenti illegali; intercettazione illegale, di cui all'art. 3, in cui si richiede l'incriminazione dell'intercettazione abusiva, senza autorizzazione di dati informatici durante trasmissioni non

[136] In argomento SARZANA DI S. IPPOLITO, *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. proc.*, 4/2002, 509 ss.

[137] Cfr. art. 1 della Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest 23.11.2001.

pubbliche, effettuata mediante strumenti tecnici; attentato all'integrità dei dati e dei sistemi, di cui agli artt. 4-5, che comprende tra le condotte da considerare penalmente rilevanti il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici, nonché il serio impedimento del funzionamento del sistema informatico mediante l'introduzione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici, senza autorizzazione; abuso di apparecchiature, che comprende la fabbricazione, la vendita, la cessione, senza diritto, di dispositivi, anche *software*, e *password* o codici validi per l'accesso al sistema, per commettere una delle condotte precedentemente elencate da qualificare come reato, nonché il semplice possesso di tali strumenti, qualora si abbia l'intenzione di usarli per commettere tali reati; falsificazione informatica, di cui all'art. 7, in cui si prevede che vadano sanzionate condotte come l'introduzione, la soppressione, l'alterazione, senza diritto, di dati informatici non autentici, con l'intenzione di utilizzarli come se lo fossero; frode informatica, di cui all'art. 8, che prevede la repressione di condotte volte a determinare un pregiudizio nella sfera patrimoniale altrui ovvero un beneficio economico proprio o di terzi; pornografia infantile, di cui all'art. 9, che prevede che siano sanzionate le condotte di produzione di pornografia minorile allo scopo della diffusione, l'offerta, la distribuzione, il procacciamento per sé o per altri e il possesso mediante un sistema informatico di tale materiale; violazione della proprietà intellettuale, che prevede che gli Stati sanzionino le condotte violanti il diritto d'autore, tenuto conto degli obblighi assunti a livello internazionale[138]. Si noti come sia richiesto nelle norme che gli autori abbiano agito intenzionalmente e senza diritto.

La Convenzione prevede che per i reati summenzionati siano previsti la repressione del concorso di persone nel reato, nonché del tentativo, ad esclusione per quest'ultima ipotesi del reato previsto dall'art. 2 – accesso illegale ad un sistema informatico – e dall'art. 6 – abuso di apparecchiature. Si afferma che ogni Stato debba predisporre le misure necessarie affinché sia prevista una responsabilità delle persone giuridiche, nel cui interesse sia stato commesso il reato da parte di una

[138] Si vedano gli artt. 2-10 della Convenzione del Consiglio d'Europea sulla criminalità informatica, Budapest 23.11.2001.

persona fisica – ad esse appartenenti o di cui sono dipendenti – ovvero che abbiano permesso la commissione del reato da parte di tali soggetti per mancanza di sorveglianza o controllo; rispetto a ciò l'Italia aveva già disposto con d.lgs. 231/2001 una normativa inerente alla responsabilità delle persone giuridiche, individuando i criteri per la relativa imputazione, ma la Convenzione ha sensibilmente aumentato le ipotesi di reato presupposto ad esse imputabili.

Importante è che l'efficacia di tali fattispecie deve essere assicurata mediante sanzioni effettive, proporzionate e dissuasive, che annoverino finanche la privazione della libertà. Si noti come l'Italia avesse già previsto la repressione penale di talune condotte all'interno della legge n. 547/1993, sulla scorta di quanto disposto dalla Raccomandazione (89) 9, con cui è possibile rinvenire delle analogie: tra queste si annoverano la fattispecie di frode informatica di cui all'art. 640-*ter* c.p.; l'accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p.; le condotte riconducibili alle ipotesi di danneggiamento di cui all'art. 635-*bis*; le ipotesi di intercettazione riconducibili agli artt. 617-*quater* e 617-*quinquies* del c.p.; ancora, le ipotesi di abuso di apparecchiature riconducibili all'art. 615-*quater* del c.p.

Il secondo capitolo della Convenzione si compone di misure procedurali da adottare affinché si abbia il perseguimento dei reati anzidetti. Si richiede l'adozione di specifiche procedure, necessarie per un corretto espletamento delle indagini e per un'effettiva repressione dei *cybercrimes*, tra cui misure atte a garantire la conservazione rapida dei dati informatici allorché siano particolarmente soggetti a modificazione, il mantenimento dell'integrità delle informazioni per il tempo necessario e la produzione di dati informatici che siano nella disponibilità di privati o del fornitore di servizi[139]. Si richiede agli Stati di assicurare misure armonizzate per consentire alle autorità competenti di procedere alla perquisizione, al sequestro ovvero all'accesso a sistemi, dati e supporti informatici, nonché di adottare regole uniformi per la raccolta e registrazione in tempo reale dei dati relativi al traffico, intercettazione e registrazione delle comunicazioni telematiche[140].

[139] In argomento CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 42.
[140] Così AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 7.

Di rilievo è la disposizione prevista in materia di competenza, che si è rivelata indispensabile per assicurare la punibilità delle fattispecie criminose caratterizzate da aterritorialità: si prevede, in accordo al principio di territorialità, che ogni Stato debba predisporre le misure necessarie atte a perseguire le condotte integranti i reati previsti dalla Convenzione, qualora siano commesse nel proprio territorio, a bordo di una nave e di un aeromobile immatricolato presso quella Parte, anche quando poste in essere da un proprio cittadino, se l'infrazione è penalmente punibile ove è stata commessa ovvero se l'infrazione non rientra nella competenza territoriale di alcuno Stato. Viene creato uno spazio giudiziario comune per cui, qualora più Stati dovessero rivendicare la propria competenza per una medesima condotta criminosa prevista dalla Convenzione, le autorità statuali, appartenenti ai Paesi coinvolti, provvederanno ad una consultazione, al fine di stabilire il modo più opportuno per esercitare l'azione penale. Tali indicazioni sono essenziali per assicurare un'efficace e pronta repressione del fenomeno, dato che la reciproca assistenza giudiziaria è fondamentale nello svolgimento di indagini transnazionali in materia di reati informatici, così da non disperdere le volatili tracce che caratterizzano i dati dei sistemi informatici e telematici, che possono essere facilmente alterati, copiati o distrutti.

Molta importanza riveste altresì il terzo capitolo della Convenzione, riguardante la cooperazione internazionale: si apre con una disposizione che impone alle autorità statali di cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti inerenti reati collegati a sistemi informatici o telematici, nonché per raccogliere prova in forma elettronica, in accordo alle disposizioni previste dalla stessa e tenendo conto dell'applicazione degli strumenti internazionali relativi alla assistenza in materia penale. In merito all'estradizione, è previsto che questa si applichi alle disposizioni previste dalla Convenzione, a condizione che siano punibili in entrambi gli Stati mediante una pena detentiva massima di un anno o con pena più severa, salva l'applicazione di accordi bilaterali cui far riferimento. Essa contempla l'assistenza giudiziaria tra i vari membri della stessa, prevedendo mutua assistenza ai fini della celerità delle indagini e dei procedimenti inerenti ai reati relativi a sistemi e dati informatici ovvero per assicurare la raccolta di prove collegate ad un fatto criminoso in formato elettronico.

È previsto, in particolare, che in caso di urgenza, la richiesta di assistenza possa essere formulata anche mediante mezzi rapidi di comunicazione, a condizione che tali strumenti mantengano le esigenze di sicurezza e di autenticazione, richiedendo altresì una conferma ulteriore ufficiale se lo Stato richiesto la ritiene necessaria[141].

Per salvaguardare la celerità delle indagini, la Convenzione include molteplici misure provvisorie, volte a snellire le procedure e i tempi richiesti, assicurando una completa indagine: conservazione rapida dei dati informatici, in relazione ai quali la Parte richiedente intende domandare l'assistenza in vista di una perquisizione, di un accesso, di un sequestro, di una divulgazione; rapida divulgazione dei dati di traffico conservati; assistenza concernente l'accesso ai dati raccolti, che si sostanzia nella richiesta ad altra Parte di perquisizione, di sequestro, di divulgazione dei dati conservati mediante un sistema informatico, locato nel territorio della Parte richiesta; accesso transfrontaliero dei dati conservati con il consenso, quando questi siano accessibili al pubblico, senza l'autorizzazione della Parte; assistenza in tempo reale della raccolta dei dati relativi al traffico, nonché assistenza in materia di intercettazione di tali dati[142]. Al fine di assicurare un'assistenza immediata per le investigazioni e in particolare per la raccolta di prove, è prevista l'istituzione di un punto di contatto – "rete 24/7" – raggiungibile in ogni momento.

Il quarto capitolo attiene alle clausole finali, inerenti alla firma e all'entrata in vigore della Convenzione, le modalità di adesione, l'applicazione, gli effetti territoriali, nonché le dichiarazioni che le Parti possono fare al momento della firma e le riserve.

La natura transnazionale della criminalità informatica rende necessaria un'uniformità legislativa in ambito internazionale, al fine di assicurare la tutela dei beni messi in pericolo dalla stessa e reprimere il fenomeno. Il raggiungimento di tale obiettivo è lo strumento scongiurare la formazione di Stati individuabili come "paradisi informatici", in cui non siano presenti le garanzie e le regole minime prospettate all'interno della Convenzione e che dovranno essere assicurate dalle legislazioni nazionali.

---

[141] Cfr. CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 43.

[142] Sul punto SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 619 s.

4.3 La legge di ratifica della Convenzione: legge n. 48/2008

Il legislatore italiano ha provveduto a ratificare, non senza ritardo, la Convenzione del Consiglio d'Europa sulla criminalità informatica con la legge 18 marzo 2008, n. 48. Essa è frutto di un *iter* travagliato, che ha assistito al coinvolgimento di varie figure istituzionali, che ebbe inizio dapprima nel 2003 – quando venne istituita, con decreto emesso di concerto tra il Ministro della Giustizia e quello degli Affari Esteri, una Commissione interministeriale, avente l'obiettivo di redigere uno schema di legge di ratifica – e dopo nel 2007 con la presentazione alle Camere del disegno di legge governativo, che recuperava una parte dei risultati a cui era giunta la precedente Commissione interministeriale: in pochissime sessioni venne approvato il testo in data 27 febbraio 2008, che non è andato esente da critiche[143]. Vi è, infatti, chi ritiene che si sia persa "un'occasione" per disciplinare in maniera organica la materia dei reati informatici, dato che la ratifica della Convenzione si è posta come un aggiornamento delle fattispecie esistenti, intervenendo in maniera settoriale e specifica su singole disposizioni, a seconda dell'esigenza di adeguamento della materia o di miglioramento[144]. La legge è intervenuta, introducendo diverse modifiche alle disposizioni penali in materia di reati informatici – concernenti le falsità informatiche, le certificazioni riguardanti la firma elettronica, le aggressioni alla sicurezza e integrità dei dati e dei sistemi – alla disciplina inerente alla responsabilità degli enti e alla disciplina processuale. Si noti come, con la legge di ratifica, si è resa effettiva la Convenzione, ma si segnala

[143] Per un approfondimento sull'iter normativo del D.D.L. AC n. 2807 si veda SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 631 ss., che procede dapprima ad esaminare l'*iter* che ha coinvolto la legge di ratifica, caratterizzata da un «andamento del tipo *stop and go*» e poi svolge un'attenta critica alle modalità con cui si è pervenuti alla legge – si evidenzia la frettolosità con cui si è giunti alla medesima nonostante la delicatezza della materia – nonché al suo contenuto. Ulteriori critiche sono state mosse da autorevole dottrina, che sottolinea come siano state approvate «norme con formulazioni delle cui "incongruenze" i parlamentari stessi si sono dichiarati consapevoli, salvo trincerarsi dietro l'auspicio che la magistratura le avrebbe sapute superare in sede interpretativa, essendo da tutti considerata preminente l'esigenza di non apportare modifiche che rallentassero od impedissero l'approvazione finale»: v. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 6/2008, 700 ss.

[144] Cfr. RESTA, Cybercrime *e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. merito*, 9/2008, 2149.

altresì l'introduzione di norme frutto di un'autonoma scelta del legislatore italiano, che ha così modificato talune disposizioni della disciplina previgente.

Le modifiche inerenti alla parte sostanziale riguardano il falso informatico di cui all'art. 491-*bis* c.p., la falsa dichiarazione o attestazione del certificatore di firma elettronica di cui all'art. 495-*bis* c.p., la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'art. 615-*quinquies* c.p., il danneggiamento informatico di cui agli artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies* c.p. con contestuali modifiche all'art. 420 c.p. e la frode informatica del soggetto che presta servizi di certificazione di firma elettronica di cui all'art. 640-*quinquies* c.p.

La prima disposizione oggetto di modifiche è stato l'art. 491-*bis* c.p., concernente l'applicazione della disciplina delle falsità documentali ai documenti informatici, introdotta con la legge 547/1993 per sanzionare le falsità riguardante i documenti informatici, mediante rinvio *per relationem* alle norme riguardanti le falsità di atti pubblici e scritture private. Con la modifica viene prevista l'applicabilità delle disposizioni riguardanti le falsità di atti pubblici o le scritture private a tutte quelle inerenti a documenti informatici pubblici o privati, avente efficacia probatoria; essa concerne, inoltre, l'abrogazione della seconda parte della disposizione, riguardante la definizione di documento informatico, intendendosi per tale "qualunque supporto contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli": tale nozione è stata ritenuta inadeguata, in quanto il riferimento al supporto sembrava attribuire rilevanza più che ai dati in sé al supporto materiale su cui erano impressi, senza tener conto che, oggi, si può discernere dal supporto materiale e senza chiarire, peraltro, il significato da attribuire all'efficacia probatoria[145], per cui la modifica è stata salutata con favore dalla dottrina.

La definizione di documento informatico può essere desunta, oggi, dall'art. 1, lett. p), d.lgs. 7 marzo 2005 n. 82, contenente il Codice dell'amministrazione digitale, secondo cui questo è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Permane il riferimento all'efficacia probatoria, che

[145] Così AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, Padova, 2010, 28 s.

secondo parte della dottrina «non dovrebbe essere inteso in chiave meramente processuale », ma «nel più ampio significato di funzione o rilevanza probatoria che assumono in concreto i dati ed i trattamenti informatici, rispondenti – nell'odierna società informatizzata – a quelle medesime esigenze di certezza ed affidamento nella "rappresentazione" (tramite atti, fatti e dati) dei rapporti rilevanti nel traffico giuridico, per cui meritano una protezione penale del tutto "equivalente" – non per questo identica – a quella apprestata ai documenti tradizionalmente intesi»[146].

La legge di ratifica ha introdotto l'art. 495-*bis*, rubricato "Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri" , che incrimina la condotta di chi dichiari o attesti falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona.

Un ulteriore intervento concerne l'art. 615-*quinquies*, diffusione di dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico, che ha rappresentato all'epoca della sua introduzione – avvenuta con la legge 547/1993 – una delle fattispecie più innovative create, in quanto la sua formulazione è stata svincolata da qualsivoglia modello esistente, andando anche oltre le previsioni della Raccomandazione (89) 9, nonostante le perplessità riguardanti la sua collocazione.

La legge di ratifica interviene mediante ampliamento dell'ambito oggettivo della fattispecie, che estende le condotte punibili anche al procacciamento, produzione, riproduzione, importazione, accanto alla già prevista diffusione, comunicazione, consegna, e aggiungendo una formula di chiusura in piena aderenza con le previsioni della Convenzione; inoltre in riferimento all'oggetto di queste condotte, concerne oggi non solo i programmi, ma anche le apparecchiature e i dispositivi, eliminando però ogni riferimento alla loro dannosità o pericolosità, e legando l'illiceità della condotta alla presenza di una finalità soggettiva in capo all'agente, che caratterizza come penalmente rilevante il fatto. Tale ultima modifica è stata criticata per il fatto di aver ancorato la rilevanza penale del fatto alla presenza del dolo specifico quale elemento soggettivo, vale a dire della volontà dell'agente

[146] V. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, Profili di diritto penale sostanziale*, cit., 704.

di "danneggiare illecitamente" eliminando l'elemento di tipicità dell'oggetto e deviando il contenuto della Convenzione, che mirava ad arricchire la qualificazione oggettiva del fatto[147].

Il più ampio intervento riguarda il settore del danneggiamento informatico: *in primis*, il legislatore ha modificato il regime di procedibilità dell'art. 635-*bis*, procedibile ora a querela della persona offesa, da individuare alla luce degli interessi giuridicamente rilevanti, modificando altresì le circostanze aggravanti e escludendo il riferimento ai sistemi informatici o telematici, diventati oggetto di un nuovo e più grave delitto; è stato infatti introdotto all'art. 635-*quater*, il danneggiamento di sistemi informatici o telematici, che si differenzia da quello summenzionato non solo per la diversità dell'oggetto materiale e per il più grave regime sanzionatorio, ma anche per la più incisiva descrizione del fatto tipico, che può essere posto in essere mediante le condotte di cui all'art. 635-*bis* e attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, condotte caratterizzate da uno degli eventi alternativi menzionati nella norma.

Il legislatore completa le disposizioni dirette a salvaguardare l'integrità dei dati e dei sistemi informatici, mediante l'introduzione all'interno del codice penale di due nuove fattispecie, l'art. 635-*ter* – riguardante il danneggiamento di dati di pubblica utilità – e l'art. 635-*quinquies* – concernente il danneggiamento di sistemi di pubblica utilità, con contestuale abrogazione del secondo e terzo comma dell'art. 420 c.p., data la sovrapposizione di questi commi con le due nuove fattispecie e da cui è emulata la struttura di delitti di attentato, a consumazione anticipata. Il legislatore ha così creato un microsistema normativo volto a punire le aggressioni informatiche in ogni sua forma, rafforzando la tutela dell'integrità dei dati e dei sistemi.

Diverse critiche sono state mosse da autorevole dottrina, che ritiene ingiustificato il riferimento a espressioni differenti per qualificare oggetti passivi aventi identica rilevanza pubblica – "informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità" da un lato e "sistemi informatici o telematici di pubblica utilità" dall'altro – nonché la previsione di distinti delitti non richiesti da fonti sovranazionali, quando sarebbe

[147] *Ivi*, 708 ss.

stato sufficiente prevedere una circostanza aggravante speciale ovvero la previsione di un'autonoma fattispecie, strutturata come delitto di evento, che non avrebbe generato una minor tutela, ma di converso garantito la punibilità di simili condotte anche a titolo di tentativo[148].

È stato previsto, infine, all'art. 640-*quinquies*, il delitto proprio del soggetto che presta servizi di certificazione di firma elettronica, il quale violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. La fattispecie è formulata con la tecnica del dolo specifico, essendo necessario che il soggetto agisca al fine di procurare a sé o ad altri un ingiusto profitto o di arrecare un danno.

Essa è stata criticata in quanto non sembrerebbe integrare una nuova figura di truffa, per la mancata presenza di connotazioni fraudolente – elemento caratterizzante le ipotesi truffaldine – e di connotati patrimoniali, consistendo nella mera violazione di obblighi *extra* penali, la cui condotta è sufficiente ad integrare il reato, qualora sia presente l'intento specifico del soggetto agente, mantenendosi pertanto, alla luce di queste considerazioni, lontana dal paradigma dei tipici delitti contro il patrimonio[149].

La legge di ratifica è intervenuta anche nel settore della responsabilità delle persone giuridiche, mediante l'introduzione dell'art. 24-*bis* al d.lgs. 231/2001 – disciplinante la materia – che ha ampliato la categoria dei reati presupposto, estendendo alla quasi totalità dei reati informatici la responsabilità da reato degli enti. In tal modo si è affiancata alla responsabilità penale del soggetto che materialmente pone in essere la condotta, la responsabilità amministrativa dell'ente per cui è predisposta una sanzione pecuniaria e interdittiva, a seconda della gravità del reato posto in essere.

Non si può far a meno di notare come, dal novero dei reati presupposto di cui al novello art. 24-*bis*, siano stati esclusi il delitto di frode informatica, di cui

---

[148] *Ivi*, 715 s.: con riferimento alla prima parte del periodo, secondo l'autore sarebbe stato sufficiente far riferimento alla formula generale "pubblica utilità" per indicare entrambi gli oggetti passivi – informazioni, dati o programmi e sistemi – essendo questa idonea ad abbracciare tutte le ipotesi menzionate; inoltre la configurazione delle due ipotesi criminose quali delitti di attentato non ha assicurato livelli sanzionatori più elevati rispetto alle ipotesi di danneggiamento afferenti ai dati o sistemi privati, non prevedendo così un regime sanzionatorio più severo.

[149] Così SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 652, il quale richiama il pensiero di autorevole dottrina: PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, Profili di diritto penale sostanziale*, cit., 706 s.

all'art. 640-*ter*, qualora il fatto non sia stato commesso in danno dello Stato o di altro ente pubblico, e il delitto di falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o qualità personali proprie o di altri, di cui all'art. 495-*bis*. Tale estromissione è stata considerata dalla dottrina come anomala, dato che tali reati si prestano ad essere commessi nell'interesse o a vantaggio di persone giuridiche, sia da parte di soggetti in posizione apicale, che da soggetti in posizione subordinata[150].

Per quanto attiene ai profili processuali, la legge è intervenuta modificando il codice di procedura penale nella parte relativa ai mezzi di ricerca della prova e alle indagini di polizia giudiziaria, dando indicazioni specifiche circa le modalità di esecuzione di ispezioni, perquisizioni e sequestri, nonché dettando regole circa la conservazione dei dati informatici e delle corrispondenti copie.

Come evidenziato da autorevole dottrina, il contributo della legge di ratifica ha inciso sulla disciplina probatoria e sull'attività di indagine indipendentemente dal fatto che il procedimento abbia ad oggetto un reato informatico, un reato comune commesso solo occasionalmente con mezzi informatici o un illecito estraneo al mondo tecnologico, «[...] essendo oramai innegabile il ruolo fondamentale che la *digital evidence* finisce coll'assumere pressoché in ogni inchiesta criminale [...][151]». In particolare, in tema di ispezioni informatiche, si prescrive, in relazione a sistemi informatici o telematici, l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati ed impedirne l'alterazione, senza disporre le misure da adottare nello specifico, così adottando le tecniche migliori secondo l'evoluzione scientifica. In tal modo viene riconosciuta la volatilità dal dato digitale, per cui è necessario adottare tecniche che ne riescano ad assicurare la genuinità.

In tema di perquisizioni, è stato previsto che qualora vi sia fondato motivo di ritenere che dati informatici siano contenuti in un sistema informatico o telematico ne è disposta la perquisizione, adottato le misure tecniche necessarie a

---

[150] Si veda CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 50 s.; PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, Profili di diritto penale sostanziale*, cit., 716; SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 658.

[151] Così LUPÁRIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, I Profili processuali*, in *Dir. pen. proc.*, 6/2008, 717 ss.

garantirne la conservazione. È stata prevista la possibilità di sequestro di dati informatici, presso i fornitori di servizi informatici, telematici e di telecomunicazioni, prevedendo così un onere di collaborazione e stabilendo che l'acquisizione avvenga mediante copia degli stessi su adeguato supporto, con una procedura che sia idonea a stabilirne la conformità agli originali, nonché la loro immodificabilità. Sempre in tema di sequestro, è stata disposta la possibilità di sequestrare oggetti di corrispondenza, anche se inoltrati per via telematica.

In tema di indagini, si prevede la possibilità per gli ufficiali della polizia giudiziaria di procedere alla perquisizione di sistemi informatici o telematici, adottando le dovute misure tecniche, quando hanno fondato motivo di ritenere che vi si trovino occultati dati informatici o comunque tracce pertinenti al reato che potrebbero andare disperse. È disposto, inoltre, che gli ufficiali della polizia giudiziaria adottino le misure tecniche necessarie, nonché impartiscano le prescrizioni necessarie al fine di assicurare la conservazione e impedire l'alterazione di dati, informazioni, programmi informatici e di sistemi informatici o telematici; è prevista altresì l'immediata duplicazione, ove possibile, su adeguati supporti, garantendo in tal modo che l'oggetto di indagine non venga alterato dallo svolgimento delle operazioni[152].

La legge interviene, altresì, sul codice in materia di protezione dei dati personali, imponendo determinati obblighi, volti alla conservazione dei dati di traffico, in capo ai fornitori di servizi informatici. Altra modifica processuale rilevante riguarda il tema della competenza investigativa sui reati informatici, che viene attribuita alle procure distrettuali, con l'intento di favorire il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati.

Da tale analisi si evince che il presente intervento normativo è frutto di un urgente bisogno di regolamentazione di un settore, che avrebbe necessitato di maggior approfondimento e qualità tecnica, in virtù della finalità di armonizzare le legislazioni degli Stati. Si noti come la normativa in esame non abbia predisposto alcuna disposizione definitoria, che recepisse le nozioni basilari contenute nell'art. 1 della Convenzione e non abbia altresì tenuto conto della Decisione quadro

[152] Legge 18 marzo 2008, n. 48 artt. 8-11. Per una completa analisi si legga LUPÁRIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa*, cit., 717 ss.

dell'Unione europea 2005/222/GAI, contro gli attacchi informatici, che aveva ad oggetto norme minime di coordinamento sul piano del diritto sostanziale. Essa, nonostante le critiche, ha il merito di aver approfondito e consolidato il rapporto tra natura giuridica del reato informatico e specialità dell'investigazione digitale, rendendo più stringente «l'interazione tra norme penali incriminatrici di parte speciale e istituti processuali, ratificando il ricorso agli strumenti operativi che si andavano affermando nella prassi giudiziaria e nelle aule dei tribunali, unitamente ad un più moderno e consapevole approccio alle problematiche afferenti l'informatica forense»[153].

La *ratio* sottesa alla legge di ratifica è stata quella di proporre un modello di contrasto alla criminalità informatica uniforme nell'area dei Paesi membri della Convenzione e in quanto tale rappresenta solo il primo passo avverso questo nuovo fenomeno, che evidenzia le trasformazioni inerenti ai rapporti sociali nella realtà odierna, di cui «il *Cyberspace* rappresenta solo l'emblema»[154].

5. La prevenzione come risposta alla criminalità informatica: la *cybersecurity*

Il costante aumento della sofisticatezza della criminalità informatica e dei relativi attacchi hanno fatto sorgere l'esigenza di predisporre, accanto agli strumenti repressivi, misure atte a prevenire questo dilagante fenomeno. Difatti, le misure puramente repressive non bastano a reprimere le condotte dei criminali informatici, date anche le difficoltà correlate alla perseguibilità, nonché all'individuazione di tali agenti. I rilevanti danni che ne conseguono si sostanziano non solo nella compromissione e alterazione di dati sensibili, ma anche nell'incidenza sul regolare funzionamento delle infrastrutture critiche, che di conseguenza determina un impatto negativo ingente per le funzioni vitali della società. Da qui nasce la necessità di adottare un quadro di misure fondate sulla sicurezza delle reti e dei sistemi informatici, improntate su meccanismi preventivi e di cooperazione tra le varie autorità coinvolte nel contrasto agli attacchi informatici.

---

[153] Cfr. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in LUPÁRIA (a cura di), *Sistema penale e criminalità informatica, Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 Marzo 2008, n. 48)*, Milano, 2009, 183 s.

[154] Così PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. dell'Internet*, 5/2008, 448.

Non esiste una definizione univoca del concetto, ma tendenzialmente si ritiene che questa consista nella capacità di proteggere il *cyberspace*, ed in particolare gli *asset* fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce informatiche.

Da questa breve premessa muove l'importanza della *cybersecurity*, «che rappresenta la risposta politica, economica, e normativa agli attacchi realizzati nello spazio virtuale, anche in termini di valutazione e gestione del rischio informatico»[155]. Numerose sono le iniziative che si annoverano a livello nazionale e sovranazionale, volte a incrementare lo standard di sicurezza, gestire il rischio e ridurre la vulnerabilità dei sistemi informatici.

Tra i primi interventi in materia, si registra una comunicazione sulla criminalità informatica adottata dalla Commissione, concernente la sicurezza delle infrastrutture dell'informazione e la repressione dei reati informatici, integrata successivamente dalla comunicazione sulla sicurezza delle reti e sicurezza dell'informazione che dopo aver dato una definizione di tale concetto – «[...] va pertanto intesa come la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema»[156] – tipizza le diverse minacce che compromettono la sicurezza delle reti[157].

Data la crescente digitalizzazione dei sistemi, l'attenzione della Comunità per la sicurezza cibernetica si è esternato ulteriormente tramite l'adozione di altre due comunicazioni – *eEurope* ed *eEurope* 2005 – nell'ottica della competitività e dinamismo del mercato, mediante un'apposita strategia, tesa ad aggiornare i servizi resi dalle infrastrutture di rete e facilitare l'accesso alla rete[158]. Altre misure, negli anni successivi, imponevano agli Stati membri di adottare misure a livello nazionale che garantissero la sicurezza delle reti.

---

[155] V. SEVERINO, *Standard globali in difesa della trasformazione digitale*, in *www.ilsole24ore.com*, 29 marzo 2019.

[156] Cfr. COM (2001) 298 del 6 Giugno 2001, 9.

[157] In argomento MENSI, *La sicurezza cibernetica*, in MENSI, FALLETTA, *Il diritto del* web, Padova, 2018, 286.

[158] *Ivi*, 287.

Un passo avanti è stato compiuto con l'istituzione dell'ENISA, l'Agenzia europea per la sicurezza delle reti e dell'informazione, nel 2004, che rappresenta il centro di sviluppo per la materia della sicurezza informatica tra gli Stati membri, con il compito di aiutare questi ultimi nella prevenzione, nonché reazione ai problemi di sicurezza delle reti, e di fornire consigli pratici e soluzioni per il settore pubblico e privato negli Stati membri e per le istituzioni dell'Unione Europea. L'istituzione di tale organismo permette di assicurare un elevato livello di sicurezza, di sviluppare e promuovere una cultura in materia di sicurezza delle reti, così assicurando un corretto funzionamento del mercato interno[159].

Relativamente ad essa e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, da ultimo si registra il Regolamento 2019/881/UE, avente l'obiettivo di realizzare un quadro europeo per la certificazione della sicurezza informatica delle ICT, che permetta di facilitare lo scambio dei prodotti e dei servizi digitali nell'Unione, aumentando così l'affidabilità degli stessi con la fissazione di standard di sicurezza condivisi. Il regolamento affida un ruolo di primo piano all'ENISA, ridisegnando la struttura e attribuendole diversi compiti, tra cui quello di predisporre gli schemi europei di certificazione per le tecnologie dell'informazione e della comunicazione, nonché dei servizi digitali. Viene istituito il quadro europeo di certificazione della cibersicurezza, che prevede un meccanismo inteso a stabilire sistemi europei competenti e ad attestare che i prodotti siano conformi a determinati requisiti al fine di proteggere la disponibilità, integrità e riservatezza dei dati conservati, trasmessi o trattati[160].

Tra gli importanti interventi, si annovera la Comunicazione della Commissione relativa a un programma europeo per la protezione delle infrastrutture critiche COM/2006/0786, con l'obiettivo di migliorare la protezione delle infrastrutture critiche nell'UE, mediante la creazione di un quadro UE per la

[159] Per un approfondimento si veda il Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013 , relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004, via *www.eur-lex.europa.eu*. Il suddetto Regolamento sulla cibersicurezza è stato abrogato dal Regolamento (UE) 2019/881, relativo all'ENISA e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

[160] In tal senso PANATTONI, Compliance, cybersecurity *e sicurezza*, cit., 13 s.

protezione delle infrastrutture critiche: esso sarà realizzato con l'istituzione di un gruppo di contatto che coordini le questioni legate alla protezione delle infrastrutture critiche, che vengono individuate in quelle che rivestono una rilevante importanza per la Comunità, il cui danneggiamento avrebbe un impatto su due o più Stati membri; nonché conferendo misure di sostegno alle infrastrutture critiche nazionali, che potrebbero essere utilizzate dagli Stati membri[161]. Sempre in tema di protezione di infrastrutture, si ricordi la Direttiva del Consiglio – CE/2008/114 – relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione: in particolare, essa si riferisce ai settori dell'energia e dei trasporti, denotati come settori di maggior criticità, in cui si potrebbe ricomprendere il settore delle ICT. Le infrastrutture critiche vengono individuate in un elemento o sistema, facente parte di uno degli Stati membri, che riveste una funzione essenziale per la tenuta dei rapporti sociali, nonché per la sicurezza, il cui danneggiamento avrebbe un impatto significativo rilevante[162].

Nel corso degli anni sono poi stati varati ulteriori provvedimenti, tra cui si inserisce nel 2013 l'istituzione dell'*European Cybercrime Centre* in seno all'Europol, volto ad assistere gli Stati membri e i privati nel contrasto al crimine e alle minacce derivanti dal *cyberspace*.

Da queste breve disamina, si può evincere come il *trend* legislativo sia quello di adottare tutte le misure ritenute necessarie per il contrasto alla criminalità informatica, dato che tale settore riveste sempre più importanza nella società odierna: esso si traduce nell'emanazione di misure volte a salvaguardare l'integrità, la confidenzialità e la disponibilità delle informazioni. Tale obiettivo si esplica anche mediante la partecipazione del privato, che permette di attribuire efficace protezione ai beni giuridici minacciati dal *cybercrime*.

Le principali regolazioni in merito sono state varate nel 2016, con l'emanazione del Regolamento 679/2016/UE – in materia di *privacy* – e della Direttiva 1148/2016/UE, nota come Direttiva NIS. Quest'ultima rappresenta il pilastro della strategia europea in tema di cybersicurezza, il cui obiettivo è emanare

[161] Comunicazione della Commissione relativa a un programma europeo per la protezione delle infrastrutture critiche COM/2006/0786.

[162] Cfr. Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008, art. 2.

le misure necessarie volte a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, tra cui si rinviene l'obbligo per gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, che evidenzia come sia di rilievo il tema della *governance* del rischio cibernetico[163]. Essa si rivolge agli operatori di servizi essenziali e ai fornitori di servizi digitali, i quali operano in determinati settori ritenuti essenziali per le funzioni vitali della società e a cui vengono imposti obblighi di sicurezza e di notifica, si verifichino eventi pregiudizievoli per la sicurezza della rete e dei sistemi informativi.

Secondo la Direttiva in esame, ogni Stato membro è tenuto a designare delle autorità competenti in materia di sicurezza delle reti e dei sistemi informativi, che controllino l'applicazione della direttiva; inoltre, designa uno o più gruppi di intervento per la sicurezza informatica in caso di incidente – CSIRT – avente il compito di trattare gli incidenti e i rischi mediante una procedura definita. Essa prevede poi che gli Stati membri stabiliscano le norme inerenti alle sanzioni da applicare, in caso di violazione delle disposizioni presenti nella direttiva.

La direttiva NIS costituisce la pietra miliare nel settore della sicurezza cibernetica, andando a promuovere una cultura della sicurezza e della gestione del rischio, nonché di segnalazione degli incidenti, in quei settori di particolare rilievo per la società e mettendo in luce come sia essenziale la cooperazione e una disciplina armonizzata per il raggiungimento di questo scopo. Essa è stata attuata, a livello nazionale, con il decreto legislativo del 18 maggio 2018, n. 65, attraverso cui vi è stato il recepimento delle definizioni rilevanti della direttiva, l'individuazione delle autorità NIS e l'adozione della strategia nazionale di sicurezza cibernetica, nonché l'adozione di norme sanzionatorie volte ad incriminare la violazione degli obblighi imposti dal decreto[164].

La sicurezza delle reti è lo strumento essenziale di prevenzione alla criminalità informatica e, a tal fine, tra gli importanti interventi, si annovera la legge

[163] V. Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[164] Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

del 18 novembre 2019, n. 133[165], che istituisce il perimetro di sicurezza nazionale cibernetica, nascente dalla necessità di sviluppare un elevato livello di sicurezza delle reti e dei sistemi informativi da cui dipende lo svolgimento di una funzione essenziale per il paese: si sostanzia nell'individuazione dei soggetti inclusi nel perimetro, che vengono considerati critici in virtù delle rilevanti funzioni rivestite e il cui danneggiamento avrebbe un impatto rilevante per la società, per cui esigono un alto grado di sicurezza.

Come si evince, sia a livello europeo che a livello nazionale, risulta imprescindibile adottare un approccio strategico in tale settore, mediante un'accurata analisi del rischio, con un atteggiamento improntato nell'ottica della prevenzione, che preveda l'istituzione di misure di sicurezza, che permettano di scongiurare gli attacchi da parte dei criminali informatici. Fondamentale risulta, pertanto, la cooperazione tra soggetti pubblici e privati, resa necessaria dalla gestione da parte dei privati di alcune infrastrutture critiche, a cui si richiede l'adozione di fonti di autoregolazione interne, che sottolineano l'importanza della *compliance*, che incidono sulla stessa portata delle norme penali e che permettono di stare al passo con l'evoluzione e il dinamismo dello spazio virtuale in quanto maggiormente flessibili. Si richiede ai privati uno stretto contatto con le autorità di contrasto, a cui segnalare le informazioni riguardanti incidenti rilevanti, per cui viene istituito il CSIRT nazionale – *Computer Security Response Team* – che assume un ruolo cardine nell'attività di contrasto e di analisi degli incidenti segnalati.

La prevenzione si è rivelata lo strumento più efficace nella lotta al crimine informatico, in quanto consente di scongiurare le minacce informatiche alla fonte, nonché di sensibilizzare gli attori operanti nei settori nevralgici della sicurezza, dato che l'efficacia dei meccanismi di contrasto tradizionali sono messi a dura prova dalle peculiari caratteristiche della realtà digitale.

6. Le caratteristiche principali del fenomeno: la desensibilizzazione e l'aterritorialità

[165] Legge 18 novembre 2019, n. 133, Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

Lo sviluppo della Rete ha innovato il modo di intendere i rapporti sociali, caratterizzati oggi dalla rapidità dei collegamenti, contribuendo alla qualità della vita, anche in termini di diffusione del sapere. L'accesso libero alla rete ha permesso ai soggetti di socializzare, conoscere ed essere informati, contribuendo alla massima esplicazione di taluni diritti costituzionali, che trovano in rete un connubio perfetto: oggi, si assiste alla trasposizione della realtà in una nuova dimensione, quella virtuale, in cui si rinvengono tutte le forme dell'agire umano, in modalità inedite che porta ad un nuovo modo di intendere dei concetti tradizionali. Eppure, non possono essere sottaciute le problematiche che la diffusione della realtà digitale porta con sé, tutte derivanti da quelle caratteristiche che i criminali informatici hanno declinato a proprio favore.

Innanzitutto, si può affermare che gli attori delle dinamiche criminose sono portati a ritenere che i comportamenti devianti perpetrati *online* non produrranno effetti al di là della dimensione virtuale del *cyberspace*, attenuando la comprensione dei reali effetti negativi della propria azione e rafforzando così il sentimento di impunità con la conseguente perdita di fattori inibitori, che potrebbe incoraggiare la reiterazione delle condotte illecite. La condotta *online* modifica i processi cognitivi nella dinamica criminosa, in quanto il mezzo informatico si inserisce tra il reo e la vittima, influenzando così l'*iter* criminoso: si evince un forte sentimento di sicurezza legato al presunto anonimato che viene fornito dal *web*, nonché legato alla sensazione della bassa probabilità che il fatto venga sanzionato[166]. Aumentano così gli illeciti di stampo tradizionale commessi *online*, come pure reati singolari che trovano nel mezzo informatico il solo strumento di perpetrazione.

Queste peculiarità portano ad una desensibilizzazione dell'agente, che attenua la reale comprensione dei crimini, andando a rendere impercettibile la soglia tra ciò che è lecito e ciò che invece non lo è: il reo percepisce la condotta posta in essere come meno grave rispetto alla commissione di un reato "tradizionale", in quanto generalmente lo spazio virtuale è considerato un luogo privo di regole e confini, nonché per via della lontananza rispetto alla vittima. Questa riflessione non deve portare però alla considerazione che la rete sia un luogo troppo pericoloso per l'esplicazione della personalità umana, in quanto tale

[166] In tal senso BALLONI, BISI, SETTE, *Principi di criminologia applicata*, cit., 271 s.

strumento è essenziale per lo sviluppo sociale, anzi ciò deve contribuire a coltivare la volontà di prevenire e contrastare i comportamenti devianti, ivi perpetrati.

Un'altra delle caratteristiche salienti della criminalità informatica si rinviene nella aterritorialità delle Rete, la quale travalica i confini spazio-temporali. La Rete ignora i confini degli ordinamenti, che invece necessitano di un luogo sul quale esercitare la propria sovranità e, essendo priva di confini, non si può operare una sua limitazione a livello territoriale. Difatti, le condotte poste in essere nel cyberspazio sono difficilmente localizzabili, in quanto potendo essere realizzate a distanza, producono effetti oltre il territorio del singolo paese e al tempo stesso pare complesso selezionare il luogo e il momento in cui le condotte possono considerarsi realizzate: accade sovente che il soggetto attivo pone in essere il comportamento deviante in un determinato luogo, ma le conseguenze si esplicheranno a danno di un sistema informatico, locato in un sito diverso[167].

L'individuazione della collocazione spaziale del soggetto risulta difficile anche per la possibilità di poter scegliere un *server* lontano dal luogo in cui viene perpetrata l'azione. Si tratta di illeciti aterritoriali e transnazionali, la cui commissione è resa possibile anche dalle difficoltà di individuazione dei soggetti responsabili e dalle difficoltà nel controllo sui traffici di dati *online*. Ciò rende complessa l'individuazione del *locus commissi delicti* e di conseguenza pone problemi nell'individuazione della giurisdizione competente, proprio a causa della struttura delocalizzata della rete, che si riversa anche sulle difficoltà di coordinamento tra le svariate norme dei diversi ordinamenti. Tale caratteristica ha portato gli interpreti ad interrogarsi sul fenomeno dei reati commessi via *web* e delle relative conseguenze in ordine al luogo del commesso reato, partendo dai principi cardine dell'ordinamento penale (v. *infra* cap. II).

Queste peculiarità costituiscono un terreno fertile per la criminalità informatica e ne hanno contribuito la proliferazione, giovandosi delle varie modalità di realizzazione della condotta, che al tempo stesso può essere commessa facilmente, data l'elevata diffusività dei sistemi e della rete – caratterizzata dal libero accesso – e giovandosi della mancata uniformità normativa, motivo per cui

[167] In argomento CASSANO, SCORZA, VACIAGO (a cura di), *Diritto dell'Internet. Manuale operativo: casi, legislazione e giurisprudenza*, Padova, 2012, 551 ss.

si richiede un elevato tasso di cooperazione, che risulta essenziale alla luce del carattere transnazionale degli illeciti.

CAPITOLO II

L'INDIVIDUAZIONE DEL *LOCUS COMMISSI DELICTI*

SOMMARIO: 1. La consumazione del reato. – 2. Il *locus commissi delicti*. – 2.1 Profili sostanziali. – 2.2 Profili procedurali. – 3. I limiti del principio di territorialità nel *cyberspace*. – 3.1 Il principio della personalità attiva e passiva: il modesto riconoscimento nel contesto nazionale. – 4. I problemi giuridici relativi ai reati informatici. – 5. Gli approdi giurisprudenziali. – 6. Le linee evolutive.

1. La consumazione del reato

Ogni reato ha una propria collocazione spazio-temporale dalla quale scaturiscono determinati effetti inerenti alla successione di leggi nel tempo, alla legge territorialmente applicabile, nonché alla prescrizione del reato.

Nel dettaglio, il codice penale italiano non conferisce una definizione giuridica diretta di consumazione, ma richiama in molteplici disposizioni tale concetto. Esso è molto spesso contrapposto al delitto tentato per cui, secondo parte della dottrina italiana, potrebbe desumersi indirettamente l'accezione che il legislatore ha inteso attribuire alla nozione di "consumazione": «un reato si dice consumato quando nel caso concreto si sono verificati tutti gli estremi del fatto descritto nella norma incriminatrice»[1]; pertanto si potrebbe evincere che, al verificarsi di tutti gli estremi del fatto, quindi l'integrazione della fattispecie, corrisponda il momento conclusivo della violazione.

Alla luce di tale premessa, emerge che il legislatore italiano ha accolto una teoria formale della consumazione, che indica quel momento in cui, avendosi una perfetta aderenza tra il fatto e lo schema normativo, la sanzione prevista dalla norma incriminatrice diviene applicabile; questa teoria è contrapposta a quella materiale, che individua la consumazione nel momento in cui si completa la concreta azione criminosa: tali nozioni non sono tra loro antitetiche, ben potendo coincidere la consumazione sia nel caso di teoria formale che materiale[2].

Inizialmente, il noto studioso criminalista Carmignani riteneva che alla consumazione non dovesse essere conferita una nozione astratta e generica, ma

[1] V. MARINUCCI, DOLCINI, *Manuale di Diritto Penale. Parte Generale*, Milano, 2017, 260.

[2] Cfr. BRASCHI, *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Padova, 2020, 4.

dovesse essere individuata in base alla singola fattispecie di reato, tuttavia tale concezione fu accantonata in vista di una prima definizione derivante dalla legislazione tedesca. Difatti, la prima definizione di reato consumato risale alla metà del XIX secolo, all'interno del Codice per il Granducato di Toscana, in cui si riteneva consumato un reato quando tutti gli elementi che ne costituiscono tratti essenziali trovano corrispondenza nel fatto criminoso. È in questo periodo, ed in particolare agli inizi del Novecento, che si ascrivono i primi studi riguardo la consumazione e la relativa affermazione della teoria formale. Sebbene, infatti, la nozione così delineata non scaturì molto successo, la dottrina classificava le diverse fattispecie criminose in base al momento consumativo, ponendo una distinzione tra delitti formali e materiali, riferendosi i primi a tutti quelli che presuppongono una data di azione – i quali generalmente sono caratterizzati dal fatto che la condotta si protrae oltre il momento di integrazione della violazione – e i secondi invece un dato successo[3].

Successivamente, fa breccia nella dottrina la teoria dell'esaurimento, con cui il suo portavoce, Carrara, opera una distinzione tra perfezione e esaurimento, attribuendo alla prima nozione la capacità di individuare il momento in cui il reato si ritiene consumato, vale a dire il momento in cui avviene l'aggressione all'oggettività giuridica tutelata; si riferisce, invece, all'esaurimento, quando viene raggiunto il fine perseguito dal reo, in grado di determinare una nuova fase dell'*iter criminis*, in altre parole quando, dopo la perfezione, si siano prodotti anche tutti gli effetti dannosi a cui mirava l'agente. Tale teoria, sebbene adotti criteri ambigui per l'individuazione del momento consumativo, ha il merito di aver distinto per la prima volta tra perfezione e momento conclusivo del reato, riconoscendo la presenza di una fase successiva alla consumazione.

Passando poi ad analizzare la prima codificazione post-unitaria, il Codice Zanardelli del 1889, si può notare come quest'ultimo abbia rinunciato a fornire una definizione astratta di consumazione, a cui peraltro fanno riferimento ulteriori disposizioni disseminate nel codice, come quella inerente alla prescrizione; si può constatare, inoltre, come il suddetto codice non abbia recepito la teoria dell'esaurimento, sebbene non abbia ignorato i problemi inerenti al prolungamento

[3] *Ivi*, 50 ss.

della violazione, specialmente in riferimento alla prescrizione[4]. Tale teoria veniva considerata in un'accezione soggettiva dalla dottrina del tempo, che riteneva il comportamento *post-delictum* un indice per la pericolosità del reo.

Agli inizi del Novecento, si ha l'abbandono della teoria della consumazione materiale o esaurimento, per abbracciare un approccio metodologico, portato avanti dallo studioso Rocco, il quale individua la nozione di consumazione nel risultato dannoso o pericoloso, dalla cui verificazione la legge fa dipendere la consumazione o perfezione del reato e da cui dipende l'applicabilità della sanzione.

Il codice Rocco si pone in linea di continuità con il precedente codice e attua innanzitutto una distinzione, come risulta dai lavori preparatori, tra "commissione" e "consumazione", intendendosi la prima come comprensiva di tutte le fasi dell'*iter criminis* giuridicamente rilevanti, ricomprendendo così sia l'ipotesi del reato consumato che tentato; mentre alla consumazione viene attribuito un significato più circoscritto, che non viene giuridicamente esplicitato, in quanto l'individuazione del momento consumativo è un'analisi da compiere in riferimento alle singole ipotesi di reato. Importante al riguardo è la previsione della forma del reato permanente, che riguarda le ipotesi in cui vi è un prolungamento del periodo consumativo, che si conclude con il cessare della permanenza: tale forma di esplicazione dell'illecito ha contribuito a far affermare la teoria formale[5].

Nella dottrina codicistica, della seconda metà del XX secolo, si sono affermate due contrapposte visioni del momento consumativo: la prima, espressione della concezione formale, considera la nozione di consumazione in modo unitario, negando una distinzione tra perfezione e consumazione e circoscrivendo il prolungamento della violazione ai soli reati di durata e ricorrendo per questi ultimi alla teoria del periodo consumativo, per cui la determinazione del momento consumativo si riferisce a tutta la durata della permanenza; la più recente dottrina distingue la perfezione del reato, che si identifica nel momento in cui sono integrati tutti i requisiti richiesti dalla fattispecie, dalla consumazione, che

[4] *Ivi*, 80.

[5] Per un'approfondita analisi storica sull'argomento si veda BRASCHI, *La consumazione del reato*, cit., 33 ss.

corrisponde, invece, al punto in cui il reato perfetto raggiunge la sua massima gravità[6].

Non si può non constatare come negli illeciti di durata non si possa far riferimento ad un'unica nozione di consumazione, ma occorra distinguere tra il momento in cui l'illecito si può dire integrato e quando esso è effettivamente concluso, potendosi avere altrimenti solamente la categoria dei reati istantanei. È accolto, pertanto, l'orientamento che distingue tra perfezione e consumazione, la quale può coincidere ovvero succedere alla perfezione. In particolare, si ha una dissociazione tra perfezione e consumazione tutte quelle volte in cui si è dinnanzi a illeciti di durata.

Analizzando nel dettaglio il binomio perfezione-consumazione, si asserisce che la perfezione indichi il momento in cui la fattispecie è integrata e la sanzione diviene applicabile. Per quanto attiene alla definizione di consumazione bisogna considerare che un suo concetto generale non può essere riscontrato, per via delle diversità che concernono le singole fattispecie, per cui l'indagine sull'individuazione di questa nozione va compiuta in riferimento alla struttura delle singole ipotesi incriminatrici. Non può essere accolto neppure l'assunto che individua la consumazione nel finalismo dell'azione criminosa, che risulta incompatibile con le fattispecie colpose[7]. Essa va piuttosto intesa – e ricercata – secondo la dottrina maggioritaria odierna, come massimo grado di realizzazione della fattispecie, vale a dire quando il reato raggiunge la massima gravità, in accordo con il principio di offensività[8].

Il nostro ordinamento, come anticipato (v. *supra* Cap. II, § 1), non fa espresso riferimento alla nozione di consumazione, ma si riferisce al reato consumato all'art. 158 c.p. al fine di fissare il momento in cui decorre la prescrizione e all'art. 8 c.p.p. attinente alla competenza territoriale, da cui emerge come questo attenga ad un momento in cui l'offesa al bene ha raggiunto la massima gravità, dato che «non avrebbe senso far decorrere il termine di prescrizione da un momento in cui l'offesa tipica non ha ancora raggiunto il suo culmine»[9].

---

[6] Orientamento seguito da MANTOVANI, *Diritto penale, parte generale*, Padova, 2017, 425.
[7] V. BRASCHI, *La consumazione del reato*, cit., 243.
[8] *Ivi*, 242 ss.
[9] Così PAGLIARO, *Tempus commissi delicti*, in *Enciclopedia del diritto*, 1992, XLIV.

Da questa conclusione, deriva la necessità per l'interprete di analizzare le ipotesi di reato per individuare il momento consumativo, non rinvenendosi un concetto generale dello stesso. È il caso quindi di operare una distinzione tra i reati istantanei e i reati permanenti: i primi si identificano in quei reati in cui il momento consumativo coincide con l'ultimo degli atti posti in essere al fine di integrare la condotta tipica, vale a dire che la realizzazione della condotta è in grado anche di integrare l'offesa al bene giuridico tutelato dalla norma incriminatrice; i reati permanenti, invece, si sostanziano in quei reati in cui vi è il protrarsi della situazione antigiuridica, circostanza che determina una distonia tra perfezione, che si ha nel momento in cui si pone in essere la condotta ed eventualmente si verifica l'evento, e la consumazione, che si ha solamente quando termina la situazione antigiuridica.

Da questi vanno tenuti distinti i reati abituali e il reato continuato, che pure registrano una dissonanza tra perfezione e consumazione: con la prima espressione ci si riferisce a quei reati che si sostanziano nella reiterazione di una serie di azioni od omissioni, idonee ad integrare l'ipotesi di reato, per cui la consumazione si avrà con l'ultimo degli atti che integrano il fatto costitutivo; il reato continuato si caratterizza, invece, per la commissione di una serie di reati diversi, uniti dall'intento di realizzare un unico disegno criminoso, per cui per ciascuno dei reati occorrerà individuare il tempo di commissione del reato.

Queste considerazioni implicano delle conseguenze, strettamente collegate al momento consumativo, che coinvolgono l'istituto della prescrizione – che nel caso di reato permanente decorre dal momento in cui cessa la permanenza e quindi si conclude l'*iter criminis* – il concorso di persone – che in caso di dissociazione tra perfezione e consumazione può avvenire anche dopo la perfezione – la legge del tempo del commesso reato – che nel caso di reato permanente è individuata in quella vigente all'inizio e entrata in vigore nel tempo intercorrente tra la perfezione e la consumazione – la competenza territoriale – per cui è competente il giudice del luogo in cui si è perfezionato l'illecito.

Le conclusioni a cui si è giunti riguardano sicuramente il diritto penale tradizionale, ma possono porre dei problemi in riferimento ai nuovi reati cibernetici, i quali connotano in modo diverso i classici concetti di azione ed evento, *res* che non permette di delineare a *priori* la dinamica di questa tipologia di illecito, e rende

complicato individuare i confini temporali, nonché la connotazione spaziale del reato perpetrato nel *cyberspace*, da cui muove la tendenza ad adottare nozioni di consumazione modellate sulle singole incriminazioni.

2. Il *locus commissi delicti*

Ogni ordinamento giuridico deve istituire dei limiti di efficacia alla propria esplicazione sia a livello temporale che territoriale, in modo tale da individuare la fattispecie criminosa nello spazio e nel tempo. L'individuazione del *locus commissi delicti* pone dei problemi sia dal punto di vista sostanziale che processuale. Bisogna considerare che tale questione non concerne solamente l'individuazione del giudice competente, ma attiene alla stessa rilevanza penale del fatto – nel caso in cui la condotta sia punita penalmente esclusivamente in Italia, ne scaturirebbe la conseguenza che se si escludesse l'applicazione della legge italiana, il fatto resterebbe impunito – ed è volto a dirimere contrasti giurisdizionali.

Storicamente il legislatore italiano ha abbracciato il principio di territorialità, che permette di istituire un collegamento tra il fatto e l'ordinamento giuridico in cui lo stesso è commesso, applicando la legge penale ai fatti commessi nel territorio dello Stato. Fin dalla vigenza del codice Zanardelli, si rendeva esplicito tale principio, ponendo però il problema della disciplina giuridica da applicare nel caso di reati commessi solo in parte nei confini nazionali. Tale questione, da cui potevano sorgere potenziali conflitti di giurisdizione, fu risolta attraverso l'adozione del criterio di verificazione dell'illecito, ossia adottando la competenza dell'ordinamento nel quale si compì il delitto, mentre la giurisprudenza del tempo tentò di legittimare l'applicazione della legge penale anche per fatti avvenuti solo in parte sul suolo italiano[10].

Il legislatore del 1930 ha codificato, dunque, le soluzioni giurisprudenziali avanzate, rievocando all'art. 6 co. 2 c.p. tali concetti. Gradualmente si è andato affermando il principio di universalità, mediante il conferimento di una nozione di "reato commesso nel territorio dello Stato" molto ampia e attraverso la previsione dell'applicabilità della legge italiana anche a condotte commesse interamente

[10] In argomento PETRINI, *La responsabilità penale per i reati via internet*, Napoli, 2004, 214 ss.

all'estero. Difatti, con il principio di universalità si determina l'applicazione della legge penale a condotte considerate illecite dall'ordinamento, commesse da qualunque uomo, in qualunque luogo si trovi. Tale principio corrisponde all'intento di estendere al massimo l'efficacia della legge penale italiana nello spazio, in accordo con l'ideologia del tempo. A ben vedere, però, già nel codice del 1889, era prevista l'applicabilità della legge italiana, a determinate condizioni, a fatti commessi all'estero dallo straniero ai danni di uno straniero, per cui si evince una sostanziale continuità nel codice Rocco con la precedente codicistica liberale, i cui elementi di novità si rinvengono nella previsione di speciali casi, stabiliti dalla legge ovvero da convenzioni internazionali, in cui si determina l'applicazione della legge italiana a fatti commessi interamente all'estero[11]. Con il codice Rocco si è pertanto avuta una evoluzione dei principi summenzionati, temperati insieme tra loro. Accanto ad essi si annoverano, poi, il principio della personalità attiva e il principio della personalità passiva o della difesa, i quali attengono alla validità della legge penale rispetto alle persone: il primo principio indica che ad un soggetto che commette un reato vada applicata la legge dello Stato cui appartiene; il principio della difesa stabilisce che l'individuazione della legge applicabile avvenga in funzione della nazionalità del soggetto passivo.

Si evince come l'individuazione dei limiti di operatività all'applicabilità della legge penale nello spazio possa avvenire mediante la combinazione di tradizionali principi, quali quello di territorialità, universalità, personalità attiva e personalità passiva, da tempo avanzati dalla dottrina penalistica, che non vanno considerati nel senso puro dei termini, ma temperati tra loro, in quanto una rigida applicazione del principio di territorialità determinerebbe una carenza di tutela per quelle situazioni che, per la gravità dei fatti o per la nazionalità della vittima, non andrebbero lasciate esenti da incriminazione; e allo stesso modo una rigida applicazione del principio di universalità rischierebbe di rendere inefficace il sistema.

Appare utile sottolineare che in dottrina, al fine di individuare il *locus commissi delicti*, si richiamano tre teorie: la prima della condotta, secondo cui il reato si intende commesso nel territorio in cui si è esplicata la condotta, in accordo

[11] *Ivi*, 220 s.

con le esigenze di prevenzione; la seconda dell'evento, secondo la quale il reato si intende commesso nel luogo in cui si è verificato l'evento, così adeguandosi alle esigenze di salvaguardia del principio di difesa; la terza dell'ubiquità, a cui il legislatore italiano ha aderito, per cui il reato si considera commesso tanto nel territorio in cui è avvenuta, anche solo in parte, la condotta criminosa, tanto in quello in cui si è verificato l'evento[12].

Fatte queste premesse, è doveroso passare ad analizzare nel dettaglio i profili, sia sostanziali che procedurali, in quanto necessitano di essere inquadrati i criteri che più specificamente attengono all'individuazione del *locus commissi delicti*.

2.1 Profili sostanziali

Essenziale, al fine di stabilire l'applicabilità della legge italiana, è individuare il luogo in cui il reato è stato commesso. A tal proposito è necessario passare in rassegna i principi cardine dell'ordinamento giuridico italiano, volti a definire i confini della legge penale nello spazio, che permettono così di determinare la rilevanza penale di una determinata condotta, nonché di scongiurare potenziali conflitti tra diversi ordinamenti statuali.

La legge italiana esplica i suoi effetti nei confronti di tutti i soggetti che si trovano sul territorio dello Stato, salvo eccezioni costituite dalle c.d. "immunità personali": l'obbligatorietà della legge penale prevista dall'art. 3, co. 1 c.p. contiene un primo riferimento alla validità personale, per cui essa esplica la sua efficacia nei confronti di cittadini o stranieri che si trovano sul suolo dello Stato e contiene la prima enunciazione del principio di territorialità, per cui l'unico limite che viene posto all'applicabilità della legge italiana è il territorio dello Stato, definendo l'ambito applicativo sia a livello personale che spaziale. Vi sono però delle eccezioni, costituite dal fatto che in alcuni casi è possibile perseguire condotte perpetrate anche al di fuori del territorio nazionale: difatti, secondo l'art. 3 co. 2 c.p., la legge penale italiana obbliga altresì coloro che, cittadini o stranieri, non si trovano sul territorio dello Stato, ma limitatamente ai casi stabiliti dalla legge o dal

[12] In tal senso FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Cybercrime*, Torino, 2019, 144 ss.

diritto internazionale, enunciando così il principio di tendenziale universalità della legge penale, che permette di temperare il primo principio summenzionato.

Fondamentale, dunque, ai fini dell'individuazione del luogo del commesso reato è stabilire quando un fatto risulta commesso nel territorio dello Stato, vale a dire individuare la base di questo criterio positivo, che consente di estendere la legge penale italiana a cittadini e stranieri. Occorre definire, preliminarmente, cosa si intenda per territorio dello Stato: l'art. 4 co. 2 c.p. identifica agli effetti della legge penale il territorio dello Stato nel territorio della Repubblica, che ricomprende tutti i territori delimitati dai confini politici stabiliti da convenzioni, nonché trattati internazionali, e ogni altro luogo soggetto alla sovranità dello Stato; sono soggetti alla sovranità statale il sottosuolo, lo spazio aereo nazionale, il mare territoriale e le acque interne; parimenti, secondo l'art. 4 co. 2 ultima parte, sono considerati territorio dello Stato le navi e gli aeromobili italiani ovunque si trovino, fatti salvi i casi in cui siano soggetti a una legge territoriale straniera, secondo il diritto internazionale: in riferimento a questo assunto occorre distinguere tra navi e aeromobili militari italiani e civili che si trovino in territorio estero, per cui nel primo caso è illimitata l'estensione della legge penale italiana, mentre nel secondo caso vi è un'estensione limitata, essendo esclusa quando il reato colpisca una persona diversa dai membri dell'equipaggio, quando il fatto incida sulla tranquillità statale ovvero quando sia richiesto l'intervento dell'autorità locale[13].

Attuata questa doverosa premessa, è possibile decretare quando un fatto si consideri commesso nel territorio dello Stato, analizzando l'art. 6 del codice penale, che al primo comma afferma che «chiunque commette un reato nel territorio dello stato è punito secondo la legge italiana», rifacendosi in tal modo al principio di territorialità. Il secondo comma tempera questo principio mediante l'adozione del criterio di ubiquità, il quale ritiene rilevante ai fini dell'individuazione del *locus commissi delicti* sia il luogo ove si è commesso anche un semplice frammento della condotta, sia ove si è esplicato l'evento, di modo da estendere l'applicabilità della legge penale italiana. L'accoglimento di questo criterio si desume, secondo la dottrina, dall'interpretazione della locuzione "si considera", che intende equiparare il realizzarsi di parte della condotta nel territorio dello Stato con l'effettiva

[13] Cfr. MARINUCCI, DOLCINI, *Manuale di Diritto Penale. Parte Generale*, cit., 143 s.

consumazione del reato. In particolare, l'art. 6 co. 2 del codice penale recita che «il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione», per cui basta che si sia realizzato anche un frammento dell'azione criminosa per determinare l'applicabilità della legge italiana. Non risultano accolte, pertanto, come visto (v. *supra* Cap. II, § 2), le ulteriori teorie avanzate dalla dottrina italiana, *ergo* la teoria della condotta e la teoria dell'evento: la prima riscontrava il luogo di commissione del reato nel luogo ove si fosse esplicata la condotta, mentre la seconda ove si fosse verificato l'evento.

Al fine di comprendere la portata della norma in riferimento alle diverse categorie di reato, è necessario effettuare un'analisi circa le formule utilizzate dal capoverso dell'art. 6. In particolare, secondo la Relazione ministeriale al progetto del codice penale, il termine "azione" ricomprende tutti gli atti facenti parte dell'*iter* criminoso[14]. Al riguardo, si sono sviluppati diversi orientamenti interpretativi in riferimento al *quantum* di azione compiuta nel territorio italiano – quando in esso non si sia svolto l'intero *iter* criminoso – per affermare l'estensione dell'applicabilità della legge italiana.

Un primo orientamento intende la nozione di "azione" in senso lato, ritenendo che occorra almeno un atto di esecuzione della fattispecie criminosa. Diversamente, in netta contrapposizione, un altro orientamento ritiene necessaria la verificazione della soglia degli atti necessari per la punibilità del tentativo, vale a dire l'idoneità e l'unicità degli atti. Tale ultima tesi è stata tuttavia respinta dalla dottrina maggioritaria per il fatto che la configurabilità di atti idonei ed inequivoci compiuti sul territorio dello Stato rendono già punibile il delitto in Italia, alla stregua dell'art. 56 c.p., mentre non sarebbero punibili, non ritenendoli commessi in Italia, i tentativi di contravvenzione, dato che l'ultimo articolo citato si riferisce ai soli delitti[15]. Vi è, poi, quella parte della dottrina che ha elaborato un'ulteriore teoria, in base alla quale si richiede che l'atto posto in essere in Italia sia un

[14] In tal senso SINISCALCO, *Locus commissi delicti*, in *Enc. del diritto*, 1974, XXIV.

[15] Così PETRINI, *La responsabilità penale per i reati via Internet*, cit., 231, che alla nt. 41 richiama il ragionamento sviluppato da VINCIGUERRA *in Diritto penale italiano. Vol. I. Concetto, fonti, validità, interpretazione*, Padova, 1999.

momento imprescindibile nella serie causale che ha poi portato alla verificazione dell'evento all'estero[16].

Alla luce di tali diversi orientamenti, è stata accolta la tesi che ritiene estensibile l'applicabilità della legge penale italiana a fatti commessi solo parzialmente in territorio italiano e consumati all'estero, quando in Italia si sia compiuto anche uno solo degli atti tipici del processo criminoso al fine di integrare la fattispecie tipica, come specificato nella Relazione al progetto definitivo del codice penale, in conformità con la *ratio legis* di estendere l'applicabilità della legge italiana. Resta da precisare che per fattispecie tipica si intendono le azioni riconducibili a quelle descritte dalla norma incriminatrice.

Continuando l'analisi delle formule analizzate dal legislatore, si consideri che "l'omissione" da questo menzionata sta ad indicare, secondo parte della dottrina, che il reato si considererà commesso nel territorio dello Stato se in tale luogo doveva essere realizzata l'azione doverosa, che invece è stata omessa[17]; mentre altra parte della dottrina ritiene che tale assunto sia troppo limitativo e non consideri le ipotesi in cui il soggetto si allontani dal luogo in cui doveva compiersi l'azione doverosa, recandosi nel territorio italiano[18].

La giurisprudenza è da tempo concorde nel ritenere che non siano necessari gli estremi del tentativo ai fini della estensione della giurisdizione italiana, in accordo con la *ratio* che aveva ispirato il legislatore di estendere al massimo la giurisdizione italiana. Difatti questa considera sufficiente ai fini della sua applicabilità che sia avvenuta in Italia anche una minima parte dell'azione o dell'omissione, seppur priva dei requisiti richiesti per il tentativo, quali l'idoneità e inequivocità degli atti, e che tale parte sia un frammento apprezzabile, considerandolo *ex post*, in modo tale da collegare tale parte di condotta con quella realizzata all'estero[19].

---

[16] *Ivi*, 232.

[17] V. MARINUCCI, DOLCINI, *Manuale di Diritto Penale. Parte Generale*, cit., 146.

[18] In questa prospettiva VINCIGUERRA, *Diritto penale italiano. Vol. I. Concetto, fonti, validità, interpretazione*, Padova, 1999.

[19] Cfr. Cass. pen. Sez. VI, 24.04.2012, n. 16115 e nello stesso senso Cass. pen. Sez. VI, 12.02.2016, n. 11442, in *www.pluris-cedam.utetgiuridica.it*; si ricordi anche Cass. pen. Sez. VI, 21.09.2017, n.56953, in *www.dejure.it*, che ha stabilito che «Ai fini dell'affermazione della giurisdizione italiana in relazione a reati commessi in parte all'estero, è sufficiente che nel territorio

L’evento a cui bisogna riferirsi va inteso, secondo la dottrina maggioritaria, nel senso di evento naturalistico, vale a dire la modificazione del mondo esterno dipendente dalla condotta del reo, non potendosi far riferimento all’evento giuridico per cui si intende l’offesa al bene giuridico tutelato: ciò emerge dallo stesso testo normativo in cui si fa espressamente riferimento al nesso causale tra la condotta e l’evento.

Per quanto concerne la figura del reato abituale, qualora il reato non venga commesso interamente in Italia, si ritiene applicabile la legge italiana quando sul suolo dello Stato è stato compiuto anche uno degli atti, la cui reiterazione integra il reato. Per il reato permanente, qualora solo una porzione della condotta sia compiuta nel territorio italiano, si considera applicabile la legge italiana se ivi è realizzata anche solo la parte iniziale dell’azione criminosa.

Giunti alla conclusione di questa breve analisi, si percepisce come il legislatore abbia inteso, in accordo con l’ideologia autarchica del tempo, estendere massimamente la giurisdizione italiana, così da non lasciare impuniti frammenti di condotta che potessero realizzarsi nel territorio nazionale e ripristinare l’ordine giuridico, ferma restando la presenza di un interesse alla repressione, tale che sia idoneo a giustificare l’intervento repressivo, in quanto tale assunto deve sempre conformarsi ai principi cardine dell’ordinamento penale, tra i primi il principio di legalità, che impedisce di considerare apprezzabili comportamenti che esulano dalla legge penale[20].

Il principio di territorialità è stato poi accantonato in favore del principio di universalità con gli artt. 7 e ss. del codice penale. La massima espansione della giurisdizione italiana trova la sua esplicazione in quei reati commessi interamente all’estero dal cittadino ovvero dallo straniero, i quali offendono determinati interessi preminenti per la Stato, a cui viene applicata la legge penale italiana. Si consideri che la *ratio* ispiratrice di queste norme risale al regime autoritario, per cui esse rispondevano alla necessità di reprimere i delitti offensivi di determinati

dello Stato si sia verificato anche solo un frammento della condotta, intesa in senso naturalistico, e, quindi, un qualsiasi atto dell'*iter* criminoso; tale connotazione, tuttavia, non può essere riconosciuta ad un generico proposito, privo di concretezza e specificità, di commettere all'estero fatti delittuosi, anche se poi ivi integralmente realizzati».

[20] In tal senso MANICCIA, *Gli incerti “confini” del principio di territorialità*, nota a Cass. pen. Sez. VI, 21.09.2017, n. 56953.

interessi, in accordo con il principio della difesa dello Stato. Si pensi all'art. 7 c.p., che individua i casi in cui i reati commessi all'estero sono incondizionatamente puniti con la legge italiana, senza considerare che il fatto sia commesso da un italiano o da uno straniero, come nel caso in cui si offendano preminenti interessi dello Stato. L'art. 7 n. 5 c.p. conferma, ancora una volta, l'adesione al principio di universalità, stabilendo l'applicabilità della legge italiana a tutti i reati per cui specifiche disposizioni legislative o convenzioni internazionali la istituiscono, conferendo altresì importanza al principio di difesa.

Si prevede, poi, la difesa dello Stato mediante l'incriminazione dei c.d. delitti politici, individuati dall'art. 8 c.p. secondo cui, «agli effetti della legge penale, è delitto politico ogni delitto che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino» o comunque un delitto comune determinato da motivi politici: nei primi due casi si parla di delitti oggettivamente politici, che offendono le componenti essenziali dello Stato, per cui si denota una forte componente offensiva, da cui si determina l'applicabilità della legge italiana; nel secondo caso si parla di delitti soggettivamente politici, che guardano al movente che ha spinto il reo a delinquere.

L'art. 8 c.p., differentemente dall'articolo precedente e salvo il caso di cui all'art. 7 co. 1, non fa scaturire l'applicazione incondizionata della legge italiana, ma subordina questa ipotesi ad una scelta di opportunità da parte del potere esecutivo, nonché alla querela della persona offesa, quando questa sia richiesta.

La tendenziale adesione al principio di universalità si evince ulteriormente dall'art. 9 c.p., rubricato delitto comune del cittadino all'estero, che dispone l'applicabilità della legge penale italiana a tutti quei delitti commessi all'estero dal cittadino puniti con pena detentiva, sottoponendo la perseguibilità a determinate condizioni. Bisogna considerare che l'applicabilità della legge italiana è riconosciuta non solo a conferma di una pretesa universalistica, ma anche a protezione degli interessi offesi in accordo con il principio di difesa, nonché in statuizione del principio di personalità attiva qualora la condotta deviante sia stata posta in essere dal reo a danno di uno Stato estero o cittadino estero, fatte sempre salve le condizioni di operatività della norma.

Con l'art. 10 c.p. si ha, invece, la massima esplicazione del principio di universalità, in quanto la norma assoggetta alla legge penale italiana i delitti comuni commessi dallo straniero all'estero a danno dello Stato, del cittadino italiano ovvero di uno Stato estero, fatti salvi i limiti e le diverse condizioni previste a seconda dei beni giuridici offesi, per cui misure e specie della pena vanno a condizionare l'esplicazione di tale fattispecie.

Al fine di mitigare i conflitti giurisdizionali tra Stati, l'ordinamento italiano ha dato attuazione con decreto legislativo n. 29 del 2016 alla decisione quadro 2009/948/GAI del Consiglio, volta a prevenire e risolvere i conflitti relativi all'esercizio della giurisdizione dei procedimenti penali, migliorando così la cooperazione tra gli Stati e promuovendo una efficace gestione della giustizia penale nei casi riguardanti diversi paesi. Si prevedono, infatti, delle consultazioni dirette, tra le autorità competenti, affinché si pervenga ad una soluzione efficace, volta ad evitare procedimenti paralleli sui medesimi fatti, che minerebbe ai principi e ai diritti dei soggetti coinvolti[21]. Tale scelta "flessibile" del legislatore europeo è volta a scongiurare possibili violazioni del principio di obbligatorietà dell'azione penale, permettendo agli Stati di giungere ad un accordo ragionevole in merito alla giurisdizione, avuto riguardo della specificità dei casi trattati[22]. Come si può intuitivamente evincere, questa decisione è rilevante in tema di reati cibernetici, caratterizzati dalla transnazionalità.

Dall'analisi di questo quadro, delineato dal legislatore del 1930, emergono le prime problematiche inerenti all'individuazione del *locus commissi delicti*, risolte dalla dottrina e dalla giurisprudenza mantenendo fede alla *ratio legis* che aveva mosso le menti del tempo, in una prospettiva di continuità con la codicistica precedente. Al fine di una completa indagine sul tema, non si possono non considerare le disposizioni processuali, che dettano dei criteri in grado di attribuire la competenza territoriale, individuando il luogo del commesso reato e in grado di scongiurare possibili questioni di conflitto di competenze, come si leggerà *infra* (v. Cap. II, § 2.2).

---

[21] Cfr. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, 146 s.

[22] *Ivi*, 147: l'autore richiama in merito l'opera di Mezzolla, riguardante la "Prevenzione e risoluzione dei conflitti di giurisdizione in ambito penale".

2.2 Profili procedurali

L'esame circa l'individuazione del *locus commissi delicti* deve essere svolta analizzando gli aspetti processuali, che consentono attuare un collegamento tra il fatto e il luogo in cui è stato commesso, permettendo così di individuare il giudice territorialmente competente. Occorre premettere che le disposizioni di ordine processuale vanno subordinate a quelle di ordine sostanziale, le quali permettono di radicare nel territorio italiano la giurisdizione, per cui i seguenti criteri vanno parametrati a quelli precedentemente analizzati. Difatti, il tema della competenza può prescindere dal luogo di commissione del delitto, mediante il riferimento ai criteri suppletivi, di cui si dirà *infra* (v. Cap. II, § 2.2).

Il codice di procedura penale ha previsto delle disposizioni idonee a stabilire la collocazione spaziale del reato, stabilendo all'art. 8 c.p.p., che la competenza per territorio è determinata dal luogo in cui il reato è stato consumato. Tale criterio generale è volto a statuire il giudice territorialmente competente, in accordo con il principio costituzionale del giudice naturale precostituito per legge, di cui all'art. 25 della Costituzione.

La fissazione di tale criterio nel luogo in cui si è consumato il reato – che, come stabilito *supra* (v. Cap. II, § 1), si considera consumato quando si sono realizzati tutti gli elementi costitutivi della fattispecie e ha raggiunto la sua massima gravità – si giustifica non solo in previsione del rispetto del principio del giudice naturale, ma anche per una finalità di economia processuale e specialmente per l'esigenza di facilitare la ricerca e la valutazione delle prove, così confacendosi all'esigenza di ripristinare la legalità nel luogo in cui questa è stata turbata; deroghe a tale principio potrebbero essere ammesse solo qualora sorrette da adeguati motivi di tutela di ulteriori interessi rilevanti.

Il luogo di consumazione va individuato, nel caso di reati di evento, nel luogo in cui questo si è verificato; nel caso di reati di mera condotta, nel luogo in cui si è realizzato il comportamento, sia esso attivo o omissivo. Questo assunto non risulta così immediato in tema di condizioni obiettive di punibilità e di reati aggravati dall'evento: vi è chi ritiene, con riferimento alle prime, che l'individuazione del luogo del commesso reato vada riscontrata nel luogo in cui si

realizza la condizione; vi è chi sostiene, per i secondi, che l'evento aggravante non vada considerato, per cui il *locus* va individuato nel luogo in cui si consuma il fatto semplice, al contrario di chi, invece, afferma la rilevanza dell'evento aggravante[23].

Il criterio generale così delineato dal primo comma dell'art. 8 c.p.p. soffre di alcune eccezioni al fine di individuare criteri più opportuni, che rispondano ad esigenze di indagine, al verificarsi di determinate circostanze. Difatti, è stabilita una deroga in caso di evento morte al secondo comma, che individua il giudice territorialmente competente nel luogo ove è stata compiuta l'azione o l'omissione. Allo stesso modo, al terzo comma, si statuisce che, in caso di reato permanente, è competente il giudice del luogo in cui ha avuto inizio la consumazione, anche qualora dal fatto illecito del reo dovesse derivare l'evento morte di uno o più soggetti passivi, giustificandosi tale scelta poiché l'opposto criterio, facente leva sulla cessazione della permanenza, avrebbe sortito strumentalizzazioni da parte degli autori del reato. Nel caso di delitto tentato, è competente il giudice del luogo in cui è stato compiuto l'ultimo degli atti diretti ad attuare il delitto. Queste deroghe sono state previste dal legislatore con lo specifico intento di adottare delle regole idonee, rispondenti all'esigenza di ripristinare l'ordine sociale violato e agevolare la reperibilità di elementi utili per l'accertamento dei fatti[24].

Alla luce di questa analisi è possibile stabilire che il criterio per decretare l'individuazione del *locus commissi delicti* vada ravvisato nel luogo in cui si è consumata la fattispecie criminosa, come espressamente sancito dal primo comma dell'art. 8 c.p.p. Bisogna avere riguardo del fatto che numerose deroghe alla regola di individuazione del *locus commissi delicti* determinano la propria legittimazione dall'art. 210 delle disposizioni di attuazione, che enuncia il continuo essere in vigore delle norme che stabiliscono la competenza per territorio sulla base di criteri differenti da quello di cui all'art. 8 co. 1 c.p.p.[25].

Fatto salvo ciò, non è sempre possibile, tuttavia, sancire con certezza il luogo ove il reato viene commesso ed è per tale motivo che il codice Vassalli

---

[23] V. "Codice penale commentato sub *art. 8 c.p.p. Regole generali*", in *www.pluris-cedam.utetgiuridica.it.*

[24] Per una completa analisi sul tema dell'individuazione del giudice competente, si veda BARGIS, CONSO, GREVI ET AL., *Compendio di procedura penale*, IX ed., Wolters Kluwer, Cedam, Milano, Padova, 2018, 15 ss.

[25] *Ivi*, 17.

enuncia dei criteri suppletivi da adottare nel caso in cui non sia possibile individuare il *locus commissi delicti* secondo le indicazioni di cui all'art. 8 c.p.p.: l'art. 9 c.p.p. enuncia, infatti, dei criteri posti tra loro in ordine di gradualità da applicarsi in via sussidiaria, presupponendo la previa mancata applicazione della regola strettamente precedente. Si stabilisce al comma 1 che il giudice competente è quello dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione, vale a dire una porzione della condotta essenziale ai fini dell'integrazione della fattispecie criminosa. Qualora tale criterio non possa sortire idonea applicazione, a causa della difficoltà di individuazione di parte della condotta, la competenza appartiene al giudice della residenza, della dimora o del domicilio dell'imputato, per cui ove sia sconosciuta la residenza si fa riferimento alla dimora ovvero in via alternativa al domicilio. Ove neppure quest'ultimo criterio risulti applicabile, la competenza appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che per primo ha provveduto ad iscrivere la notizia di reato nell'apposito registro. La *ratio* delle regole suppletive è da ravvisarsi nell'esigenza di stabilire criteri oggettivi nell'individuazione del *locus commissi delicti,* quando a causa del tipo di reato o di altre biasimevoli ragioni non è possibile individuarlo mediante i criteri generali.

È importante ricordare che tali regole trovano impiego anche qualora il reato sia commesso in parte all'estero, mentre qualora sia commesso interamente all'estero la competenza è determinata dal luogo di residenza, dimora, domicilio o ancora arresto ovvero consegna dell'imputato; ove non si rinvenga in tal modo il giudice competente, va individuato nel giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato, ai sensi dell'art. 10 comma 2 c.p.p.; qualora si tratti di reato commesso all'estero a danno di un cittadino e non è possibile individuare in altro modo il giudice competente, si fa riferimento alla regola *ex* art. 10 comma 1-*bis* che statuisce la competenza del tribunale o corte d'assise di Roma, fatti salvi i casi in cui ricorrano le ipotesi di connessione.

La disamina di ordine generale che precede permette di avere le basi per affrontare il prossimo argomento oggetto di analisi, vale a dire i problemi concernenti i limiti del principio di territorialità nel *cyberspace.*

3. I limiti del principio di territorialità nel *cyberspace*

L'avvento delle tecnologie informatiche ha reso possibile le interconnessioni a livello globale, permettendo ai soggetti di collegarsi da vari punti nel globo, agendo e comunicando a distanza. La realtà del *cyberspace* travalica i confini spazio-temporali e consente l'accesso in rete, anche contemporaneamente, in più luoghi virtuali, essendo priva di confini spaziali, mediante operazioni automatizzate, le quali possono avvenire anche in assenza di un collegamento tra il soggetto e il sistema informatico, senza così consentire l'individuazione del punto esatto in cui viene realizzata la condotta. Gli ordinamenti giuridici necessitano di un luogo sul quale esercitare la propria sovranità e ciò contrasta con le caratteristiche tipiche della Rete, la quale invece ignora la territorialità degli ordinamenti giuridici. Risulta, quindi, problematica l'applicazione dei principi basilari, che appaiono per questo limitati: si fa riferimento al principio di territorialità, alla luce del quale la legge italiana si applica ai fatti commessi nel territorio dello Stato.

Le condotte poste in essere, infatti, si distanziano dalla fisicità dei comportamenti tradizionali, in grado di inglobare l'accadimento materiale che si è concretizzato, rendendo difficile indicare il luogo ove il fatto viene commesso e parimenti ostica l'individuazione del responsabile. Il soggetto agente ben potrebbe consapevolmente declinare a proprio favore la diversità tra realtà materiale e virtuale, sfruttando la diffusività di Internet e la presenza di paradisi informatici, in cui vi è la mancanza di una legislazione che sanzioni gli illeciti perpetrabili attraverso la rete. Si tratta di comportamenti devianti atemporali e aterritoriali, caratterizzati dalla transnazionalità, a cui mal si concilia il principio di territorialità, espressione della sovranità statale. Le attività compiute *online* constano di diverse operazioni, le quali partono da una postazione ma poi si snodano nella rete, utilizzando diversi *server,* che possono essere collocati in svariate parti nel globo. L'esplicazione così intesa della condotta comporta la polverizzazione del fatto unico in diversi spazi fisici, che rende problematica l'applicazione del principio di territorialità, in quanto spesso risulta complesso individuare il luogo in cui il soggetto esegue quell'illecito.

Come evidenziato da autorevole dottrina, l'agente ben potrebbe falsificare il proprio indirizzo *IP* ovvero recarsi in uno Stato estero per compiere l'azione disdicevole e in entrambi casi il luogo in cui si è operato non sarebbe identificabile, mentre sarebbe individuabile il luogo in cui è ubicato il *server* che permette l'accesso in Rete[26]: esistono, quindi, luoghi spaziali identificabili, a cui è possibile ancorare dei criteri, al fine di garantire l'effettività e la certezza del diritto. Pertanto, sebbene il principio di territorialità venga limitato in questa nuova dimensione, non può essere accolto il suo definitivo abbandono, piuttosto questo deve tener conto delle peculiarità proprie della criminalità informatica al fine di individuare soluzioni, che permettano di collocare nello spazio l'illecito perpetrato *online*. Tendenzialmente, sarebbe ideale puntare ad un provvedimento di carattere sovranazionale, che coinvolga il maggior numero di ordinamenti giuridici, tale da emendare i criteri di collegamento tra fatto commesso online e ordinamento giuridico, in modo tale da abbracciare le peculiarità degli illeciti commessi in Rete. Tale auspicio ha alla base l'assunto che l'emanazione di una normativa sovranazionale in materia non permetterebbe ai cybercriminali di eludere facilmente la disciplina istitutiva di un collegamento tra la realtà virtuale e lo spazio fisico, idonea ad identificare il luogo di commissione del reato.

Un primo contributo atto a dare concretezza alla teoria summenzionata è fornito dalla Convenzione del Consiglio d'Europa sulla criminalità informatica, la quale pone in luce la necessità di attuare una politica comune in ambito penale, con lo scopo di combattere la cybercriminalità mediante la cooperazione internazionale e il ravvicinamento delle disposizioni penali.

Essa all'art. 22 prevede che le parti devono adottare le misure necessarie per stabilire la propria competenza per tutti i reati previsti dalla stessa Convenzione, qualora questi siano commessi nel proprio territorio; a bordo di una nave battente bandiera della Parte interessata; a bordo di un aeromobile immatricolato presso quella Parte; da un proprio cittadino, se l'offesa è penalmente punibile nel luogo ove è stata commessa o se l'offesa non rientra nella competenza territoriale di alcuno Stato; inoltre, la stessa non esclude alcuna competenza penale esercitata da una Parte, secondo il proprio diritto interno; qualora, poi, più di una Parte rivendichi

[26] Così PETRINI, *La responsabilità penale per i reati via internet*, cit., 238.

il proprio diritto a perseguire una determinata violazione della Convezione, le Parti devono consultarsi per stabilire la competenza maggiormente appropriata per l'esercizio dell'azione penale[27].

La Convenzione di Budapest non è l'unico atto internazionale che ha cercato di porre fine ai dubbi sorti dalle caratteristiche peculiari della Rete. Accanto ad essa si annoverano ulteriori fonti europee, emanate nella prospettiva di regolare le procedure inerenti a illeciti informatici, nella prospettiva di sanare le divergenze tra Stati che possono solo ostacolare la lotta contro codesta forma di criminalità. Si fa riferimento alla Direttiva europea 2013/40/UE, concernente gli attacchi contro i sistemi di informazione, che all'art. 12 dispone che gli Stati membri stabiliscano la propria competenza giurisdizionale relativamente a determinati reati[28], quando questi siano stati commessi in tutto o in parte sul territorio o da un loro cittadino, quanto meno, come affermato, nei casi in cui l'atto costituisca un reato nel luogo in cui è stato compiuto; essa statuisce, inoltre, che uno Stato assicura di avere la competenza giurisdizionale laddove l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, al di là del fatto che il reato sia stato compiuto o meno avverso un sistema di informazione nel suo territorio ovvero al di là della presenza o meno del reo nel territorio suddetto al momento della commissione del reato; è statuito che uno Stato membro informi la Commissione ove voglia stabilire la competenza giurisdizionale per un reato commesso al di fuori del territorio anche qualora l'autore risieda abitualmente nel suo territorio e il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio.

Nello stesso senso si pone la Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, la quale dispone che gli Stati membri adottino le misure necessarie a stabilire la propria giurisdizione in caso di reato commesso a mezzo di tecnologie informatiche a cui l'autore ha avuto accesso dal loro territorio,

[27] Art. 22 della Convenzione del Consiglio d'Europea sulla criminalità informatica, Budapest 23.11.2001.

[28] Artt. 3-8 della Direttiva europea 2013/40/UE: si tratta dei reati di accesso illecito a sistemi di informazione, interferenza relativamente a sistemi e dati, intercettazione illecita, istigazione, favoreggiamento, complicità e tentativo, nonché reati di fabbricazione, vendita, approvvigionamento per l'uso, importazione, distribuzione o messa a disposizione di programmi atti a compiere uno di tali delitti ovvero di password volte ad accedere a sistemi informatici.

nonché nei casi in cui il reato sia stato commesso in tutto o in parte sul proprio territorio o se l'autore del reato è un loro cittadino, stabilendo altresì la propria giurisdizione in caso di reato commesso al di fuori del proprio territorio a danno di un proprio cittadino o soggetto residente stabilmente in suddetto territorio ovvero sia commesso a vantaggio di una persona giuridica avente sede nel proprio territorio oppure nel caso in cui l'autore del reato risieda stabilmente in detto territorio.

Al fine di arginare le difficoltà inerenti all'individuazione dello Stato territorialmente competente quando ci si trovi dinnanzi ad un illecito cibernetico, si è posta anche la Decisione quadro 2008/913/GAI sulla lotta contro talune forme di razzismo e xenofobia, che ha statuito che ciascuno Stato membro debba adottare le misure necessarie affinché, per garantire che la propria giurisdizione, si estenda anche ai casi in cui la condotta illecita sia posta in essere mediante un sistema di informazione e il reo sia presente sul suo territorio, a prescindere dall'utilizzo di materiale situato su un sistema collocato nel suo territorio o comunque il comportamento implichi l'uso di materiale presente su un sistema ubicato nel suo territorio, a prescindere dalla presenza dell'autore sul territorio della parte interessata[29].

Tali fonti sono importanti per evitare la duplicazione di procedimenti penali, riconoscendo così l'adozione di criteri – come quello di territorialità, personalità attiva e passiva – i quali vanno coniugati con la realtà informatica. Esse consentono di attrarre la competenza sia nel caso in cui il soggetto operi nel territorio dello Stato sia nel caso in cui costui operi dall'estero e il sistema attaccato si trovi sul suolo nazionale, sia *a contrario* nel caso in cui costui operi nel territorio dello Stato e il sistema violato si trovi all'estero. Si svincola parzialmente l'individuazione della competenza territoriale dai tradizionali principi, adottando criteri giudiziali flessibili che si adeguino alla realtà cibernetica e arricchiscano il tradizionale principio di territorialità. Difatti, proprio per far fronte ai limiti risultanti dal principio tradizionale, le fonti summenzionate adottano il criterio di territorialità, ma non solo, dato che qualora il reato sia punibile nel luogo in cui è stato commesso ovvero non rientri nella competenza territoriale di nessuno Stato, viene adottato il

[29] V. art. 9 della Decisione quadro del Consiglio 2008/913/GAI del 28.11.2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale.

principio della personalità attiva; accanto ad essi, la direttiva contro l'abuso e lo sfruttamento sessuale dei minori accoglie il principio della personalità passiva[30] (v. *infra* Cap. II, § 3.1). Questo avviene a causa della sempre più frequente distonia tra l'esplicazione della condotta da parte del reo e la sua collocazione territoriale per cui, attenendosi al criterio della personalità attiva, si istituisce un collegamento tra il soggetto, la condotta criminosa e l'ordinamento giuridico dello Stato – sebbene il reo non abbia operato su quest'ultimo – per evitare che i comportamenti devianti restino impuniti. Si noti come le suddette disposizioni menzionino il luogo della condotta e di verificazione dell'evento nonché, in particolare nella Direttiva del 2011, il luogo di accesso alla rete, luoghi che assumono rilevanza ai fini della determinazione del luogo del commesso reato. Ciò è dovuto al fatto che i tradizionali concetti di azione ed evento subiscono un'astrazione quando si esplicano in rete, affrontando una sorta di obsolescenza e necessitando di una ridefinizione, per cui la condotta si dematerializza e viene integrata dalla successiva esecuzione automatica di ulteriori attività, come la trasmissione di dati, da parte di ulteriori *software* operanti nella rete, così attuandosi l'attività propriamente voluta dal soggetto agente; mentre l'evento va ravvisato nel risultato di una procedura automatizzata, assumendo tratti di ubiquità e astrazione[31].

Tendenzialmente, oggi, l'individuazione del *locus commissi delicti* tiene conto della concreta possibilità di individuazione del luogo in cui ha operato l'agente, adottando contrariamente il criterio che individua il luogo di commissione del delitto nel luogo ove è situato il *server* del *provider* che concede l'accesso alla Rete, richiamandosi così al principio di ubiquità, tale che si attribuisce rilevanza, parimenti, sia al luogo ove l'agente ha operato e sia a quello in cui è situato fisicamente il *server* menzionato[32]. Proprio alla luce di tali mutati concetti, si ritiene che la rigida applicazione del principio di territorialità andrebbe limitata in vista di

[30] In argomento FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 150.

[31] Sul punto SEMINARA, voce Internet *(diritto penale)*, in *Enc. del Diritto*, Annali VII, Milano, 2014, 567 ss..

[32] In tal senso PETRINI, *La responsabilità penale per i reati via internet*, cit., 246 s.

una sua flessibile interpretazione, tale da adattarlo al contesto dematerializzato e aterritoriale della Rete, evitando forzature interpretative[33].

Concludendo, si può affermare che l'individuazione del *locus commissi delicti*, in questo campo d'indagine, deve discernere dalle classiche nozioni adottate di ambito territoriale, in virtù della necessità di interpretare in maniera evolutiva i concetti tradizionali.

3.1 Il principio della personalità attiva e passiva: il modesto riconoscimento nel contesto nazionale

Come analizzato nel precedente paragrafo, per supplire ai limiti dati dal tradizionale principio di territorialità, le fonti europee adottano ulteriori principi volti a stabilire la giurisdizione competente e l'individuazione del *locus commissi delicti*. Tali ulteriori criteri operano in via subordinata, qualora non sia possibile identificare il luogo in cui il soggetto pone in essere l'azione. Difatti, il criterio di territorialità è alla base di tutti gli ordinamenti giuridici, mentre gli ulteriori criteri sono diversamente regolati nei vari Stati dell'Unione, come evidenziato da autorevole dottrina: questi possono avere un massimo riconoscimento fino ad un riconoscimento limitato[34].

Nel codice penale italiano vi è un modesto riconoscimento dei summenzionati criteri, mentre come visto *supra* (v. Cap. II, § 2.1), vi è l'accoglimento del principio di territorialità, acquisendo rilevanza, per stabilire l'estrinsecazione della legge penale italiana, il luogo di realizzazione della condotta o di verificazione dell'evento – fatte salve le opportune deroghe all'operatività di tale principio in favore di quello più ampio di universalità – seppur la relativa applicazione si riveli problematica in virtù delle peculiarità che assumono le condotte perpetrate *online*. Diversamente, il principio di personalità attiva – o di nazionalità – considera, appunto, rilevante la nazionalità del soggetto attivo. Un parziale riconoscimento di tale principio si rinviene all'art. 9 del codice penale, in

[33] Cfr. l'intervento di FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, cit., 1309.

[34] V SEMINARA, Locus commissi delicti, *giurisdizione e competenza nel cyberspazio*, relazione al Convegno "Presi nella rete – Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012, reperibile su www.informaticagiuridica.unipv.it/convegni/2012/SEMINARA.

cui si fa riferimento per determinare la legge applicabile alla nazionalità del cittadino, sebbene questo abbia commesso il reato all'estero, a danno di uno Stato estero. Il principio di personalità passiva – o principio di difesa – conferisce rilievo, invece, agli interessi offesi. La manifestazione di tale principio si riscontra all'art. 10 c.p., in cui si statuisce l'applicazione della legge italiana a fatti commessi dallo straniero all'estero, in danno dello Stato italiano.

Tali principi hanno il proposito di svincolare la condotta del reo dal territorio in cui questa viene posta in essere, caratteristica che potrebbe essere confacente alle peculiarità tipiche degli illeciti *online,* così da estendere la potestà punitiva anche laddove concretamente l'azione si sia esplicata altrove.

Come si può evincere da queste brevi considerazioni, l'applicabilità di questi principi non fa riferimento alle condotte perpetrate *online,* ma attiene ad un livello più generale di estrinsecazione della potestà punitiva dell'ordinamento giuridico italiano.

Volendo considerare tali principi in vista di una possibile applicazione a suddette condotte, si consideri che, come evidenziato da autorevole dottrina, i reati consistenti in comunicazione o diffusione di contenuti illeciti *online* «risultano sottoposti alla legge italiana solo se realizzati da un soggetto operante in Italia o, al più, collegato a un *server* installato su territorio italiano»[35], facendo emergere come in questo caso si faccia riferimento all'esplicazione del principio di territorialità. Nel caso di reati informatici, l'applicabilità della legge italiana a fatti commessi all'estero da cittadino italiano, come si evince dagli artt. 7 e seguenti del codice, si traduce nell'applicazione del principio di universalità e personalità attiva, il quale viene applicato in considerazione degli effetti del collegamento del sistema informatico alla rete, ma in virtù della nazionalità del reo.

Considerando le peculiarità dell'azione commessa *online* emerge che non può essere assunto, come momento rilevante per la consumazione del reato, il luogo di immissione dei contenuti o di collegamento con la Rete, che renderebbe possibile all'agente di agire nel territorio con la legislazione più permissiva, così da indurre la produzione del fenomeno di *forum shopping*. Si noti come nel sistema tedesco per evitare tale fenomeno si attribuisca rilevanza al luogo in cui è situato il *server*

[35] Cfr. SEMINARA, voce Internet *(diritto penale)*, cit., 579.

sul quale sono salvati consapevolmente i dati. Al fine di attuare una limitazione del fenomeno di *forum shopping*, sarebbe auspicabile l'applicazione del principio di personalità passiva, che tutelerebbe maggiormente la vittima del reato mantenendosi vicino al luogo in cui si esplicano gli effetti negativi del reato, *locus* in cui possono rinvenire con maggior probabilità riscontri probatori[36]. Questo criterio ancorerebbe l'applicabilità della legge italiana ad un esito certo e avrebbe il merito di indurre i soggetti, in specie le imprese, a collocare ivi la propria sede, così da essere protetti da eventuali attacchi illeciti, nonché rispondere ad un'esigenza di tutela delle vittime.

Diversamente, in dottrina e giurisprudenza si è fatto più volte riferimento al luogo in cui è ubicato il *server* e ciò potrebbe far sorgere eventuali conflitti tra Stati competenti, dovute al fatto che l'azione *online* si traduce in molteplici operazioni che si snodano tra diversi *server* della rete situati in diversi luoghi; si prenda ad esempio il caso in cui il soggetto agente invii un messaggio di posta elettronica volto a diffondere codici di accesso: in tal caso l'operazione si snoda tra diversi *server* situati in luoghi diversi, tra cui il *server provider* gestore del servizio di posta elettronica del soggetto agente e del destinatario, coinvolgendo così diversi Stati. Proprio a tal fine le fonti europee sopra citate hanno il merito di dirimere tali possibili contrasti, richiedendo agli Stati membri di adottare una legislazione armonizzata volta a contrastare la criminalità informatica, ma ciò non risolve il problema di individuazione del luogo di commissione del reato. Tale problema potrebbe essere risolto mediante il ricorso ai criteri suppletivi, esplicitati dall'art. 9 del c.p.p., che permettono di considerare quale luogo rilevante ai fini della consumazione quello in cui si è verificata parte dell'azione o dell'omissione, che potrebbe essere, secondo il principio della personalità passiva, quello dell'area informatica violata, che qualora non individuabile, va rinvenuta mediante il legame con il titolare[37].

[36] V. infra cap. II paragrafo 6, in cui si esaminano le possibili interpretazioni evolutive che permettono di arginare i problemi di individuazione del locus sorti con le fattispecie cibernetiche.

[37] Così FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, cit., 1307.

Al fine di comprendere al meglio tali problematiche, è doveroso analizzare i problemi giuridici che attengono ai reati informatici ed in particolare quali di essi vengono in considerazione nella difficile individuazione del *locus commissi delicti*.

4. I problemi giuridici relativi ai reati informatici

L'illecito informatico è caratterizzato da un alto tasso di delocalizzazione, che rende difficoltoso determinare dove è stata realizzata una condotta. Alla luce di questo motivo, e date le caratteristiche della rete, occorre analizzare lo spazio virtuale, vale a dire il luogo in cui avvengono i collegamenti, nonché gli scambi di informazione tra i vari attori della rete. Le difficoltà inerenti all'individuazione del *locus commissi delicti* derivano dalla modalità in cui si svolge la dinamica dell'illecito cibernetico, in quanto non solo risulta di difficile collocazione l'effettivo luogo di consumazione del reato – data la complessità dei processi con cui vengono elaborati i dati sovente anche in luoghi distanti dalla postazione del reo – ma l'accessibilità alla rete da ogni parte del globo implica la complessa circoscrizione delle conseguenze dell'illecito sul piano spaziale[38].

È necessario precisare, fin da subito, che infatti la rete gode di libertà di accesso, per cui ogni soggetto dotato degli strumenti necessari è in grado di accedere alla rete e ai dati ivi immessi. Tale libero accesso viene garantito da *server*, gestiti da *service provider*, che non necessariamente si collocano sul medesimo territorio del soggetto che si connette alla rete, per cui le informazioni da questo inserite viaggiano nei diversi snodi della stessa prima di giungere a destinazione. Le operazioni compiute dal singolo utente vengono registrate, conservate – a seconda del tipo di *provider* – e identificate mediante l'indirizzo *Internet Protocol*. Fondamentale per il funzionamento della Rete risulta, quindi, l'*Internet service provider*, che è competente a fornire agli utenti i servizi della rete, quali memorizzazione e indicizzazione, che consente un corretto funzionamento della stessa, in quanto permette di sfruttare le capacità del *server*. La Rete si basa su un protocollo di comunicazione *client-server*, in cui un soggetto dalla propria postazione – *client* – si connette ad un *server*, per la fruizione di determinati servizi,

[38] Sul punto BRASCHI, *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, cit., 11 ss.

sulla base di una struttura centralizzata della rete. Diverse modalità di funzionamento adotta, invece, il protocollo *peer-to-peer*, ove vi è una rete paritaria a struttura decentralizzata, per cui ogni sistema compone un nodo di rete, sia *client* che *server*, terminali che dialogano tra pari e che si collocano alla base delle pratiche di *file sharing*[39]. È proprio la rete che, per le sue modalità di funzionamento, consente la dispersione delle informazioni in vari *server* e non permette di individuare facilmente il punto preciso in cui il reato si consuma.

Dopo una breve premessa sul *modus operandi* della Rete, appare doveroso attuare un'ulteriore considerazione di ordine generale. Difatti, il problema di individuazione del *locus commissi delicti* non coinvolge tutti i reati informatici, ma attiene solo a determinate strutture di reato. In particolare, la questione concerne la categoria dei *cybercrimes*, vale a dire quei reati in cui la Rete assume tratti caratterizzanti, in quanto questi si commettono ovvero si possono commettere in Rete.

In virtù di questo assunto è possibile escludere dai termini della questione i reati di evento e i reati informatici che non necessitano di una connessione in rete. Con riferimento ai primi è opportuno, però, operare una distinzione tra reati di evento e reati a evento c.d. cibernetico, i quali ultimi si esplicano mediante il *cyberspace*. Pare, quindi, adottarsi una nozione di evento che si discosta da quella tradizionalmente intesa in senso naturalistico, come precedentemente affermato, in quanto nascente da una procedura automatizzata, la quale però ne mantiene le caratteristiche peculiari sul piano degli effetti scaturenti in capo alla vittima e di offesa ai beni giuridici[40]. Tale evento si caratterizza per i suoi caratteri di ubiquità, che rende ostica l'individuazione del luogo in cui il reato raggiunge la sua massima offensività, diversamente dall'evento tradizionalmente inteso, autonomamente verificabile nella realtà materiale. Accanto ad essi, fanno parte della summenzionata questione anche il tentativo di commettere un reato di evento *online*, per cui gli atti idonei e inequivoci si traducono in operazioni automatizzate

[39] V. MARINELLI, voce "*Internet e* web", in *Enc.* online *Treccani*, *www.treccani.it*.

[40] Per un approfondimento si veda PICOTTI, con il contributo di SALVADORI e FLOR, *Reati informatici, riservatezza, identità digitale*, elaborato presentato durante il Convegno Nazionale dell'Associazione Italiana dei Professori di Diritto Penale, 2019, reperibile presso il sito *www.aipdp.it.*

commesse *online* che mettono in pericolo i beni giuridici tutelati dalle norme, e i reati di mera condotta commessi *online*, tra cui l'accesso abusivo a sistema informatico commesso a distanza – mentre non vi rientra quello commesso *offline* vale a dire nella stessa postazione in cui si trova il soggetto agente – per cui dato il funzionamento della rete sulla base del protocollo *client-server*, la condotta del soggetto si esaurisce nel compiere una data operazione *online* che pone in pericolo il bene giuridico tutelato dalla norma incriminatrice. A ben vedere è proprio dal modo di intendere il funzionamento della Rete, quale struttura centralizzata o unitaria – come stabilito dalle Sezioni Unite nel 2015 con sentenza n. 17325 – che scaturisce un diverso modo di individuazione del *locus commissi delicti*.

Proprio riguardo ai reati cibernetici appare utile riportare alla memoria la tradizionale distinzione tra perfezione del reato – intesa come momento in cui vengono integrati gli elementi costitutivi essenziali – e sua definitiva consumazione, quale momento di massima esplicazione dell'offesa, in quanto accade sovente che i due momenti non coincidano. Tale distinzione è importante alla luce del fatto che le caratteristiche del *cyberspace*, ed in particolare le tecniche di automazione delle operazioni, determinano la circolazione e permanenza dei dati e dei contenuti in codesta realtà, che di conseguenza impone di riconsiderare le condizioni che consentono di individuare il momento della consumazione: il fatto di reato riproduce i suoi effetti nel tempo, proprio per via delle funzioni automatizzate, che ne permettono la circolazione, condivisione e messa a disposizione[41]. Autorevole dottrina fa riferimento ad essi come reati a consumazione protratta, vale a dire quei fatti di reato che presentano una consumazione che si estende oltre il momento di perfezione formale, da cui deriva la peculiare nozione di evento, che verrà considerato alla stregua dell'identificazione del momento consumativo, che includerà l'ulteriore fase di

[41] Cfr. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, che richiama a ragione le riflessioni svolte da Picotti, in sede del Convegno Nazionale dell'Associazione Italiana dei Professori di Diritto Penale, il quale ha statuito che «è lo stesso "fatto" tipico che, nella parte in cui si realizza tramite i sistemi informatici, si deve ritenere che si protragga, espanda ed eventualmente "riproduca" in quei suoi elementi essenziali, che dipendono dall'esecuzione delle funzioni automatizzate di memorizzazione, trasmissione, messa a disposizione, condivisione, circolazione, ricerca, ecc., pur non sempre del tutto "dominabili" dai titolari, gestori e fruitori dei sistemi stessi»: l'autore ritiene che è la stessa automazione a determinare la protrazione nel tempo degli effetti, che possono addirittura sfuggire al controllo del reo che li ha posti in essere tramite le Tecnologie dell'Informazione.

prolungamento degli effetti, che comporta l'estensione dell'evento cibernetico[42]. In tal modo si scongiura un riferimento agli stessi come reati a consumazione prolungata, sviluppati in giurisprudenza, i quali possono presentare momenti alternativi di consumazione e presuppongono azioni volontarie da parte dell'autore del reato[43]. Non è neppure corretto dunque riferirsi alla permanenza degli effetti quale mero *post factum* non punibile, in quanto tale prolungamento non è scindibile dagli altri elementi costitutivi del fatto di reato, configurandosi anzi come una caratteristica peculiare del reato cibernetico[44].

Proprio in ragione del differente atteggiarsi delle classiche nozioni di condotta e evento e dalla ostica individuazione del luogo in cui il reato si ritiene consumato, non sempre appare applicabile il criterio di individuazione della competenza per territorio enunciata dall'art. 8 co. 1 del codice di rito, che andrebbe in questa sede parametrato su spazi virtuali. Tendenzialmente il luogo di commissione del reato andrebbe rinvenuto nel luogo di prima manifestazione dell'evento nel caso in cui ci si trovi dinnanzi a reati di evento, o di verificazione della condotta. Tuttavia, qualora non sia possibile stabilire il luogo della consumazione, bisogna accogliere i criteri suppletivi delineati dall'art. 9 c.p.p., dovendosi riferire, ai fini dell'individuazione della competenza, all'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione ovvero – qualora ignoto – alla residenza, dimora o domicilio del reo ovvero al luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato.

In virtù di questa disamina, si evidenzia come sempre più frequentemente si assista alla presenza di voci favorevoli ad un diritto flessibile, che consenta di adeguarsi alle esigenze di tutela emergenti, tale da rispondere all'inerzia del legislatore di fronte a queste dispute. In considerazione di tali problematiche, i giudici hanno, infatti, cercato di adattare i criteri di individuazione del *locus commissi delicti* al caso di specie, in modo tale da tutelare adeguatamente il soggetto leso. Si evince, nella maggior parte dei casi, come si tenti di adottare un

[42] V. PICOTTI, con il contributo di SALVADORI e FLOR, *Reati informatici, riservatezza, identità digitale*, cit., 16 ss.

[43] *Ibidem*.

[44] In argomento PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 91.

approccio pragmatico che tenga conto dei principi cardine dell'ordinamento giuridico.

5. Gli approdi giurisprudenziali

L'esigenza di adattare la tradizionale nozione di "*locus commissi delicti*" alla crescente dimensione tecnologica si è accentuata nel corso degli anni, data la continua evoluzione delle condotte illecite che ha posto l'interprete dinnanzi a questioni giuridiche di varia natura. In particolare, la giurisprudenza si è pronunciata diverse volte sull'argomento oggetto di analisi ed è a tal fine utile ripercorrere le pronunce rilevanti, per comprendere l'evolversi del contesto ermeneutico.

Al riguardo, appare utile richiamare gli sviluppi interpretativi inerenti alla fattispecie di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p., che ha riguardato il problema di individuazione del *locus commissi delicti* e fatto sorgere numerosi orientamenti contrastanti in seno alla giurisprudenza. Le Sezioni Unite della Corte di Cassazione sono intervenute per dirimere il contrasto giurisprudenziale relativo al *locus commissi delicti* con sentenza n. 17325 del 26 marzo 2015, aderendo all'orientamento che individua il luogo di consumazione del reato in quello in cui si trova il soggetto che effettua l'accesso abusivo o si mantiene abusivamente nello spazio informatico. Importante è, tuttavia, retrocedere per comprendere appieno i termini della questione, evidenziando come dalla diversa collocazione del momento consumativo e dal diverso modo di intendere la rete si arrivi a conclusioni parzialmente differenti, tenendo presente che il principio di diritto espresso dalla Corte appare applicabile ad altri casi di reato di mera condotta commessi *online*.

In particolare, il caso fondante l'ordinanza di remissione alle Sezioni Unite concerneva l'imputazione, tra gli altri, dell'art. 615-*ter* co. 2 e 3 c.p. nei confronti di un'impiegata della Motorizzazione Civile di Napoli e di un amministratore di una agenzia automobilistica, per essersi introdotti senza autorizzazione nel sistema informatico di un ente pubblico, per effettuare operazioni che esulavano dalle ordinarie mansioni assegnate all'imputata, e avvalendosi per lo scopo delle credenziali di accesso della stessa e delle postazioni informatiche di altri suoi

colleghi[45]. Orbene, il G.U.P. del Tribunale di Napoli aveva dichiarato la propria incompetenza territoriale in favore del Giudice del Tribunale di Roma, alla luce del fatto che i *server* violati fossero ubicati fisicamente a Roma; il G.U.P. del Tribunale di Roma dichiarava, a sua volta, conflitto negativo di competenza per territorio, ritenendo che il luogo rilevante per stabilire la consumazione del reato dovesse rinvenirsi nel posto in cui operava il soggetto agente, vale a dire dalla postazione *client* ove si era materialmente realizzato l'accesso. La Corte di Cassazione chiamata a dirimere tale conflitto ha postulato l'intervento delle Sezioni Unite, dati i possibili conflitti rinvenibili in casi non dissimili. Si contrapponevano, in sintesi, due diversi orientamenti: l'uno che riteneva competente il giudice del luogo ove era posto il soggetto, che effettuava il collegamento logico con il sistema; l'altro che riteneva, *a contrario*, competente il giudice del luogo ove era allocata la banca dati, il *server*, oggetto di violazione. Difatti, la precedente giurisprudenza di legittimità aveva individuato, con sentenza del 27 maggio 2013 n. 40303, il luogo di commissione del reato nel luogo di ubicazione del *server* centrale, ove si elaboravano e controllavano le credenziali di autenticazione delle postazioni remote, considerando irrilevante il momento in cui il reo poneva in essere il dialogo con il sistema, mediante digitazione e invio delle proprie credenziali. Quest'ultima sentenza considera rilevante, ai fini della consumazione, la collocazione del *server* del sistema violato, ove avviene il superamento delle barriere logiche che impediscono l'accesso a terzi ovvero ove si esaurisce il mantenimento non autorizzato nel sistema da parte del soggetto agente, dopo esservi entrato in modo legittimo, sicché in quel luogo si riscontrano dati probatori e si consente di riaffermare il diritto e la giustizia, ove è stata violata[46]. La Prima Sezione della Corte si discosta da questa interpretazione, ritenendo irrilevante la verificazione di una lesione del diritto alla riservatezza dei titolari dei diritti di *privacy*, in quanto la collocazione del *client* non verrebbe a considerarsi quale mero punto di accesso,

[45] Per un approfondimento concernente le considerazioni in fatto si veda l'ordinanza di rimessione della questione Cass. pen., Sez. I, ord. 28.10.2014, n. 52575.

[46] In tal senso PECORELLA, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico*, in commento alla sentenza della Cass. pen., Sez. I, sent. 27.05.2013 n. 40303, in *Dir. pen. cont.*, 11 ottobre 2013.

ma verrebbe a configurarsi quale componente informatica essenziale[47] e, essendo l'accesso abusivo un reato di mera condotta, non si pone il problema di individuare il luogo dell'evento. In virtù del presente contrasto, la Prima Sezione della Corte con l'ordinanza remittente ha posto il seguente quesito di diritto: «se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-*ter*, c.p., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il *server* che elabora e controlla le credenziali di autenticazione fornite dall'agente»[48]. Come si può evincere, un orientamento è legato alle modalità di funzionamento della rete, considerando rilevante il luogo in cui si instaura il dialogo con il sistema, e l'altro si ancora al classico concetto di fisicità del luogo in cui è situato il *server*. Le Sezioni Unite aderiscono alla tesi del giudice remittente, per cui ha preferito la tesi che privilegia le modalità di funzionamento dei sistemi informatici e telematici, piuttosto che il luogo ove è situato il *server*, vale a dire che conferisce rilevanza al luogo in cui parte il dialogo logico con il sistema, che viene individuato nel luogo ove è situata la postazione periferica. La Corte osserva che qualora il sistema debba considerarsi quale unitario – in virtù del fatto che è coordinato da un *software* di gestione che presiede al funzionamento della Rete – non sarebbe corretto ritenere che i flussi di dati si trovino solo nella banca dati, poiché quest'ultima sarebbe ubiquitaria sul territorio, compresente e consultabile da disparate postazioni remote abilitate all'accesso: ne deriva che sarebbe arbitrario scomporre le componenti della rete, separando i terminali periferici dal *server* principale, in quanto il sistema va inteso quale complesso inscindibile, in cui i terminali non si limitano a svolgere una funzione passiva accedendo alla rete, ma sono abilitati a immettere nuove informazioni e modificare parimenti quelle esistenti[49]. Le Sezioni Unite provvedono, poi, a specificare la nozione di "accesso", che non va a identificarsi con l'accesso al *server*

[47] Cfr. DE MARTINO, *Rimessa alle Sezioni Unite una questione in tema di competenza territoriale del delitto di accesso abusivo ad un sistema informatico,* in commento a Cass. Pen. Sez. I, ord. 28.10.2014, n. 52575, in *Dir. pen. cont.,* 20 gennaio 2015.

[48] Sul tema cfr. DE MARTINO, *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico,* in commento Cass. pen., Sez. Un., sent. 26 marzo 2015 n. 17325, in *Dir. pen. cont.,* 11 maggio 2015.

[49] V. Cass., Sez. Un., sent. 26 marzo 2015 n. 17325, 9 s., in *www.pluris-cedam.utetgiuridica.it.*

fisicamente allocato in un dato luogo, ma con l'introduzione telematica, vale a dire con l'instaurazione del dialogo logico con il sistema centrale e con i terminali ad esso collegati: l'accesso, pertanto, inizia con l'unica condotta umana avente natura materiale, consistente nella digitazione delle credenziali dalla postazione del *client*, per cui tutti gli atti successivi, secondo la Corte, deriverebbero dalle procedure automatizzate di comunicazione tra *client* e *server*. Una volta eseguita la procedura di *login*, infatti, si ha la violazione delle misure di sicurezza imposte dal titolare del sistema, che integra la condotta. Il riferimento al luogo in cui il soggetto ha agito è, peraltro, concorde con il principio del giudice naturale precostituito per legge, radicato al *locus commissi delicti*, di cui all'art. 25 della Costituzione, che nelle ipotesi più frequenti incarna il luogo in cui maggiormente si reperiscono le prove del reato e ove si sente maggiormente il bisogno di un ritorno alla legalità; per cui se l'azione del reo – perpetrata mediante un sistema informatico e pur priva dei classici connotati di fisicità – si è esplicata in quel luogo, sarebbe opportuno ivi collocare anche il fatto costituente reato, tale da rispondere all'individuazione di un giudice anche naturalisticamente competente, diversamente dal caso in cui si faccia riferimento al luogo ove è ubicato il *server*. Tali conclusioni sono state estese anche al mantenimento abusivo in un sistema informatico, in virtù del fatto che la condotta omissiva rilevante corrisponde all'inizio di un uso illecito dell'elaboratore, che violerebbe le regole imposte dal titolare del sistema: a questa bisogna riferirsi e non al momento di inserimento delle credenziali, posto che in quel momento il soggetto poneva in essere un'attività lecita[50]. Dall'uso illecito dell'elaboratore scaturirebbe parimenti un dialogo logico con il sistema da parte dell'operatore che agisce dalla postazione periferica, rendendo irrilevante il luogo in cui il *server* è allocato. Si rilevi come la Corte non abbia mancato di far riferimento per i casi dubbi ai criteri sussidiari di cui all'art. 9 c.p.p., volti a supplire all'inevitabile mancata identificazione del luogo da cui il soggetto opera. Ciononostante, permangono dei punti oscuri, che avrebbero meritato un maggior approfondimento, posto che il principio di diritto affermato risponde alle esigenze pratiche e giuridiche di evitare l'accentramento della competenza nei luoghi ove sono ubicati i *server* centrali e di

[50] In argomento FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative,* cit., 178.

rispettare il principio del giudice naturale, ma non è del tutto rispondente alle diverse questioni, che invece attengono al luogo di individuazione del reato in caso di reati cibernetici.

Si può notare come, in riferimento al delitto di frode informatica di cui all'art. 640-*ter*, si siano affrontate le medesime questioni. In particolare, le condotte tipiche del delitto in esame – l'attività manipolativa – sono l'alterazione del funzionamento di un sistema informatico o telematico ovvero l'intervento senza diritto su dati, informazioni o programmi in esso contenuti, le quali causano il duplice evento consumativo, l'ingiusto profitto con altrui danno. Parte della giurisprudenza, ritiene rilevante ai fini della consumazione la realizzazione dell'attività manipolativa o di alterazione del sistema, e quindi considera di ivi determinare il luogo di consumazione del reato, utilizzando quale criterio di collegamento per la competenza territoriale il luogo in cui si trova il *server* al cui interno sono archiviati i dati[51]. Diversamente, in pronunce successive, la Cassazione ha precisato che si considera maggiormente coerente con la struttura tipica della fattispecie, quale reato di evento, determinare il luogo di consumazione del reato, e il momento di consumazione, nel luogo e nel momento in cui si realizza l'ingiusto profitto con altrui danno, vale a dire ove si realizza l'evento: è necessario pertanto avere riguardo del luogo del profitto[52] (v. *infra* Cap. III, § 5). È opportuno notare che il delitto di frode informatica ha la medesima struttura e medesimi elementi costitutivi della truffa di cui all'art. 640 c.p., dalla quale se ne differenzia per esser l'attività fraudolenta rivolta all'elaboratore per cui, come la truffa, anche la frode informatica «si consuma nel momento e nel luogo in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui»[53].

La giurisprudenza di legittimità si è pronunciata finanche sul reato di diffamazione commessa da soggetto operante mediante uno spazio *web* di cui all'art. 595 del c.p., aggravata ai sensi del comma 3 per la particolare diffusività del mezzo[54]. Basti dire che, considerandosi la diffamazione c.d. *online* un reato a

[51] Cfr. Cass. pen., Sez. III, 24.05.2012, n. 23798, in *www.dejure.it*.

[52] V. Cass. pen., Sez. I, 07.10.2014, n. 46101, in *www.dejure.it*.

[53] Così, da ultimo, si è pronunciata la Cass. pen., Sez. II, 05.02.2020, n.10354, in *www.diritto24.ilsole24ore.com*.

[54] Per un'analisi più accurata concernente il delitto in questione vedi *infra*, Cap. III § 5, in quanto in questo paragrafo si intende evidenziare la conclusione a cui è giunta la giurisprudenza.

evento c.d. psicologico, la sua consumazione è stata ravvisata, secondo la giurisprudenza maggioritaria, nel momento e nel luogo in cui i terzi percepiscono l'espressione offensiva, vale a dire quando il collegamento viene attivato[55]. Essenziale, pertanto, ai fini della consumazione appare che la comunicazione debba essere ricevuta o recepita da almeno due persone, evidenziando come ciò non coincida con la semplice pubblicazione in rete del contenuto offensivo. Occorre sottolineare, tuttavia, che ai fini dell'individuazione della competenza risulta ostica l'applicazione di criteri oggettivi unici, in quanto di difficile identificazione: si pensi al criterio di prima pubblicazione, di immissione della notizia in rete o ancora di accesso del primo visitatore ovvero luogo in cui è allocato il *server*[56]: nei casi in cui sia impossibile individuare il luogo in cui si è consumato il reato, la competenza territoriale va determinata, qualora sia individuato il luogo in cui il contenuto offensivo dell'altrui reputazione è stato caricato e poi immesso in rete, ai sensi dell'art. 9 comma 1 c.p.p. in relazione a tale luogo in cui è avvenuta una parte dell'azione[57]; qualora questo non sia determinabile, si fa ricorso al secondo comma del medesimo articolo, in via suppletiva, che individua il giudice territorialmente competente in quello del luogo di residenza, dimora o domicilio dell'imputato.

Alla luce di queste pronunce emerge che la questione riguardante il *locus commissi delicti* deve essere affrontata in modo casistico, proprio al fine di tentare di dare soluzioni pratiche a livello interpretativo, che siano del resto compatibili con i principi cardine dell'ordinamento. Difatti, si scorge come, a seconda della fattispecie incriminatrice che viene in rilievo di volta in volta, siano state adottate soluzioni diverse intese ad adattare i criteri tradizionali al mutato contesto d'azione, che si rinviene nel campo virtuale.

6. Le linee evolutive

[55] Così Cass. pen., Sez. I, 5.02.2009, n. 8513, in *www.dejure.it*; in riferimento a questa pronuncia occorre premettere che particolare importanza riveste la sentenza Cass. Pen., Sez. V, 17.11.2000, n. 4741, la quale statuisce che la diffamazione è un reato di evento, il quale si consuma nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa.

[56] In questo senso Cass. pen., Sez. I, 15.03.2011, n. 16307, che riporta la motivazione di Cass. pen., Sez. I, 21.12.2010, n. 2739, in *www.dejure.it*.

[57] V. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 159, che richiama la giurisprudenza della Corte in riferimento alla sentenza Cass. pen., Sez. V, 22.02.2017, n. 8482.

Gli approdi giurisprudenziali appena esaminati fanno emergere come vi sia stata un'evoluzione ermeneutica nel corso degli anni, al passo con il crescente evolversi della realtà cibernetica. Le nuove tecniche con cui i criminali pongono in essere le fattispecie incriminatrici fanno sorgere nuove esigenze di tutela nei luoghi in cui il reato si consuma, in virtù del ripristino della giustizia nel luogo in cui questa risulta violata. Prima però di affrontare un'analisi circa le possibili interpretazioni evolutive dei classici principi, è opportuno attuare una precisazione di carattere terminologico: è bene evidenziare che la stessa nozione di spazio, intesa come aerea fruibile dai soggetti, perde i connotati di fisicità nell'ambito cibernetico, per cui non sarebbe delimitabile entro luoghi fisici. Va assegnata a tale nozione una duplice dimensione, da intendersi come spazio accessibile e fruibile da parte di tutti gli utenti e come spazio esclusivo del soggetto, quale area riservata, la quale sempre più spesso diviene oggetto di attacco. Queste diverse accezioni di spazio fanno sorgere diverse esigenze di tutela da parametrare ai principi dell'ordinamento penale, in quanto tale semantica peculiare si affaccia al mondo del diritto penale e richiede un approccio giudiziale flessibile su cui vanno modellati i principi tradizionali dell'ordinamento, tra cui quello di individuazione del luogo di consumazione del reato. In virtù di questa premessa, si evince che il *cyberspace* fa sorgere la necessità di adeguare i classici principi tradizionali al mutato contesto d'azione, principi che vanno interpretati in maniera evolutiva, in quanto rivestono un ruolo cardine per l'ordinamento giuridico.

Appare, a questo punto, utile partire dal principio di diritto espresso dalla sentenza delle Sezioni Unite n. 17325/2015, in materia di accesso abusivo ad un sistema informatico o telematico, per tentare di tracciare linee evolutive, tali da conformarsi alle diverse caratteristiche delle stesse nozioni basilari proprie del *cyberspace* e le diverse caratteristiche degli illeciti informatici. Suddetta sentenza, infatti, enuncia il principio di diritto per cui rilevante ai fini della determinazione del *locus commissi delicti* risulta il luogo ove il soggetto si trova nel momento in cui realizza la condotta, riconducendo a ipotesi determinate il caso in cui non sia possibile identificare la fonte dell'attacco, vale a dire la postazione del *client*. Preme considerare che tale assunto potrebbe essere strumentalizzato dal reo, il quale potrebbe così scegliere il Paese da cui far partire l'attacco, potendo quindi sferrare

l'attacco da quei Paesi in cui vi è una bassa tutela in campo tecnologico, i c.d. paradisi cibernetici[58]. Sarebbe ragionevole più che far riferimento al luogo dove si instaura il dialogo logico con il sistema, tener conto del legame tra il titolare dello spazio informatico e il bene giuridico protetto, riconoscendo rilevanza al luogo in cui si rinviene lo spazio informatico violato, che solitamente corrisponde al luogo in cui il titolare ha il proprio centro di interessi: in tal modo la competenza territoriale viene individuata in capo al giudice del luogo in cui la vittima possiede il centro di interessi, espressione dell'area virtuale violata. Ciò risponderebbe alle esigenze di impossibilità di identificazione del *client* da cui parte l'azione criminosa o del *server*, dato che sempre individuabile risulta la vittima del reato, valorizzando dunque il luogo di produzione del danno ed evitando eventuali azioni strumentali del reo; questo approccio, inoltre, conduce i singoli Paesi ad incrementare le disposizioni di tutela contro la criminalità informatica sia sul piano tecnico che giuridico, in quanto il titolare del diritto leso sarebbe spinto a collocare in quel luogo il proprio centro di interessi, in vista dell'ampia tutela accordatagli[59]. Resta da considerare, sempre a evidenziare la tenuta di tale approccio evolutivo, che è proprio nel luogo di produzione del danno che si svolgono le prime attività investigative, concernenti l'analisi dell'accesso e dei *file* del sistema, da cui si partirà per identificare la sorgente dell'attacco. Questo approccio è stato dapprima formulato dalla Corte di Giustizia europea in ambito civile in tema di vittima di una lesione del diritto della personalità via internet – Corte di Giustizia europea, 25 Ottobre 2011, C-509/09, C- 161-10 – la quale ha statuito che la competenza del giudice civile può essere allocata nel luogo di produzione del danno, in quanto il danno al diritto della personalità derivante da un'informazione immessa in rete verrebbe opportunamente valutato nel luogo in cui la vittima possiede il proprio centro di interessi, rispondendo così all'obiettivo di buona amministrazione della giustizia[60]. Tale approccio flessibile potrebbe essere istituito anche nell'ambito del

[58] Sul punto FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, cit., 1305 s.

[59] *Ivi*, 1308.

[60] Corte di Giustizia europea, 25 Ottobre 2011, C-509/09, C- 161-10, essa così stabilisce al punto 48: «Poiché l'impatto, sui diritti della personalità di un soggetto, di un'informazione messa in rete può essere valutata meglio dal giudice del luogo in cui la presunta vittima possiede il proprio centro di interessi, l'attribuzione di competenza a tale giudice corrisponde all'obiettivo di una buona

diritto penale, modellandosi così sulle esigenze di tutela del soggetto leso. Si consideri, inoltre, che tale criterio si rivela applicabile non solo in caso di accesso abusivo, ma anche in caso di commissione di ulteriori reati cibernetici, quali le truffe *online* o ancora il delitto di diffamazione *online*, in quanto ha il proposito di apprestare diretta tutela al soggetto leso dal reato, riferendosi al luogo di effettiva produzione del danno; diversamente, invece, si atteggia il criterio accolto dalle Sezioni Unite, il quale non sempre risulta di immediata applicazione, come nel caso di comunicazione abusiva di codici di accesso a sistemi informatici di cui all'art. 615-*quater*, qualora la condotta sia posta in essere tramite posta elettronica. Proprio la presenza di questi casi dubbi fa sorgere la necessità di adottare un criterio maggiormente universale, che tenga conto della realtà in cui va ad esplicarsi.

Tali considerazioni tentano di accogliere un'interpretazione evolutiva di un principio tradizionale, quale quello di territorialità, proprio al fine di adattarlo al differente contesto tecnologico. Queste conclusioni potrebbero essere sopite mediante un intervento legislativo nazionale che tenga conto delle peculiari caratteristiche che il delitto viene ad assumere nel *cyberspace*, evitando in tal modo forzature in campo ermeneutico. Occorre però tener conto della natura transnazionale degli illeciti cibernetici, che richiamano la necessità di una stretta cooperazione internazionale per un efficace contrasto a tale criminalità, mediante l'armonizzazione delle legislazioni, che superi i limiti degli interventi legislativi nazionali, vincolanti per il singolo Stato.

Al fine di comprendere al meglio i termini della questione ancora in corso, è opportuno passare in rassegna le singole fattispecie incriminatrici, che risentono del difficile problema dell'individuazione del *locus commissi delicti* e successivamente condurre un'analisi circa le soluzioni *de iure condito* adottabili e trarre spunti per un'ulteriore riflessione, che miri ad individuare le possibili prospettive *de iure condendo* nell'attesa di un intervento legislativo.

amministrazione della giustizia». La sentenza è consultabile presso il sito *www.pluris-cedam.utetgiuridica.it*.

CAPITOLO III

LE SINGOLE FATTISPECIE INCRIMINATRICI

SOMMARIO: 1. L'accesso abusivo ad un sistema informatico o telematico: art. 615-*ter*. – 1.1. Criticità della sentenza della Corte di Cassazione S.U. n. 17325 del 2015 – 2. La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici: art. 615-*quater* c.p. – 3. Interruzione illecita di comunicazioni informatiche o telematiche: art. 617-*quater* c.p. – 4. La diffamazione online: art. 595 co. 3 c.p. – 5. La frode informatica: art. 640-*ter* c.p. – 6. La truffa comune realizzata mediante l'utilizzo di strumenti tecnologici o la rete: art. 640 c.p. – 7. Indebito utilizzo e falsificazione di carte di credito e di pagamento: art. 493-*ter* c.p.

1. L'accesso abusivo ad un sistema informatico o telematico: art. 615-*ter*

L'esplosione delle nuove tecnologie informatiche e telematiche, l'utilizzo, sempre più inteso, di sistemi di elaborazione dei dati hanno prodotto, anche sul piano giuridico, delle rilevanti conseguenze, come più volte sottolineato nei precedenti capitoli. Per quanto concerne il diritto penale, l'avanzare del modello della c.d. società digitale ha spinto i vari Stati ad introdurre nuove figure di illeciti, i c.d. *computer crimes*[1], che risentono dell'aterritorialità della rete, ponendo problemi sul punto di individuazione del *locus commissi delicti*.

Tra i principali *computer crimes* della disciplina italiana figura l'accesso abusivo ad un sistema informatico o telematico, ai sensi dell'art. 615-*ter* c.p. Ripercorrendo brevemente la struttura della fattispecie, è utile riportare alla memoria che tale disposizione punisce chiunque "abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo".

Si rammenti che l'articolo in commento è stato inserito all'interno del codice penale dalla legge n. 547 del 23 dicembre 1993[2], al fine di contrastare i fenomeni degli attacchi informatici da parte degli *hackers*, dando così seguito alla

[1] Cfr. ZENO ZENCOVICH, *Informatica ed evoluzione del diritto,* in *Il diritto dell'informazione e dell'informatica*, 1/2003, 89 ss., ove si evidenzia che «Se il diritto si atteggia alla società come un guanto alla mano, è inevitabile che la diffusione delle tecnologie informatiche influenzi il diritto». Per un approfondimento riguardante i reati informatici, si veda MANTOVANI, *Diritto Penale parte speciale I*, "*Delitti contro la persona*", Padova, 2008.

[2] V. *supra* Cap. I, § 4.1.

Raccomandazione del Consiglio di Europa del 1989[3], che equipara il domicilio informatico a quello fisico[4].

I luoghi di dimora, infatti, non si esauriscono oggi nei luoghi connotati da materialità, ma comprendono i luoghi immateriali considerati alla stregua di un'espansione ideale del domicilio tradizionale, andando a costituire la proiezione spaziale della persona, la cui libertà individuale si traduce anche nell'interesse alla sicurezza dei propri sistemi informatici. La norma, dunque, è correttamente collocata tra i delitti contro l'inviolabilità del domicilio, tutelato a livello costituzionale dall'art. 14 della Costituzione, e svolge la medesima funzione sociale riconosciuta all'art. 614 c.p., concernente la violazione del domicilio fisico.

Il reato in oggetto viene dai più ritenuto plurioffensivo, in quanto, oltre al domicilio, esso è posto a presidio di ulteriori beni giuridici quali il c.d. *ius excludendi alios*, tutelando così la riservatezza e la *privacy* dell'individuo[5]. Continuando l'analisi della disposizione, si ritiene pacificamente che il 615-*ter* sia un reato di condotta e, pertanto, non è necessario, ai fini della relativa integrazione, che l'agente violi effettivamente la riservatezza del titolare del sistema[6]. Proprio per tale motivo la struttura pone problemi quando la condotta è commessa *online* ai fini dell'individuazione del luogo di commissione del reato.

---

[3] Sul punto, il Consiglio dell'Unione Europea ha recentemente evidenziato nella decisione quadro presentata dalla Commissione COM (2002) relativa agli attacchi contro i sistemi di informazione, Bruxelles, del 19 aprile 2002 che: "*Le legislazioni penali nel settore degli attacchi ai sistemi di informazione devono essere ravvicinate al fine di garantire la cooperazione giudiziaria e di polizia più ampia possibile nel settore dei reati attinenti ad attacchi a sistemi di informazione, e di contribuire alla lotta contro la criminalità organizzata ed il terrorismo*". Cfr. anche Cap. I, § 4.

[4] Per quanto concerne le raccomandazioni del Consiglio d'Europa, prima dell'entrata in vigore della l. n. 547 del 1993, si veda PICOTTI, *Studi di diritto penale dell'informatica,* Verona, 1992; PICOTTI, *voce Reati informatici*, in *Enc. giur.*, Agg., VIII, Roma, 2000, 1 ss.; PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. Internet*, 2005, 189 ss. Si veda inoltre GERCKE, *Impact of the Lisbon Treaty on Fighting Cybercrime in the EU. The redefined role of EU and the change in approach from patchwork to comprehensiveness*, in *Cri*, 3/2010, 75 ss.

[5] Così BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 9/1995, 2329 ss.

[6] In questo senso, PECORELLA, *Diritto penale dell'informatica*, cit., 306 ss., 349-350; FLOR, *Art. 615*-ter *c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto* in *Dir. pen. proc*., 2008, 106 ss.; FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo* jus excludendi alios, in *Dir. pen. proc*., 2005, 85 ss.

La norma incriminatrice punisce due precipue condotte: l'accesso abusivo al sistema nonché quella del mantenimento illecito[7]. Proprio per comprendere compiutamente la portata applicativa del 615-*ter* sotto il profilo oggettivo, è necessario innanzitutto individuare l'esatta nozione sia di sistema informatico che di condotta abusiva, entrambe rimesse all'interpretazione giurisprudenziale, alla luce del silenzio legislativo sul punto. In particolare, il diritto vivente ha fornito una definizione di sistema informatico applicabile, tendenzialmente, a tutte le fattispecie penali che ad esso si richiamano: con sistema informatico si intende il complesso di apparecchiature finalizzate a compiere una qualsivoglia funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche[8].

Per quanto concerne, invece, il termine "abusivamente" si è chiarito che con esso non si indicano solo e unicamente le condotte di chi raggiri i sistemi di sicurezza nell'accesso, ma si indicano altresì come abusive le condotte di chi, pur conoscendo la *password,* si introduca nel sistema senza il consenso del titolare o comunque oltre i limiti delle prescrizioni impartite[9]. Sul punto, una recente sentenza della Cassazione a Sezioni Unite[10] ha riconosciuto integrato il reato *de quo* nel caso del pubblico ufficiale che, pur essendo abilitato ad accedere al sistema, vi acceda o vi si mantenga per ragioni estranee rispetto al compimento delle proprie mansioni. L'orientamento giurisprudenziale richiamato, da considerarsi prevalente, si fonda sulla considerazione preliminare, in base alla quale l'illecito non si caratterizza per l'effrazione del sistema informatico, altrimenti, ragionando *a contrario*, non si dovrebbe punire la condotta di chi, avendo effettuato l'accesso mediante le chiavi di sicurezza, vi si mantenga contro la volontà del titolare. Da quanto rilevato, ne risulta una nozione di accesso abusivo particolarmente ampia.

L'art. 615-*ter* c.p. prevede, inoltre, un aggravamento di pena qualora il fatto venga commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio,

---

[7] Per un approfondimento, si vedano: PICA, Computer crimes *e uso fraudolento delle nuove tecnologie*, Seminario di studi, Roma, 15 dicembre 2000; MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ*., 1992, 364 ss.; FONDAROLI, *Osservazioni intorno ad alcune delle norme contenute nella recente normativa italiana sui computer crimes*, in SOLA, FONDAROLI, *La nuova normativa in tema di criminalità informatica: alcune riflessioni*, CLUEB, Bologna 1995, 20.

[8] Per quanto concerne la definizione di sistema informatico, si veda Cass. pen., Sez. VI, 04.10.1999, n. 3067, in *Cass. pen*., 11/2000, 2990.

[9] Si consideri Cass. pen., Sez. V, 06.06.2017, n. 52572, in *www.dejure.it*.

[10] Si veda Cass. pen, S.U., 08.09.2017, n. 41210, in *www.giurisprudenzapenale.it*.

con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, ovvero da chi eserciti, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema; la pena è aggravata qualora per commettere il fatto si adoperi violenza sulle cose o alle persone o si sia palesemente armati; risulta altresì aggravata se dal fatto derivi la distruzione o il danneggiamento del sistema o dei dati in esso contenuti ovvero l'interruzione totale o parziale del suo funzionamento; ancora, costituisce aggravante, l'accesso a sistemi di interesse militare, di ordine pubblico o di pubblica sicurezza. Per quanto concerne quest'ultima circostanza aggravante si è evidenziato che, per sistema di interesse pubblico, si intende anche il sistema appartenente all'operatore privato concessionario pubblico allorquando lo stesso operi per il soddisfacimento di bisogni generali della collettività[11].

La presenza di una delle circostanze aggravanti rileva, non solo ai fini del trattamento sanzionatorio, che di conseguenza risulterà più severo, ma anche ai fini della procedibilità. La fattispecie base è, difatti, procedibile a querela della persona offesa, mentre la fattispecie aggravata è procedibile d'ufficio.

Sotto il profilo soggettivo, è richiesto il dolo generico: l'agente deve, con coscienza e volontà, accedere al sistema informatico protetto da misure di sicurezza.

Volgendo l'attenzione alla problematica oggetto di studio, già a far data dall'entrata in vigore della disposizione, si sono posti problemi in ordine alla corretta individuazione del *locus commissi delicti.* Difatti, non sono di poco conto i problemi applicativi posti dall'art. 8 c.p.p. che, nel definire il criterio attributivo di competenza territoriale, guarda agli spazi fisici e non di certo virtuali[12].

Al fine di esaminare nel dettaglio la questione, è utile riprendere le considerazioni avanzate *supra* (v. Cap. II, § 5).

Un primo orientamento giurisprudenziale stabilisce che il luogo di consumazione corrisponde al luogo in cui si trova il *server* violato[13]. Pertanto, chiarisce tale orientamento richiamato che «il luogo in cui si consuma il reato,

[11] Cass. pen., Sez. V, 18.12.2014, n. 10121, in *www.pluris-cedam.utetgiuridica.it*.
[12] Per un approfondimento si veda Cap. II, § 2.2.
[13] Cass. pen., Sez. I, 27.09.2013, n. 40303, in *www.dirittopenalecontemporaneo.it*.

quindi, non è quello nel quale vengono inseriti i dati idonei a entrare nel sistema, bensì, quello in cui si entra nel sistema [...]. Non possono prendersi in considerazione, pertanto, ai fini della determinazione del luogo di consumazione del reato, né le eventuali condotte successive di acquisizione ed uso dei dati, né il luogo in cui l'accesso al sistema è iniziato attraverso i terminali che costituiscono strumenti di accesso. La procedura di accesso deve ritenersi atto prodromico alla introduzione nel sistema che avviene solo nel momento in cui si entra effettivamente nel server, dopo avere completato la validazione delle credenziali dell'utente che viene fatta dal sistema centrale che, nella specie, si trova a Roma. D'altro canto, il luogo in cui si forma la volontà dell'agente di commettere il reato, ovvero quello in cui l'agente predispone le attività prodromiche e preparatorie, finalizzate alla condotta illecita, ben può essere diverso da quello nel quale si pone in essere la condotta giuridicamente rilevante e in cui, per i reati di mera condotta come quello in esame, si consuma il reato. E la condotta sanzionata non è costituita dall'utilizzo delle credenziali o altra attività equipollente effettuata nell'elaboratore remoto»[14].

Invero, un secondo orientamento, sposato dalle Sezioni Unite della Cassazione in commento, critica la precedente impostazione rilevando che la rete deve essere considerata unitaria, da cui ne deriva che la gestione e lo scambio di dati corrisponde ad una sola unità di elaborazione, per cui il terminale attraverso cui il soggetto agente inserisce le credenziali costituisce un elemento strutturale essenziale della rete, a tal fine assume, quindi, rilevanza «il luogo di ubicazione della postazione con cui l'utente accede o si introduce nel sistema che contiene l'archivio informatico»[15].

La Corte ritiene dunque preferibile la tesi che individua il *locus commissi delicti* facendo riferimento alla condotta del soggetto agente, piuttosto che quella che privilegia il luogo ove è materialmente allocato il *server* che controlla le credenziali di accesso del *client.*

Le Sezioni Unite giungono a queste conclusioni sulla base di una serie di argomenti. Innanzitutto, mettono in evidenza le peculiarità della fattispecie,

[14] *Ivi*, 7 ss.
[15] Cass. pen., Sez. Un., sent. n. 17325 del 26 marzo 2015.

ponendo in luce come le nozioni delle due condotte incriminate non siano collegate ad una realtà spaziale comunemente intesa, bensì ad una realtà immateriale dato che hanno ad oggetto sistemi informatici o telematici che archiviano ovvero gestiscono componenti immateriali. Pertanto, dato che le due nozioni prescindono dal dato spaziale, è da considerare erroneo l'orientamento che individua, quale luogo di consumazione, il luogo fisico ove è posizionato il *server* che controlla l'autenticazione del *client*[16]. Difatti, muovendo da una visione strettamente tecnica, il sistema telematico si connota per la sua unitarietà essendo coordinato da un *software* di gestione che presiede al funzionamento della rete, alla condivisione della banca dati, alla archiviazione delle informazioni, alla distribuzione e all'invio dei dati ai singoli terminali tra loro interconnessi[17].

Alla luce di ciò, l'accesso nel sistema informatico non si identifica con l'ingresso dell'agente nel *server* fisico, ma con l'ingresso telematico nel circuito del sistema centrale.

[16] Sul punto le Sez. Un. del 2015 evidenziano che: «Non può essere condivisa, allora, la tesi secondo la quale il reato di accesso abusivo si consuma nel luogo in cui è collocato il *server* che controlla le credenziali di autenticazione del *client*, in quanto, in ambito informatico, deve attribuirsi rilevanza, più che al luogo in cui materialmente si trova il sistema informatico, a quello da cui parte il dialogo elettronico tra i sistemi interconnessi e dove le informazioni vengono trattate dall'utente. Va rilevato, infatti, come il sito ove sono archiviati i dati non sia decisivo e non esaurisca la complessità dei sistemi di trattamento e trasmissione delle informazioni, dal momento che nel cyberspazio (la rete internet) il flusso dei dati informatici si trova allo stesso tempo nella piena disponibilità di consultazione (e, in certi casi, di integrazione) di un numero indefinito di utenti abilitati, che sono posti in condizione di accedervi ovunque. Non è allora esatto ritenere che i dati si trovino solo nel server, perché nel reato in oggetto l'intera banca dati è "ubiquitaria", "circolare" o "diffusa" sul territorio, nonché contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso. A dimostrazione della unicità del sistema telematico per il trattamento dei dati, basti considerare che la traccia delle operazioni compiute all'interno della rete e le informazioni relative agli accessi sono reperibili, in tutto o in parte, sia presso il *server* che presso il *client*. Né può in contrario sostenersi, come afferma l'orientamento che in questa sede si ritiene di non condividere, che le singole postazioni remote costituiscano meri strumenti passivi di accesso al sistema principale e non facciano altrimenti parte di esso».

[17] Le Sezioni Unite richiamate, dunque, affermano che «è arbitrario effettuare una irragionevole scomposizione tra i singoli componenti dell'architettura di rete, separando i terminali periferici dal server centrale, dovendo tutto il sistema essere inteso come un complesso inscindibile nel quale le postazioni remote non costituiscono soltanto strumenti passivi di accesso o di interrogazione, ma essi stessi formano parte integrante di un complesso meccanismo, che è strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del *client*. I terminali, secondo la modulazione di profili di accesso e l'organizzazione della banca-dati, non si limitano soltanto ad accedere alle informazioni contenute nel *database*, ma sono abilitati a immettere nuove informazioni o a modificare quelle preesistenti, con potenziale beneficio per tutti gli utenti della rete, che possono fruire di dati più aggiornati e completi per effetto dell'interazione di un maggior numero di operatori».

L'introduzione abusiva si integra, dunque, nel luogo in cui l'operatore materialmente procede a digitare la chiave di accesso o esegue la procedura di *login*, così superando le misure di sicurezza. Da ciò consegue che il *locus commissi delicti* si andrà a identificare con quello della postazione remota mediante la quale l'agente si interfaccia con l'intero sistema, digita le credenziali di autenticazione e preme il tasto di avvio: la condotta è antigiuridica nel momento in cui l'agente accede senza o oltre i limiti delle autorizzazioni.

L'avvenuta risposta o validazione delle credenziali da parte del *server* rileva, tuttavia, ai fini della definizione del tentativo punibile. Se l'agente inserisce delle credenziali, ma il *server* non accetta l'ingresso allora la condotta verrà punita come tentativo, ai sensi del combinato disposto di cui agli artt. 615-*ter* e 56 c.p.

Le Sezioni Unite, al fine di avallare la propria tesi, richiamano anche la Carta costituzionale, affermando che far coincidere il *locus commissi delicti* con il luogo in cui l'utente ha agito sul computer è compatibile con il concetto di giudice naturale radicato al luogo di consumazione del reato di cui all'art. 25 della Costituzione. Viene, difatti, specificamente richiamata la giurisprudenza della Corte Costituzionale[18] dalla quale si deduce che se l'azione dell'uomo è posta in essere in un certo luogo – sia pure attraverso l'uso di uno strumento informatico, che prescinde dunque dal concetto di territorialità – non vi sono ragioni per escludere che quel "fatto" non si sia verificato proprio in quel luogo ai fini della legge penale, così consentendo l'individuazione di un giudice competente anche naturalisticamente, oltre che formalmente, in accordo con i principi cardine dell'ordinamento.

L'ultimo argomento richiamato dalla Corte a Sezioni Unite si fonda sulla configurazione dell'aggravante di cui al comma 2 n. 2, concernente il soggetto che abbia usato violenza sulle cose o sulle persone ovvero sia palesemente armato: tale aggravante risulta strettamente ancorata al comportamento dell'agente, situato in un determinato luogo, per cui non avrebbe alcun senso ritenere che il *locus* debba rinvenirsi nel luogo in cui è ubicato il *server* e non in quello in cui si sia posta in essere l'attività violenta dell'agente, che legittima l'aggravio del trattamento sanzionatorio.

[18] Si veda Corte Cost., sent. n. 168, del 5.04.2006, in *www.giurcost.it*

Alla luce di tutte queste considerazioni le Sezioni Unite enucleano il seguente principio di diritto – cui si è fatto riferimento anche nel precedente capitolo – «Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter c.p., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente»[19].

1.1. Criticità della sentenza della Corte di Cassazione S.U. n. 17325 del 2015

Con la sentenza in oggetto le Sezioni Unite hanno inteso dirimere un contrasto emergente in giurisprudenza concernente l'individuazione del luogo di commissione del reato. La scelta accolta dalle Sezioni Unite è volta, certamente, ad evitare l'accentramento della competenza nei luoghi ove sono ubicati i server centrali e mantenere saldo il principio del giudice naturale, ma manca di considerare nel dettaglio le ipotesi dubbie, i c.d. casi *border line,* per cui la Corte ha inteso rinviare ai criteri suppletivi di cui all'art. 9 c.p.p. Il principio avanzato dalla Corte di Cassazione presta, inoltre, il fianco all'adozione di una *fictio* giuridica, in quanto afferma di considerare la rete come un sistema unitario, sebbene tale scelta non si concili con il tradizionale protocollo di comunicazione *client-server*[20].

Sulla base di questa breve premessa, la prima e saliente critica mossa dalla dottrina alla soluzione ermeneutica avanzata dalle Sezioni Unite consiste nella insensibilità ad interpretazioni in chiave evolutiva, alla luce del progresso tecnologico, dell'accesso abusivo[21].

Si è visto che la decisione argomenta la scelta del *locus commissi delicti* nei termini sopracitati valorizzando la centralità, nella stesura della norma, della condotta dell'agente, le cui peculiarità svolgono la funzione di distinguere la fattispecie base da quelle aggravate. Tale impostazione ermeneutica appare errata, in quanto va sottolineato che la redazione della norma è fortemente ancorata al tempo in cui la stessa venne alla luce. Difatti, negli anni 90' le tecnologie e le strutture informatiche non avevano raggiunto il loro massimo apice e, spesso, nella

[19] Cass. pen., Sez. Un., sent. n. 17325 del 26 marzo 2015.

[20] V. Cap. II, § 4.

[21] In tal senso FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite,* cit., 1291; PICOTTI, Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati, in PICOTTI (a cura di*), Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 ss.

prassi, gli accessi non autorizzati venivano effettuati attraverso un contatto materiale tra l'agente e il terminale oggetto della violazione. Molto più rari erano, dunque, gli accessi da remoto, non disponendosi delle tecnologie adatte a tal fine. Va evidenziato, inoltre, che sul piano strutturale, l'art. 615-*ter* è formulata in termini paralleli all'art. 614 c.p., per cui i riferimenti impliciti al luogo della condotta sarebbero frutto di questa formulazione speculare.

Ulteriori problematiche emergenti da tale principio di diritto si rinvengono nella possibilità per il soggetto agente di strumentalizzare la decisione in esame, scegliendo, a tal proposito, il luogo da cui far partire il comportamento deviante, così rischiando l'istituzione di prassi che vedono i criminali informatici agire dai c.d. paradisi cibernetici, luoghi in cui la legislazione posta a tutela di tali attacchi risulta carente.

Sempre in virtù dell'evoluzione tecnologica, occorre sottolineare che non è infrequente – sebbene le Sezioni Unite sembrino definirla come un'evenienza residuale[22] – l'ipotesi in cui vi sia l'impossibilità di determinare il luogo dal quale il *client* agisce, violando il sistema. Sulla base di questo assunto, si può affermare, dunque, che anche il rapporto agente-dispositivo, considerato momento centrale della condotta, sovente è connotato da una dimensione immateriale – basti pensare alle ipotesi di accesso abusivo perpetrate mediante *devices* mobili. L'attività umana, infatti, si manifesta esteriormente con l'operazione di digitazione di comandi, di sovente mediante una tastiera, da cui deriva l'attivazione di un procedimento automatizzato di elaborazione delle informazioni immesse, che viene svolto da un *software*[23]. Non va trascurato, tuttavia, che l'incessante evolversi della tecnologia ha dato vita ad un continuo progredire dei rapporti tra le condotte materiali e gli elaboratori elettronici, per cui oggi l'attività umana di dialogo con il sistema non richiede necessariamente un contatto diretto con il sistema violato, ma si esplica attraverso processi di automazione: esemplificando, l'agente potrebbe utilizzare un dispositivo di sua proprietà o solo in suo possesso per effettuare l'accesso ad

[22] Le Sezioni Unite così testualmente affermano «Nelle ipotesi, davvero scolastiche e residuali, nelle quali non è individuabile la postazione da cui agisce il *client*, per la mobilità degli utenti e per la flessibilità di uso dei dispositivi portatili, la competenza sarà fissata in base alle regole suppletive (art. 9 c.p.p.)».

[23] V. FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, cit., 1302.

Internet attraverso diversi *server*, sistemi delocalizzati rispetto al luogo in cui si trova, per poi introdursi abusivamente in uno specifico sistema-spazio informatico che potrebbe essere non individuabile territorialmente e fisicamente[24].

Alla luce di tali dati, si evince che l'assunto accolto dalle Sezioni Unite – che relega ad ipotesi "scolastiche" i casi in cui non risulti possibile individuare il luogo da cui parte il dialogo logico con il sistema – si riveli in evidente contrasto con la realtà odierna caratterizzata dall'esplosione di nuove tecnologie, che confinano a ipotesi residuali i casi in cui risulti identificabile il luogo da cui parte l'azione del soggetto.

Al fine di prospettare una soluzione rispondente alle esigenze emergenti dal particolare contesto cibernetico, la dottrina ha avanzato proposte ermeneutiche, che mirano a valorizzare il luogo ove si è prodotto il danno e, in particolare, ove il soggetto passivo ha il proprio centro di interessi, tutelando così maggiormente il soggetto leso in accordo con il bene giuridico tutelato dalla norma[25]. Peraltro, anche la Corte di Giustizia[26], in tema di offesa ai diritti di personalità effettuata mediante *Internet*, ha ritenuto che il foro competente coincidesse con il luogo in cui si concretizza il danno cagionato e non il luogo della condotta. Ciò si giustifica in virtù del fatto che la lesione subita da un soggetto, derivante da un'informazione diffusa in rete, può essere meglio valutata dal giudice del luogo in cui la vittima ha il proprio centro di interessi, così perseguendo una migliore amministrazione della giustizia.

[24] *Ivi*, 1303.

[25] *Ivi*, 1307 ss.; si noti che le linee evolutive concernenti l'individuazione del *locus commissi delicti* sono state trattate nel precedente capitolo: v. *supra* Cap. II, § 6.

[26] Corte di Giustizia UE, 25 ottobre 2011 (C-509/09, C161-10) che così dispone: «L'art. 5, punto 3, del regolamento (CE) del Consiglio 22 dicembre 2000, n. 44/2001, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, deve essere interpretato nel senso che, in caso di asserita violazione dei diritti della personalità per mezzo di contenuti messi in rete su un sito Internet, la persona che si ritiene lesa ha la facoltà di esperire un'azione di risarcimento, per la totalità del danno cagionato, o dinanzi ai giudici dello Stato membro del luogo di stabilimento del soggetto che ha emesso tali contenuti, o dinanzi ai giudici dello Stato membro in cui si trova il proprio centro d'interessi. In luogo di un'azione di risarcimento per la totalità del danno cagionato, tale persona può altresì esperire un'azione dinanzi ai giudici di ogni Stato membro sul cui territorio un'informazione messa in rete sia accessibile oppure lo sia stata. Questi ultimi sono competenti a conoscere del solo danno cagionato sul territorio dello Stato membro del giudice adito».

2. La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici art. 615-*quater* c.p

Il problema del *locus commissi delicti* coinvolge ulteriori fattispecie criminose a cui non risulta applicabile il principio di diritto espresso dalle Sezioni Unite con la sentenza precedentemente analizzata. Tra queste vi è la norma di cui all'art. 615-*quater* c.p., la quale incrimina chiunque si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiavi o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, punendolo con la reclusione sino a un anno e con la multa sino a euro 5.164.

Si tratta di un reato introdotto con la legge Conso, plurioffensivo e dal carattere sussidiario che, come l'art. 615-*ter* c.p., volge alla tutela del domicilio in senso dematerializzato e della riservatezza dei dati e delle comunicazioni informatiche.

La fattispecie in esame si sostanzia, il più delle volte, in una condotta prodromica all'accesso abusivo. In virtù di tale assunto recentissima giurisprudenza, sulla scia di un orientamento sostanzialmente unitario, ha evidenziato come i due reati non possano concorrere tra loro in quanto la detenzione ovvero diffusione di codici di accesso rimane assorbita, qualora si consumi il più grave delitto di accesso abusivo, in quanto si ritiene che la condotta di cui all'art. 615-*quater* costituisca un antecedente logico necessario, «sempre che quest'ultimo sia contestato, procedibile e integrato nel medesimo contesto spazio-temporale, in danno della medesima persona fisica»[27].

Vi è, tuttavia, dottrina che invece riconosce la possibilità di concorso in quanto ritiene che le due fattispecie incriminatrici si connotino per profili di differenziazione riguardanti la struttura e l'oggetto di tutela delle stesse, ritenendo possibile il concorso attenendo i reati summenzionati a condotte diverse, per cui nel caso in cui il soggetto si procuri un codice e successivamente lo utilizzerà per accedere ad un sistema altrui, integrerà entrambe le fattispecie criminose[28].

[27] Cfr. Cass. pen., Sez. II, 20.05.2019, n. 21987, in *www.pluris-cedam.utetgiuridica.it*.
[28] PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 83.

Con la disposizione in commento pare che il legislatore italiano, tra i pochi al mondo[29], abbia inteso recepire le indicazioni fornite nell'ambito del XV Congresso dell'*Association Internationale de Droit Pénal*, nell'ambito del quale si è affermata l'utilità dell'incriminazione del commercio di codici d'accesso ottenuti illecitamente, al fine di bloccare lo scambio di credenziali di accesso tra *hackers*[30], ponendo in luce come ci si trovi dinnanzi a condotte transnazionali, indice della necessità di arretrare la soglia di punibilità, mediante un'anticipazione della tutela penale.

Sotto il profilo oggettivo, uno dei problemi interpretativi che pone la norma riguarda la punibilità o meno della condotta di mera detenzione dei codici di accesso. Come precedentemente affermato – v. *supra* Cap. I, § 4.1 concernente l'introduzione della legge n. 547/1993 – nella rubrica di cui all'art. 615-*quater* c.p. viene menzionata la condotta della "detenzione", ma la stessa viene omessa nel corpo dell'articolo. Da ciò deriva che, stando ad una lettura rigorosa della disciplina volta al rispetto del principio di legalità, si dovrebbe ritenere penalmente irrilevante la mera detenzione di codici di accesso, dovendosi escludere, peraltro, l'ipotesi di configurabilità del tentativo, che arretrerebbe ulteriormente la soglia di rilevanza penale. Ciononostante, vi è chi ritiene che, al contrario, anche la detenzione sia una condotta tipica e idonea, rientrante nell'atto di "procurarsi" i codici, tale da integrare la fattispecie[31]: essa costituirebbe, infatti, una prova di procacciamento dei codici.

Altri profili ostici della fattispecie, i quali pongono seri dubbi di costituzionalità, si rinvengono rispetto alla conciliabilità della stessa con il principio di proporzione. L'art. 615-*quater* c.p. appartiene ai reati di pericolo indiretto quindi

[29] La scelta del legislatore italiano si accompagna a quella intrapresa dagli Stati Uniti d'America che puniscono con una legge federale del 1986 il commercio di codici d'accesso. Sul punto, si veda GRIFFITH, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem, in Vanderbilt Law Review*, 1990, 481.

[30] Colloquio di *Wurzburg* nell'ottobre 1992 e pubblicato in *Rev. int. dr. pén.*, (vol. 64), 1993, 673 ss. Contrariamente, gli altri stati di *civil law* non hanno provveduto ad introdurre una norma analoga a quella dell'art. 615-*quater* c.p., ritenendo probabilmente insuperabili le problematicità legate ad un'eccessiva anticipazione della tutela penale della riservatezza.

[31] BORRUSO, BUONOMO, CORASANITI, D'AIETTI, *Profili penali dell'informatica*, Milano, 1994.

al *genus* di quei reati che, in via del tutto eccezionale, puniscono atti meramente preparatori[32].

In questi casi straordinari, bisogna, dunque, vagliare se l'arretratezza della soglia di tutela penale ad una fase di pericolo solo indiretto sia giustificata dalla particolare preminenza del bene giuridico protetto. Sulla base di questo assunto, secondo alcuni, sebbene la riservatezza dei dati informatici sia un bene giuridico di rilievo esso certamente non assurge ad un bene di rango primario.

Sotto il profilo oggettivo, l'art. 615-*quater* c.p. definisce l'oggetto materiale del reato come "codici, parole, chiave o altri mezzi idonei". La fattispecie può dunque concernere dei codici di accesso – siano essi alfabetici, numerici, o alfanumerici – ovvero, più in generale, "altri mezzi idonei all'accesso" – tra essi si rinvengono, ad esempio, un tesserino magnetico da inserirsi in un lettore ottico. La norma, inoltre, punisce anche la condotta di colui che fornisce delle indicazioni o istruzioni idonee volte all'elusione dei sistemi e dei meccanismi di sicurezza[33]. Vi è, tuttavia, dottrina minoritaria che interpreta l'idoneità dell'indicazione o istruzione in senso differente, sostenendo, invece, che l' espressione valga a indicare quelle che siano idonee a permettere o comunque semplificare l'individuazione, la realizzazione, ovvero la riproduzione o ancora la diffusione, comunicazione e consegna di mezzi di accesso a sistemi informatici o telematici protetti[34].

Interessante è notare che la giurisprudenza ha ritenuto applicabile la fattispecie in esame in una serie di particolari casi. Il primo di essi riguarda l'acquisizione abusiva del numero di serie attribuito all'apparecchio telefonico, appartenente ad altro soggetto, ritenendola configurabile sull'assunto che, mediante

---

[32] Si veda ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Milano 1983, 163 ss. Sul principio di proporzione si veda anche la pronuncia della Corte Costituzionale del 25.07.1994, n. 341, in *Giur. cost*., 1994, 2802 ss., che rinviene il principio di proporzione nell'art. 27 comma 3 Cost., in quanto «la palese sproporzione del sacrificio della libertà personale» provocata dalla previsione di una sanzione penale manifestamente eccessiva rispetto al disvalore dell'illecito «produce [...] una vanificazione del fine rieducativo della pena», sia nell'art. 3 Cost., dal momento che «il principio di uguaglianza esige che la pena sia proporzionata al disvalore del fatto illecito commesso, in modo che il sistema sanzionatorio adempia nel contempo alla funzione di difesa sociale ed a quella di tutela delle posizioni individuali», così ritenendo legittimo un sindacato sulla ragionevolezza delle scelte del legislatore nell'esercizio della sua discrezionalità.

[33] MARINI, *Delitti contro la persona*, II ed., Torino 1996, 391.

[34] MUCCIARELLI, *Commento all'art. 10 della legge n. 547 del 1993*, in *Legisl. pen.*, 1996, 138.

l'utilizzo di suddetto codice in un altro apparecchio, si rende possibile la clonazione dello stesso, con la conseguente possibilità di connettersi alla rete di telefonia mobile, che costituisce un sistema informatico protetto[35]. Il secondo caso concerne, invece, le c.d. *pic cards*, vale a dire schede informatiche che consentono la fruizione di programmi televisivi criptati attraverso la decodifica di segnali trasmessi secondo modalità tecniche di carattere telematico[36].

Rispetto al rapporto con la ricettazione, la giurisprudenza ha inoltre chiarito che integra il reato di cui all'art. 615-*quater* la condotta di chi riceve codici di carte di credito abusivamente scaricati dal sistema informatico e li inserisce in carte di credito clonate.

Sul piano soggettivo, il reato richiede il dolo specifico, consistente nel fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno. Tale qualificazione è volta a restringere il campo d'azione della norma, di per sé molto ampio, escludendo la rilevanza penale di tutti quei casi in cui la ricezione del codice sia avvenuto per finalità lecita.

Rilevante è approfondire il tema dell'individuazione del *locus commissi delicti* in relazione a tale peculiare fattispecie, che punisce condotte prodromiche all'accesso abusivo. Come più volte accennato nel corso della trattazione, la condotta che si perpetra mediante un sistema informatico si snoda in una serie di operazione automatiche che entrano in contatto con diversi *server*. Tali connotazioni caratterizzano anche la fattispecie di comunicazione abusiva di codici di accesso a sistemi informatici, per cui la condotta consistendo in un transito di

[35] V. Cass. pen., Sez. II, 17.12.2004, n. 5688. La sentenza richiamata trova ulteriore conferma in una recente pronuncia: Cass. pen. Sez. II, 26.11.2013, n. 47021, secondo cui «Integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici e telematici (art. 615-*quater* cod. pen.) e non quello di ricettazione la condotta di chi riceve i codici di carte di credito abusivamente scaricati dal sistema informatico, ad opera di terzi e li inserisce in carte di credito clonate poi utilizzate per il prelievo di denaro contante attraverso il sistema bancomat», in *www.dejure.it*.

[36] Cass. pen., Sez. V, 02.07.1998, n.4389. Si veda anche Cass. pen., Sez. V, 27.06.2002, n. 24847. *Contra* Cass. pen. Sez. V, 20.05.2003, n. 22319, secondo cui «non configura il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615-*quater* c.p.) il possesso di un decodificatore di segnali satellitari e di schede per la ricezione degli stessi (c.d. "*Pic-card*" o "*Smart-card*"), atteso che con tali strumenti non si viola alcun domicilio informatico, protetto da misure di sicurezza, ma si utilizzano irregolarmente servizi di trasmissione o comunicazione ad accesso condizionato, contravvenendo in tal modo alle disposizioni sul diritto d'autore di cui all'art. 6 D.lgs. 15 novembre 2000, n. 373, sanzionato solo in via amministrativa prima dell'entrata in vigore della legge 7 febbraio 2003, n. 38», in *www.avvocato.it*.

informazioni, non esaurisce il proprio disvalore con l'attività posta dal terminale di partenza, ma necessita che la comunicazione arrivi a destinazione, vale a dire giunga a conoscenza del destinatario. In relazione a tale ipotesi appare improbabile l'applicazione del principio di diritto precedentemente affermato dalla Corte di Cassazione a Sezioni Unite, dato che il terminale di partenza rappresenta solo il punto da cui parte la condotta, senza peraltro acquisire rilevanza, in virtù dell'anticipata soglia di punibilità della fattispecie, che altrimenti violerebbe il principio di offensività, non concretandosi un pericolo per il bene giuridico. Con tali considerazioni si intende aprire la questione alla configurabilità di diverse ipotesi di luoghi del commesso reato, che potrebbero acquisire rilievo alla luce di tale complesso *iter criminis*. Il delitto in esame si consuma nel momento in cui si realizza la comunicazione o la consegna dei codici al soggetto interessato[37]. Qualora la condotta consti di una comunicazione di codici via Internet, come nel caso di comunicazione via posta elettronica, si possono rinvenire quattro possibili luoghi di commissione del delitto, tra cui il luogo ove è situato il soggetto attivo che instaura il dialogo, facendo partire la comunicazione; il luogo ove si rinviene il *server* del *provider* di posta elettronica dell'agente; il luogo ove si trova il *server* del gestore di posta del destinatario; e da ultimo il luogo ove si trova il destinatario, recettore della comunicazione. In riferimento a questo schema criminoso non pare suscettibile di applicazione il principio di diritto summenzionato, in virtù del fatto che sarebbe errato considerare il sistema in modo unitario, data la presenza di diversi *server* che consentono la comunicazione, tale che sarebbe scorretto ritenere che il soggetto agente si colleghi direttamente al *server* di posta del ricevente. In relazione a tali ipotesi, ben si conformano le prospettive avanzate in dottrina che intendono valorizzare il momento in cui il destinatario prende conoscenza della comunicazione, così da radicare ivi il luogo di commissione, ove effettivamente viene prodotto il danno e il delitto raggiunge l'apice della gravità.

3. Interruzione illecita di comunicazioni informatiche o telematiche art. 617-*quater* c.p.

[37] PECORELLA, *Diritto penale dell'informatica*, cit., 356 ss.

La norma punisce chi "fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe" con la pena della reclusione da sei mesi a quattro anni, applicando, sempre che il fatto non costituisca più grave reato, la stessa pena a chiunque riveli al pubblico, anche in parte, il contenuto delle comunicazioni in oggetto[38].

Il delitto è procedibile a querela della persona offesa, salvo che siano integrate le circostanze aggravanti di cui al comma quarto, che concernono i casi in cui il fatto sia commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; da chi esercita anche abusivamente la professione di investigatore privato.

La condotta di cui al primo comma dell'articolo in commento si caratterizza per la necessaria fraudolenza, dovendosi caratterizzare per la particolare insidiosità del mezzo utilizzato[39]. La giurisprudenza ha, inoltre, ritenuto che la disposizione del primo comma potesse trovare applicazione anche nei confronti di un soggetto, titolare di un esercizio commerciale, che utilizzi, mediante un terminale POS in sua dotazione, una carta di credito contraffatta, atteso che il titolare dell'esercizio commerciale è ben legittimato ad usare il terminale POS e l'accesso abusivo genera un flusso di informazioni ai danni del titolare della carta contraffatta diretto all'addebito sul suo conto della spesa fittiziamente effettuata[40].

---

[38] Per approfondire si veda CORRIAS LUCENTE, *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in *Dir. informaz. informat.*, 1987, 531; MARINI, *Condotte in alterazione del reale aventi ad oggetto nastri ed altri supporti magnetici e diritto penale*, in *Riv. it. dir. proc. pen.*, 1986, 381.

[39] Sul punto si veda Cass. pen. Sez. V, 31.07.2007, n. 31135, secondo cui «Integra il delitto di intercettazione illecita di comunicazioni informatiche o telematiche (art. 617-*quater*, comma primo, c.p.) la condotta di colui che si avvalga di mezzi atti ad eludere i meccanismi di sicurezza preordinati ad impedire l'accesso di estranei alle comunicazioni. (In applicazione di questo principio la S.C. ha escluso che abbiano rilievo la circostanza che l'autore di siffatta condotta rivesta la qualità di amministratore di sistema connessa alla qualità di responsabile dei servizi informatici, abilitato pertanto ad inserirsi nel sistema, perché tale qualità non lo abilita, comunque, ad accedere — come accaduto nella fattispecie — alla casella di posta elettronica del singolo account protetta da apposita password nonché la agevole identificabilità quale autore e installatore del programma di intercettazione dello stesso amministratore di sistema)» in *www.avvocato.it*.

[40] V. Cass. pen., Sez. V, 19.11.2003, n. 44362, in *www.avvocato.it*.

Alla luce di questa breve premessa concernente i tratti salienti della fattispecie criminosa, è bene addentrarsi nella annosa tematica che attiene al *locus commissi delicti*. Avuto riguardo del *modus operandi* della condotta, pare suscettibile di applicazione il principio di diritto enunciato dalle Sezioni Unite del 2015, in quanto l'agente interagisce con il sistema informatico, al fine di interrompere una data comunicazione, per cui il luogo di commissione del reato potrà essere agevolmente individuato nel luogo ove è posto il *client*, che agendo dalla propria postazione, da remoto, ne interrompe la comunicazione.

Continuando l'analisi della norma in esame, essa punisce, altresì, la condotta di chi divulga le informazioni utili a raggirare il sistema, di cui al secondo comma, con cui viene incriminata qualsivoglia tipologia di divulgazione al pubblico delle comunicazioni intercettate, mediante ogni mezzo di informazione al pubblico. Da ciò si evince che non si richiede, quale presupposto del reato, la previa intercettazione fraudolenta delle comunicazioni, in quanto la norma è volta ad evitare che siano divulgate con qualsiasi mezzo di informazione al pubblico comunicazioni che siano destinate a rimanere segrete, ma delle quali l'agente sia comunque venuto a conoscenza[41].

È interessante notare che la tutela della segretezza delle comunicazioni informatiche è presidiata anche dalla norma immediatamente successiva alla disposizione oggetto di analisi, vale a dire l'art. 617-*quinquies*, che anticipa ulteriormente la tutela penale. In particolare, l'art. 617-*quinquies* c.p. punisce , ad evidenziar l'importanza dell'inviolabilità dei segreti, la mera installazione di apparecchiature idonee all'intercettazione di comunicazioni telematiche ovvero informatiche, a prescindere dal loro concreto utilizzo. Tuttavia, ogniqualvolta venga ad integrarsi la fattispecie più grave di cui all'art. 617-*quater* c.p., il seguente articolo si ritiene assorbito, ciò in considerazione del fatto che l'attività di fraudolenta intercettazione di comunicazioni informatiche ha quale presupposto necessario la previa installazione delle apparecchiature, volte a realizzare tale intercettazione, configurandosi un'ipotesi di progressione criminosa[42].

[41] Cfr. Cass. pen., Sez. V, 19.05.2005, n. 4011, in *www.dejure.it*.
[42] V. Cass. pen., Sez. V 18.12.2015, n.4059, in *www.pluris-cedam.utetgiuridica.it*.

4. La diffamazione *online*: art. 595 comma 3 c.p.

Il reato di diffamazione, di cui all'art. 595, è contenuto nel Libro Secondo, Titolo Dodicesimo, del codice penale nell'ambito dei delitti contro la persona. In particolare, tale reato, al primo comma, punisce chiunque offenda l'altrui reputazione, comunicando con più persone, mentre al terzo comma viene sanzionato più severamente colui che compia tale condotta col mezzo della stampa o con qualsiasi altro mezzo di pubblicità.

Si osserva, quindi, che il bene giuridico protetto dal delitto di diffamazione è l'interesse dello Stato all'integrità morale della persona, nello specifico è costituito dalla reputazione dell'uomo, dalla stima diffusa nell'ambiente sociale, dalla opinione che gli altri hanno del suo onore e decoro. La reputazione, infatti, non va ravvisata in un sentimento individuale che prescinde dalla realtà esterna, ma è da riscontrare nel senso della dignità personale nell'opinione degli altri, vale a dire nell'idea socialmente esigibile da tutti in un dato momento storico[43]. La libertà di pensiero, quindi, garantita dall'art. 21 della Costituzione, trova un preciso limite nella legge penale, che, attraverso il reato in oggetto, tutela il diritto di ogni cittadino all'integrità dell'onore, del decoro e della reputazione[44].

Quanto all'elemento oggettivo ai fini dell'integrazione della diffamazione, continuando nell'esame della disposizione, si possono, principalmente, ravvisare due requisiti tipici della condotta: l'offesa alla reputazione altrui e la comunicazione con più persone.

Ai fini dell'integrazione dell'offesa è necessario che si adoperino termini che risultino offensivi, in base al significato che essi vengono oggettivamente ad assumere, nella comune sensibilità di un essere umano, collocata in un determinato contesto storico e in un determinato ambito sociale. La stessa divulgazione di comportamenti sentiti quali riprovevoli dalla *communis opinio*, in quanto lontani dai canoni etici condivisi dalla generalità dei consociati, vale ad integrare una lesione alla reputazione altrui, per cui essa non risulta integrata solamente da un'attribuzione di un fatto illecito, contrario alle norme giuridiche[45].

[43] Si veda Cass. pen., Sez. V, 28.02.1995, n.3247, in *www.dejure.it*.
[44] Cfr. Cass. pen., Sez. V, 16.10.1972, n.811.
[45] Cfr. Cass. pen., Sez. V, 12.12.2013, n. 13350, in *www.penalistiassociati.net*.

Configura, invece, l'altro requisito della comunicazione con più persone, oltre all'ipotesi auto-evidente della conversazione orale al cospetto di più persone, anche l'ipotesi più problematica di comunicazione del messaggio diffamatorio mediante scritti. La giurisprudenza, infatti, ritiene integrato il reato in esame anche quando le espressioni offensive siano contenute in uno scritto diretto ad una sola persona, ma per via delle modalità utilizzate, le stesse ivi contenute giungeranno sicuramente a conoscenza di altri soggetti[46].

Occorre, comunque, mettere in luce fin da ora, che nel caso della diffamazione *online* la sussistenza di tale requisito non deve essere provata, ma si deve presumere, in virtù del fatto che il sito *web* è liberamente accessibile da un numero indeterminato di soggetti, per cui qualora in tale sito sia situato il messaggio diffamatorio, questo è ontologicamente destinato ad essere visualizzato da un numero indicibile di soggetti[47].

Quanto, infine, all'elemento soggettivo, il delitto di diffamazione è un reato a dolo generico. Ai fini della sua configurabilità, si richiede, pertanto, la consapevolezza di pronunciare espressioni lesive dell'altrui reputazione e la volontà che tali espressioni vengano a conoscenza di più persone[48].

Dopo avere compiuto una breve disamina della fattispecie base del reato comune di diffamazione, è bene andare ad analizzare l'ipotesi aggravata prevista dal terzo comma dell'art. 595 c.p., soffermandosi sulle questioni giurisprudenziali di maggiore interesse, le quali attengono altresì all'individuazione parimenti del *tempus* e *locus commissi delicti*.

Addentrandoci nel dettaglio, il terzo comma dell'art. 595 c.p., come già in precedenza evidenziato, punisce, più severamente, la stessa condotta di cui al primo comma qualora recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità. In particolare, si può osservare come rientri in questa particolare ipotesi di diffamazione aggravata, quella commessa tramite Internet, in quanto posta in

[46] Si veda Cass. pen., Sez. V,17.05.2012, n. 30329, in *www.dejure.it*. Nel caso di specie, infatti, è stata ravvisata la sussistenza della consapevole diffusione a più di una persona nel caso di un esposto a carico di un avvocato che, pur essendo stato formalmente diretto al presidente del Consiglio dell'ordine degli avvocati, lo era stato con la consapevolezza che il destinatario ne avrebbe investito il Consiglio nella sua interezza, trattandosi di doglianza diretta a sollecitare un eventuale procedimento disciplinare.

[47] V. Cass. pen., Sez. V, 4.04.2008, n. 16262, in *www.penale.it*.

[48] Si veda Cass. pen., Sez. I, 22.01.2014, n. 16712 in *www.penale.it*.

essere con altro mezzo di pubblicità[49]. Del resto, essendo Internet un potente mezzo di diffusione di qualsivoglia tipo di informazione, è anche e soprattutto attraverso tale strumento di comunicazione che si può estrinsecare il diritto di esprimere le proprie opinioni, garantito dall'art. 21 della Costituzione, che deve sempre essere esercitato nel rispetto del contrapposto diritto all'integrità della reputazione altrui, ugualmente tutelato dall'ordinamento, per cui il "*free speech*" risulta temperato alla luce di ulteriori diritti che richiedono tutela, quali la reputazione e l'onore[50].

Si deve osservare, inoltre, che la *ratio* dell'aggravante dell'uso del mezzo di pubblicità si spiega proprio in ragione dell'idoneità del mezzo a coinvolgere e raggiungere una vasta platea di soggetti, ampliando in tal modo la capacità diffusiva del messaggio lesivo della reputazione della persona offesa. Tale previsione costituisce uno degli strumenti più efficaci nella tutela dei diritti fondamentali su Internet. Pertanto, la giurisprudenza è ormai consolidata nel ritenere che l'uso dei *social network,* e quindi la diffusione di messaggi offensivi veicolati a mezzo Internet, integra un'ipotesi di diffamazione aggravata ai sensi dell'art. 595, terzo comma, c.p., alla luce del fatto che si tratti di una condotta potenzialmente capace di raggiungere un numero indeterminato di persone, qualunque sia la modalità informatica di condivisione e di trasmissione[51].

Occorre, infine, esaminare un tema in materia di diffamazione *online*, che per lungo tempo ha impegnato il dibattito giurisprudenziale, di cui si tenterà brevemente un'esposizione. In particolare, si è trattato di capire a che titolo dovesse rispondere il gestore o il proprietario di un sito *web*, piuttosto che il direttore di una testata giornalistica telematica, rimasto inerte, a seguito della pubblicazione sul portale di un commento offensivo da parte di un utente.

Innanzitutto, la giurisprudenza ha chiarito che sussiste una netta differenza tra il concetto di giornale telematico e gli altri nuovi mezzi di manifestazione del pensiero destinati ad essere trasmessi in via telematica quali *forum*, *blog*, *newsletter*, *newsgroup*, *mailing list* e *social network*.

[49] Si veda Cass. pen., Sez. V, 01.07.2008, n. 31392, in *www.diritto.it*.

[50] *Ivi*.

[51] Cfr. Cass. pen., Sez. V, del 23.01.2017, n. 8482, in *www.dejure.it*; Cass. pen., Sez. I, 02.12.2016, n. 50, in *www.dejure.it*.

Nel dettaglio, seppure a seguito di un lungo contrasto, la giurisprudenza ad oggi si è orientata nel ritenere, sulla base di una interpretazione evolutiva della nozione di "stampa" di cui all'art. 1 della legge n. 47 del 1948, che il giornale telematico è assimilabile ontologicamente e funzionalmente a quello tradizionale in formato cartaceo, soggiacendone quindi alla normativa di rango costituzionale e di livello ordinario[52]. I *forum*, i *blog* e le altre piattaforme di informazione, invece, non avendo la stessa struttura professionale di un giornale *online* e quindi di un giornale cartaceo non possono essere ad esso equiparati[53].

Alla luce di tali precisazioni, dunque, tornando a sciogliere l'interrogativo originariamente posto, la giurisprudenza ha affermato che i direttori di testate giornalistiche *online*, essendo assimilabili ai direttori delle testate cartacee, possono essere ritenuti responsabili di concorso omissivo nel reato di diffamazione, *ex* art. 57 c.p., essendo, per legge, titolari di una posizione di garanzia da cui deriva un obbligo di controllo preventivo sui dati messi in rete.

I gestori di *blog online*, invece, non essendo assimilabili ai direttori di testate giornalistiche, non possono essere imputati a titolo di responsabilità *ex* art. 57 c.p., non avendo nessun obbligo di impedire le pubblicazioni di contenuti diffamatori, oltre a trovarsi nell'impossibilità di riuscirci, ma possono concorrere nel reato di diffamazione *ex* art. 595 c.p. con l'autore del commento offensivo, se, venuti a conoscenza dell'esistenza dello stesso non lo abbiano tempestivamente rimosso, consentendo che continuasse a esercitare la sua efficacia diffamatoria[54].

Si evince da questa breve disamina che la diffusività della rete e dei *social network* ha concesso l'instaurarsi di rapporti sociali anche a notevole distanza, per cui qualora venga commesso un illecito, ci si trova sovente dinnanzi a condotte transnazionali, per cui la condotta deve intendersi effettuata *erga omnes*, data la comunicazione con un'indeterminata platea di soggetti, nonché essendo le informazioni fruibili in qualsiasi parte del globo[55]. Tutto ciò comporta delle

[52] V. Cass. pen., Sez. V, 25.02.2016, n. 12536, in *www.giurisprudenzapenale.com*.

[53] Sul punto Cass. pen., Sez. V, 23.10.2018, n. 1275, in *www.archiviodpc.dirittopenaleuomo.org*.

[54] In tal senso Cass. pen., Sez. V, 14.07.2016, n. 54946, in *www.giurisprudenzapenale.com*.

[55] Così Cass. pen., Sez. V, 27.12.2000, n. 4741, richiamata altresì da autorevole dottrina: FALLETTA, *La diffamazione* online, in MENSI, FALLETTA, *Il diritto del* web, Padova, 2018, 157 ss.; FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 155 ss.

implicazioni quanto al fondamentale tema oggetto di trattazione, concernente il *tempus* e il *locus commissi delicti,* per cui si è puntato ad estendere massimamente la giurisdizione italiana, adottando la teoria dell'ubiquità, e per cui si è adoperata una ricostruzione della fattispecie orientata, tale da distinguere il momento della perfezione da quello della consumazione.

Si evidenzia, in particolare, che la diffamazione è un reato di evento c.d. psicologico che si consuma nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa e dunque, nel caso in cui frasi e immagini lesive siano state immesse sul *web*, nel momento in cui il collegamento viene attivato atteso che l'accesso ad essi è solitamente libero e, in genere, frequente, di talché l'immissione di notizie in Rete ne implica la fruibilità da parte di un numero elevato di persone[56]. Si deduce, pertanto, che il suddetto evento risulta differenziato dalla condotta, distinguendo nettamente il momento in cui il soggetto immette il messaggio in rete, da quello in cui questo viene percepito da terzi: è solo in tale momento che si intenderà consumata la fattispecie. Alla luce di tale assunto, va accolta la teoria della ubiquità, che consente al giudice italiano di conoscere del fatto criminoso, tanto nel caso in cui sul territorio nazionale si sia verificata la condotta, quanto in quello in cui in tale luogo si sia verificato l'evento[57].

È bene sottolineare che riguardo al momento consumativo della fattispecie, si era prospettato un ulteriore approccio ermeneutico che ancorava tale *tempus* all'immissione del messaggio in rete, così confondendo la condotta con l'evento e qualificando di tal modo la stessa come un reato di mera condotta. Ciononostante, risulta prevalente il precedente orientamento esaminato che ravvisa la consumazione nel momento e nel luogo in cui terzi percepiscono il messaggio, essendo il reato in esame un reato a evento psicologico, tenendo presente che la diffusività della rete permette la sostanziale prossimità temporale tra il momento di immissione in rete e il momento in cui terzi percepiscono il messaggio lesivo dell'altrui reputazione.

[56] Si veda Cass. pen., Sez. V, 21.06.2006, n. 25875; Cass. pen., Sez. I, 05.02.2009, n. 8513, in *www.penale.it*.

[57] In tal senso FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 155.

Ciò detto, il luogo di consumazione del reato non può essere identificato nella sede ove è ubicato il *server* in cui vengono immesse le notizie, che potrebbe rinvenirsi nelle zone più disparate ma – presupponendo che la diffamazione risulta integrata quando il contenuto lesivo sia percepito da almeno due soggetti – andrebbe individuato il secondo soggetto che percepisce il messaggio diffamatorio. Agevole risulta, peraltro, intuire che tale individuazione risulti impossibile nella prassi. Il problema è che, in riferimento a tale ipotesi di diffamazione aggravata, risultano sostanzialmente inapplicabili criteri univoci e oggettivi che permettano l'individuazione del *locus commissi delicti* ai fini della determinazione della competenza territoriale[58]. Proprio per tale motivo si è ritenuto, in giurisprudenza, che qualora sia impossibile determinare il luogo del commesso reato ai sensi dell'art. 8 c.p.p. comma 1, risulti indispensabile far riferimento ai criteri suppletivi, di cui all'art. 9 comma 2 c.p.p., riguardanti il luogo di residenza, domicilio, dimora del soggetto imputato[59].

A diversa conclusione giunge, peraltro, la giurisprudenza civile che ritiene che vada identificato un unico luogo ove si rinviene il pregiudizio effettivo, che deve essere ravvisato nel luogo in cui il soggetto leso aveva il proprio domicilio al momento della divulgazione del messaggio lesivo, luogo in cui il danneggiato esplica la propria personalità e "costruisce la sua immagine"[60]. Questo assunto trova conferma nella giurisprudenza della Corte di Giustizia europea, che ha affermato che, in tema di lesione di un diritto della personalità a mezzo Internet, il soggetto vittima può adire il foro del luogo ove si è prodotto il danno, vale a dire ove il danneggiato ha il proprio centro di interessi, adeguandosi in tal modo all'obiettivo di una corretta amministrazione della giustizia[61].

Concludendo, sebbene sembri sufficiente ai fini dell'integrazione del reato la divulgazione del messaggio in rete, va considerato che la disposizione richiede l'effettiva comunicazione con più persone, per cui occorre far riferimento, ai fini

---

[58] In questo senso Cass. pen., Sez. I, 15.03.2011, n. 16307, che riporta la motivazione di Cass. pen., Sez. I, 21.12.2010, n. 2739, in *www.dejure.it*.

[59] Sul punto SEMINARA, Locus commissi delicti, *giurisdizione e competenza nel cyberspazio*, cit., 2012.

[60] Cfr. Cass. civ., Sez. Un., 29.09.2009, n. 21661, in *www.aduc.it*.

[61] V. Corte di Giustizia europea, 25 Ottobre 2011, C-509/09, C- 161-10, via *www.pluris-cedam.utetgiuridica.it*.

dell'individuazione del *tempus* e *locus commissi delicti*, al momento in cui terzi percepiscono il contenuto lesivo, fatte salve le ultime considerazioni su esposte per il caso in cui non sia possibile individuare la seconda persona che ha percepito il messaggio diffamatorio.

5. La frode informatica: art. 640-*ter* c.p.

Il reato di frode informatica di cui all'art. 640-*ter* c.p. è contenuto nel Libro Secondo, Titolo tredicesimo, nell'ambito dei delitti contro il patrimonio.

Tale reato punisce, al primo comma, chiunque, per procurare a sé o ad altri un ingiusto profitto con altrui danno, altera in qualsiasi modo il funzionamento di un sistema informatico o telematico o interviene senza autorizzazione su dati, informazioni o programmi contenuti in un sistema informatico o telematico.

Nei commi successivi, inoltre, è punito più severamente sia chi commette frode informatica, di cui al primo comma, a danno dello Stato o di altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare, sia chi ha commesso tale frode con abuso delle qualità di operatore del sistema, o con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Particolare risulta quest'ultima ipotesi di frode informatica aggravata dal furto o dall'indebito utilizzo dell'identità digitale in danno di uno o più soggetti di cui al comma 3, da tempo al centro di dubbi ermeneutici concernenti gli aspetti definitori da attribuire alla nozione di identità digitale e alle nozioni riguardanti le condotte tipiche.

Con riferimento a queste ultime, si può affermare, brevemente, che il "furto" andrebbe inteso alla stregua di un'apprensione dell'identità digitale, mentre l'"indebito utilizzo" dovrebbe intendersi quale utilizzo non autorizzato della stessa[62]. Restano fermi i dubbi interpretativi concernenti il senso da attribuire alla nozione di identità digitale, che si traducono in tentativi tutti da riferire in ogni modo alla fase autenticativa[63].

---

[62] Si veda MALGIERI, *La nuova fattispecie di "indebito utilizzo di identità digitale". Un problema interpretativo*, in *Dir. pen. cont. – Riv. Trim.*, 2/2015, 147.

[63] In dottrina si sono avanzate numerosi orientamenti. Vi è chi ritiene che debba essere intesa alla stregua di un profilo abilitativo ovvero credenziali di autenticazione; vi è chi, invece, ritiene debba essere ricondotta nel sistema di protezione dei dati personali; altra parte intende tale nozione come insieme di informazioni e risorse concesse da un sistema ad un utilizzatore: per un approfondimento si veda FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 169 s.

Si discute su quale sia il bene giuridico che il legislatore ha inteso tutelare con la norma di cui all'art. 640-*ter* c.p. Secondo un orientamento della dottrina e della giurisprudenza tale reato è posto a tutela sia della riservatezza e della regolarità dei sistemi informatici, che del patrimonio altrui[64].

Trattasi di un reato apparentemente a forma vincolata, ma che sostanzialmente può essere realizzato in qualsiasi modalità, prevedendo alternativamente una condotta consistente nell'alterazione del funzionamento del sistema informatico o telematico, ovvero in un intervento non autorizzato – che è possibile effettuare con qualsiasi modalità – sui dati, informazioni e programmi ivi contenuti[65].

La condotta di alterazione investe la modalità di funzionamento del sistema informatico o telematico[66]. In particolare, sul punto, va precisato che la condotta manipolatoria può arrivare fino a modificare gli aspetti essenziali del sistema, come i suoi scopi; ciononostante è da qualificarsi parimenti come intervento manipolativo quello che, pur rispettando la destinazione del sistema, agisca manipolando i suoi contenuti[67].

La condotta alternativa di "intervento abusivo", invece, è rivolta ai dati, alle informazioni o ai programmi – *software* – installati nell'*hardware*. Tale intervento è qualificato dal legislatore come abusivo, vale a dire che deve avvenire senza diritto. Riguardo al significato da attribuire alla locuzione "senza diritto", si ritiene che con essa vada inteso sia l'intervento avvenuto senza il doveroso consenso del titolare dei dati, informazioni o programmi contenuti nel sistema, sia l'intervento avvenuto in contrasto con le norme giuridiche dell'ordinamento[68].

---

[64] Così FIANDACA, MUSCO, *Dir. Pen. P. s., I delitti contro il patrimonio*, Bologna, 2002; PAGLIARO, *Principi di diritto penale, P. s., Delitti contro il patrimonio*, Milano, 2003; ANTOLISEI, *Manuale di diritto penale, P.s.*, I, Milano, 2002. Si veda anche MASI, *Frodi informatiche e attività bancaria, in Riv. pen. econ.*, 1995, il quale sostiene che l'oggetto della tutela nel delitto ex art. 640-*ter* c.p. sia la libertà negoziale. Si veda altresì Cap. 1 § 4.1.

[65] Si veda Cass. pen., Sez. V, 24.11.2003, n. 4576, via *www.ius-web.it*.

[66] Si fa riferimento ad esempio al caso di un'alterazione della modalità di *log-in* e *log-out* del sistema da un determinato sito internet, di talché, ove il computer rimanesse collegato alla rete e al sito nonostante la convinzione dell'utilizzatore di aver effettuato il *log-out*, ciò comporterebbe un ingiusto guadagno per il gestore del sito e, specularmente, il danno economico in capo all'utente.

[67] V. DESTITO, DEZZANI, SANTORIELLO, *Il diritto penale delle nuove tecnologie*, Cedam, Padova, 2007.

[68] *Ivi*.

Stando sempre all'elemento oggettivo del reato in esame, nonostante la supposta somiglianza con la fattispecie di truffa comune – di cui ripercorre la struttura – occorre specificare che non è richiesta l'induzione in errore di un soggetto attraverso artifici o raggiri, caratterizzandosi così rispetto alla norma di cui all'art. 640 c.p., il quale richiede ai fini dell'integrazione del delitto che la condotta sia posta in essere con tali modalità. Difatti, nel caso della frode informatica, l'attività dell'agente, caratterizzata da specifici connotati fraudolenti, è rivolta al sistema informatico che viene manipolato al fine di ottenere una infiltrazione abusiva, per cui la persona offesa titolare di detto sistema resta esclusa dalla condotta che non è ad essa diretta[69].

Proseguendo nell'analisi del reato, si sottolinea che, oggetto della condotta di reato sono i sistemi informatici o telematici. Dunque, occorre individuare la nozione esatta e le caratteristiche del sistema informatico, da un lato, e di quello telematico, dall'altro, per inquadrare esattamente la portata applicativa dell'art. 640-*ter* c.p.

In particolare, con riferimento alla nozione di sistema informatico, la Corte di Cassazione, con una sentenza piuttosto risalente, ha affermato che tale espressione si riferisce ad una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione, anche solo parziale, di tecnologie informatiche[70]. È stato sottolineato, altresì, che il sistema informatico, per essere definito tale, debba presentare tre caratteristiche essenziali, vale a dire la registrazione o memorizzazione, mediante impulsi elettronici e su supporti adeguati, di dati rappresentati da *bit* e codici numerici, disposti in combinazioni diverse; l'elaborazione automatica da parte della macchina di tali dati; l'organizzazione degli stessi secondo una logica che consenta loro di esprimere un particolare significato per l'utente[71].

Chiarita la portata della nozione di sistema informatico, occorre esaminare il concetto di sistema telematico. A tal proposito, in termini più semplicistici, si può affermare che è telematico un sistema formato da un insieme di sistemi informatici

[69] Cfr. Cass. pen., Sez. II, 10.09.2018, n. 48553, via *www.canestrinilex.it*.

[70] Si veda Cass. pen., Sez. VI, 04.10.1999, n. 3065, in *www.dejure.it*.

[71] Sul punto STALLA, *L'accesso abusivo ad un sistema informatico o telematico*, 2003, in *www.penale.it.*

connessi tra loro attraverso una rete elettrica ovvero mediante un sistema di trasmissione via etere al fine di trasmettere e ricevere informazioni.

La frode informatica è un reato di evento, per cui ai fini della integrazione della fattispecie è necessario che si verifichi l'evento tipico descritto della norma, vale a dire l'ingiusto profitto e l'altrui danno, per cui la stessa si consuma nel momento in cui l'agente consegue l'ingiusto profitto, con correlativo altrui danno[72].

In considerazione dell'espressa locuzione "ingiusto profitto" all'interno della disposizione normativa, si ritiene che la modalità con cui si ottiene tale profitto deve essere ingiusta, illecita, per cui il soggetto attivo deve avere agito contrariamente alle norme dell'ordinamento nell'apprensione di tale profitto. Va, inoltre, precisato che in virtù della presenza della locuzione "a sé o ad altri" all'interno della disposizione criminosa, l'ingiusto profitto può essere conseguito sia dal reo che da un soggetto terzo, mantenendo fermo pertanto il disvalore della condotta[73].

Quanto, invece, alla natura del profitto, si è affermata la non necessarietà della natura economia dello stesso, alla luce di un autorevole orientamento giurisprudenziale pronunciatosi con riferimento al delitto di truffa comune, che ha affermato altresì la rilevanza di altri tipi di vantaggi, quali quelli di tipo affettivo o morale[74]. Quale diretta conseguenza di tale profitto ingiusto, si richiede la verificazione di un altro evento ai fini della consumazione del reato, vale a dire il danno altrui.

Prima di concludere questa analisi del delitto di frode informatica, si ritiene opportuno esaminare il rapporto di tale reato con la truffa e con l'indebito utilizzo di carte di credito e di pagamento di cui all'art. 493-*ter* c.p.

Brevemente, si osservi che nella fattispecie prevista dall'art. 640-*ter* c.p., l'attività fraudolenta è diretta al sistema informatico che viene manipolato e non al soggetto titolare dello stesso, per cui viene a mancare l'induzione in errore del soggetto passivo – requisito essenziale del reato di cui all'art. 640 c.p. – per cui

[72] V. Cass. pen., Sez. VI, 04.10.1999, n. 3065, in *www.dejure.it*.

[73] Cfr. ANTOLISEI, *Manuale di Diritto penale, P. S.,* cit., 374.

[74] Cfr. Cass. pen., Sez. Un., 16.12.1998, in *Giur. it.*, 2000; in senso contrario, e con specifico riferimento alla frode informatica, MARINI, *Digesto delle discipline penalistiche,* (voce) *Truffa (Frode informatica)*, Torino, 2006.

sebbene abbia la medesima struttura e quindi i medesimi elementi costitutivi della truffa comune, da essa se ne differenzia per la particolare destinazione che assume la condotta manipolatoria.[75].

Integra, invece, il delitto di cui all'art. 493-*ter*, c.p. – di cui si parlerà più nel dettaglio nell'ultimo paragrafo del presente elaborato – e non quello di frode informatica *ex* art. 640-*ter* c.p., la condotta di colui che, in assenza di frode, utilizzi indebitamente il codice e una tessera bancomat per effettuare prelievi di denaro[76].

Pertanto, l'elemento caratterizzante della frode informatica consiste nell'utilizzo "fraudolento" del sistema informatico, che viene così manipolato al fine di ottenere una penetrazione abusiva.

In questa sede è opportuno concentrarsi sulla fattispecie di frode informatica in relazione al *locus commissi delicti*. Data la particolare struttura della fattispecie, sovente il luogo di consumazione si radica in luogo diverso da quello in cui agisce il reo. La fattispecie si intende consumata nel momento in cui l'agente consegue il profitto con altrui danno e nel caso in cui sia impossibile individuare il luogo esatto di consumazione, al fine di determinare la competenza territoriale si fa riferimento al luogo in cui è avvenuta parte dell'azione o omissione, vale a dire al criterio suppletivo di cui all'art. 9 co. 1 c.p.p. o in subordine quello indicato dal comma 2, residenza, domicilio, dimora dell'imputato[77]. Tale fase consumativa può coincidere con il luogo di esecuzione dell'attività manipolatoria del sistema di elaborazione di dati: difatti, una volta alterato il funzionamento del sistema, il soggetto ben potrebbe conseguire l'ingiusto profitto anche non economico. Questa considerazione non esclude la struttura della fattispecie quale reato di evento, atteso che la condotta manipolativa risulta etiologicamente collegata con il duplice evento. Bisogna, però, aver riguardo ai fini dell'individuazione del luogo e momento di commissione del reato, del luogo e momento in cui si è realizzato l'ingiusto profitto con altrui danno.

---

[75] Così Cass. pen., Sez. II, 9.06.2016, n. 41435: nel caso di specie, in applicazione del principio nel testo richiamato, la S.C. ha ritenuto sussistente la penale responsabilità dell'imputato in ordine ad una fattispecie di truffa, originariamente qualificata in termini di frode informatica, avvenuta mettendo in vendita tramite la piattaforma *web eBay* materiale di cui l'imputato non aveva l'effettiva disponibilità, ed utilizzando per le comunicazioni un *account e-mail* per la cui acquisizione l'imputato aveva sfruttato generalità di fantasia e per i pagamenti una carta prepagata che riportava le sue effettive generalità, in *www.studiolegaleramelli.it*.

[76] Si veda Cass. pen., Sez. II, 30.10.2019, n. 50395, in *www.dejure.it*.

[77] In argomento PECORELLA, *Truffe* on-line: *momento consumativo e competenza territoriale*, in *Dir. pen. cont.*, 10 maggio 2012.

6. La truffa comune realizzata mediante l'utilizzo di strumenti tecnologici o la rete: art. 640 c.p.

Prima di addentrarsi nel vivo del tema oggetto di indagine, si osservi che la truffa è un reato contenuto nel Libro secondo, Titolo tredicesimo, del codice penale nell'ambito dei delitti contro il patrimonio.

In particolare, punisce chiunque procura a sé o ad altri un ingiusto profitto con altrui danno attraverso l'induzione in errore di un soggetto con artifizi o raggiri. Trattasi di un reato a forma vincolata, che richiede, ai fini dell'integrazione, che la condotta sia posta in essere con artifici o raggiri.

Al secondo comma, invece, sono previste delle ipotesi di truffa aggravata qualora il fatto sia commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare ovvero ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità, o avendo approfittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa.

È un reato, quindi, di danno che si perfeziona con il profitto ingiusto e con l'altrui danno, ma ai fini dell'integrazione deve sussistere anche un ulteriore elemento, non espressamente menzionato dal legislatore: l'atto di disposizione patrimoniale della vittima del raggiro. Vi è difatti un elemento implicito: attraverso l'induzione in errore della persona offesa si mira ad ottenere un suo atto di disposizione patrimoniale ed è proprio questo atto di disposizione patrimoniale a procurare all'agente il profitto ingiusto con altrui danno. Si parla, dunque, di reato a necessaria cooperazione della vittima.

A tal proposito, occorre far presente che si è posto il problema di capire chi deve porre in essere questo atto di disposizione patrimoniale e, in particolare, se occorre la coincidenza soggettiva tra il depauperato, vale a dire colui che subisce la diminuzione di patrimonio e quindi il danno, e il soggetto indotto in errore che quindi compie l'atto di disposizione patrimoniale. Sotto tale profilo, in realtà, la tesi prevalente, quantomeno in giurisprudenza ritiene che non vi deve necessariamente essere una coincidenza soggettiva, in quanto sovente accade che un soggetto abbia

il potere di disporre del patrimonio altrui; in virtù di tale assunto si statuisce che laddove sia presente tale potere di disposizione patrimoniale altrui, possa accadere che l'induzione in errore investa un soggetto diverso, ad esempio il rappresentante che compie un atto che pregiudica appunto il rappresentato[78]. In altre parole, non è richiesta l'identità tra l'indotto in errore e la persona offesa ai fini dell'integrazione del reato di truffa, vale a dire l'identità con il titolare dell'interesse patrimoniale leso che subisce le conseguenze patrimoniali dell'azione truffaldina, in quanto la condotta fraudolenta può essere indirizzata a un soggetto diverso dal titolare del patrimonio: tale assunto può essere accolto solamente ove sussista il rapporto causale tra l'induzione in errore e gli elementi del profitto e del danno[79].

Inquadrata brevemente la truffa, va posto in luce che il delitto in esame può essere ormai realizzato anche mediante l'utilizzo di strumenti tecnologici o mediante la Rete. Da tale assunto, si evince come i beni tradizionali siano soggetti ad aggressioni sempre diverse, tali da implicare un'attenta interpretazione dei tradizionali principi. In via preliminare, occorre evidenziare che tale ipotesi di manifestazione del reato non rientrano in una particolare ipotesi criminosa, ma fanno parte delle maglie dell'art. 640 c.p., declinato sulla base delle moderne tecnologie. A tal proposito, numerosi problemi ermeneutici sono sorti in relazione alla determinazione del momento e luogo di consumazione del reato.

Sulla questione, vi è chi ritiene che vada valorizzato il momento di effettivo pregiudizio patrimoniale, tenendo a mente la particolare struttura del reato in oggetto, vale a dire quale reato evento che viene integrato nel momento in cui, alla condotta tipica, segua la *deminutio patrimonii* della vittima.

Tali problematiche si sono poste con riferimento alle truffe *online*, per cui va considerato il particolare caso in cui il soggetto vittima, a seguito di artifici o raggiri, sia stato indotto in errore e abbia effettuato il pagamento di beni mai ricevuti, mediante ricariche *PostePay*. Si possono prospettare due orientamenti interpretativi: da un lato si identificherebbe il luogo di commissione del reato nel luogo in cui viene eseguito il pagamento, da cui deriva il pregiudizio per la vittima; dall'altro si valorizzerebbe il luogo di destinazione del pagamento. Tale ultima tesi,

[78] Cfr. Cass. pen., Sez. II, 12.11.2010, n. 44929, in *www.exeo.it*.
[79] Cfr. Cass. pen., Sez. II, 21.02.2008, n. 10085, in *www.exeo.it*.

come è stato evidenziato da autorevole dottrina, risulta conforme alla struttura della fattispecie, per cui il reato può dirsi perfezionato solo con l'effettivo conseguimento del profitto, da cui scaturisca un'effettiva diminuzione del patrimonio della vittima[80]. Tale contrasto è emerso proprio a causa delle caratteristiche proprie dello strumento di pagamento *PostePay*, che consente di effettuare operazioni di prelievo e pagamento, nonché di effettuare operazioni *online*. Questo comporterebbe che il luogo del profitto verrebbe a coincidere con quello in cui viene poi utilizzata la carta in questione, che ben potrebbe essere identificabile nell'abitazione del reo, alla luce del fatto che tali strumenti vengono utilizzati essenzialmente per effettuare operazioni *online*: tale conclusione porta a ritenere rilevante, ai fini della determinazione del luogo di consumazione, i criteri suppletivi di cui all'art. 9 co. 2 c.p.p. che hanno riguardo del luogo di residenza, domicilio o dimora dell'agente[81].

Ipotesi diversa si configura nel caso in cui il pagamento venisse realizzato mediante un bonifico bancario, in cui si rinvengono diverse tempistiche di accredito e in cui viene meno l'immediatezza che caratterizza lo strumento della carta prepagata in questione. In quest'ultimo caso andrebbe attribuito rilievo al luogo in cui il soggetto attivo consegue la somma derivante dalla condotta truffaldina, poiché altrimenti si anticiperebbe la consumazione del reato[82].

Nel caso in cui, ancora, ci si trovi dinnanzi ad un pagamento attuato con titolo di credito, prevale l'orientamento in base al quale la truffa deve ritenersi consumata nel momento e luogo in cui viene riscosso il titolo di credito e non semplicemente nel luogo in cui si rinviene la disponibilità dello stesso[83].

In giurisprudenza al fine di individuare il giudice territorialmente competente, si attribuisce rilievo ai criteri suppletivi di cui all'art. 9 c.p.p. comma 2, date le difficoltà applicative di cui al comma 1 del medesimo articolo.

---

[80] Così espone FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 164.

[81] Sul punto PECORELLA, *Truffe* on-line*: momento consumativo e competenza territoriale*, cit., 2012.

[82] V. Cass. pen., sez. II, 20.10.2016 n. 48027, in *www.penale.it*; si veda anche DI PRISCO, *Truffe* online *e* PostePay*: quando e dove si consuma il reato?* , 29 gennaio 2018, in *www.iusinitinere.it*, che richiama Cass. pen., sez. II, 04.11.2014 n. 7749.

[83] Cfr. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 166.

Da questa analisi emerge che la determinazione del *locus commissi delicti* è strettamente legata alle modalità di manifestazione della condotta criminosa, per cui non è possibile trarre un principio di ordine generale.

7. Indebito utilizzo e falsificazione di carte di credito e di pagamento: art. 493-*ter* c.p.

La norma di cui all'art. 493-*ter* c.p. ha inserito nel codice penale, ai sensi dell'art. 4, del D.Lgs. n. 21/2018, in attuazione della delega contenuta all'art. 1, comma 85, lett. q), L. n. 103/2017 sulla riserva tendenziale di codice nella materia penale, il delitto di indebito utilizzo e falsificazione di carte di credito o di pagamento, già previsto all'art. 55, comma 5, del D.Lgs. n. 231/2007, che è stato contestualmente abrogato.

La norma abrogata è stata ritenuta dal legislatore delegato del tutto estranea al testo normativo di riferimento dedicato alla prevenzione del riciclaggio e, pertanto, adeguatamente inseribile nel codice penale[84]. Il reato in esame, dunque, è ora contenuto nel codice penale al Libro secondo, Titolo settimo nell'ambito dei delitti contro la fede pubblica.

Più specificamente, il delitto in oggetto, al primo comma, punisce chiunque utilizzi indebitamente, non essendone titolare, carte di credito o di pagamento o qualsiasi altro documento che abiliti al prelievo di denaro contante, all'acquisto di beni o alla prestazione di servizi, al fine di trarre un profitto per sé o per altri; nella seconda parte del primo comma, invece, punisce con la stessa pena chiunque falsifichi o alteri carte di credito o di pagamento o qualsiasi altro documento analogo, nonché chiunque possieda, ceda, acquisisca tali carte o documenti, tra cui gli ordini di pagamento prodotti con essi, di provenienza illecita, o comunque falsificati o alterati, sempre al fine di trarne un profitto per sé o per altri.

Il comma terzo dell'art. 493-*ter* riprende, invece, le disposizioni in materia di confisca di cui al previgente sesto comma, secondo periodo, dell'art. 55, D.Lgs. n. 231/2007, anch'esso abrogato dall'art. 7, D.Lgs. n. 21/2018.

---

[84] Cfr. la *Relazione governativa allo Schema di decreto legislativo recante: "Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'articolo 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103"*.

Inoltre, ai sensi dell'art. 8, D.Lgs. n. 21/2018 ogni richiamo all'art. 55, comma quinto e sesto del D.Lgs. n. 231/2007, ovunque presente, deve ora intendersi riferito all'art. 493-*ter* c.p.

Si deve, dunque, osservare che il delitto di indebito utilizzo di carta di credito tutela l'interesse pubblico all'utilizzo corretto del sistema elettronico di pagamento, al fine di evitare fenomeni riciclativi e a garanzia della fede pubblica. Va considerato, tuttavia, che la tutela della norma in oggetto si estende anche al patrimonio del singolo, in quanto l'oggetto materiale della condotta costituisce una modalità sempre più diffusa di "portabilità" del denaro. In ogni caso, rileva fin da ora sottolineare che, essendo la norma in oggetto posta a tutela anche della fede pubblica e dell'integrità complessiva del sistema bancario interno, ne consegue che l'utilizzo della carta indebitamente detenuta, anche senza il materiale conseguimento del profitto da parte dell'agente, integra la fattispecie penale di cui alla norma in parola.

Ai fini della consumazione del reato di cui all'art. 493-*ter* c.p., rileva l'utilizzazione della carta "*bancomat*" stessa, al di là delle modalità con cui la stessa è stata utilizzata, nonché a prescindere da un conseguimento concreto di somme di denaro, per cui è stata posta in essere la condotta[85].

Con riferimento sempre all'elemento oggettivo della presente fattispecie, si evidenzia che ai fini della sua configurabilità, rileva l'utilizzo della carta di credito nominativa da parte di colui che non ne è titolare; mentre, nei casi in cui la carta sia al portatore[86], per poterne sostenere l'indebito utilizzo occorre dimostrare che il soggetto abbia fatto uso della carta essendo consapevole di non esserne titolare e pertanto essendo consapevole dell'altrui appartenenza, in virtù della considerazione

[85] Si veda Cass. pen., Sez. V,12.01.2018, n. 17923: nel caso di specie la Corte, accogliendo il ricorso del procuratore generale, ha ritenuto il reato consumato e non solo tentato, sul rilievo che la accertata utilizzazione della carta "*bancomat*", di provenienza furtiva, da parte di chi non sia in possesso del codice Pin, realizzata mediante la digitazione casuale di sequenze numeriche presso uno sportello di prelievo automatico di denaro, doveva considerarsi tale da esaurire l'attitudine lesiva dei beni giuridici dell'ordine pubblico economico e della fede pubblica, sufficiente a integrare la fattispecie consumata di utilizzazione indebita di carta abilitante al prelievo di denaro contante.

Altro caso, si veda Cass. pen., Sez. V, 11.02.2019, n. 5692: in cui si è statuito che il delitto è integrato indipendentemente dall'effettivo conseguimento di un profitto o dal verificarsi di un danno e, dunque, anche in caso di introduzione della carta di credito di provenienza illecita nello sportello bancomat, senza digitare il PIN. Consultabili entrambe via *www.dejure.it*.

[86] Si veda l'ipotesi della carta ricaricabile *Viacard*.

che è possibile essere titolare di un tale tipo di carta, qualora la si possegga in buona fede nell'inconsapevolezza dell'altrui titolarità[87].

Si tratta di una norma a più fattispecie, la cui condotta tipica, dunque, può consistere alternativamente nell'indebita utilizzazione, declinabile in qualsivoglia modalità, ovvero nell'attività di falsificazione o contraffazione delle carte di credito o di pagamento da parte dell'agente. A tal proposito, la giurisprudenza ha, però, precisato che le due ipotesi di reato previste al comma primo sono autonome. Risponde, pertanto, delle ipotesi criminose in oggetto, in concorso tra loro, l'autore della contraffazione che proceda anche all'utilizzo indebito del mezzo di pagamento. Non integra, invece, il reato la detenzione di supporti magnetici ai quali non siano state ancora impresse le credenziali idonee all'uso di pagamento o di prelievo[88]. La giurisprudenza, inoltre, ha chiarito che al delitto in commento, non è applicabile l'esimente di cui all'art. 649 c.p., quando la condotta sia stata posta in essere da un familiare del titolare della carta[89].

Quanto, infine, ai rapporti del reato in esame con altri reati, il delitto può concorrere con quello di rapina della carta di credito. Diversi, infatti, sono i beni giuridici protetti dal reato di rapina e dal reato di cui all'art. 55, comma 9, d.lgs. 231/2007 – ora art. 493-*ter* c.p. – in quanto il primo tutela il patrimonio della persona offesa, mentre il secondo tutela la fede pubblica in merito all'utilizzo dei mezzi di pagamento. Si può aggiungere, inoltre, che le due fattispecie hanno anche oggetto giuridico ed elementi costitutivi diversi, in quanto mentre elemento oggettivo del reato di rapina è l'uso della violenza o minaccia da parte dell'agente al fine di impossessarsi della cosa mobile altrui ed il momento consumativo coincide con il conseguimento del profitto con altrui danno, elemento oggettivo del reato di indebito utilizzo di carte di credito è l'uso indebito in sé considerato della carta di credito altrui indipendentemente dal conseguimento di un profitto[90].

Il reato di cui all'art. 493-*ter* c.p. può concorrere anche con quello di ricettazione[91]. In particolare, risponde dei reati di ricettazione di cui all'art. 648 c.p.

[87] Così Cass. pen. Sez. II, 04.07.2012, n. 26613, in *www.dejure.it*.
[88] Cfr. Cass. pen, Sez. V, 11.03.2019, n. 15665, in *www.dejure.it*.
[89] Cfr. Cass. pen, Sez. II, 08.04.2011, dep. 21.04.2011, n. 15834, in *www.dejure.it.*
[90] Si veda Corte Appello, Torino del 3 luglio 2009, in *www.dejure.it*.
[91] V. Cass. pen. Sez. II, 18.09.2019, n. 46652, in *www.pluris-cedam.utetgiuridica.it*.

e di indebito utilizzo di carte di credito di cui all'art. 493-*ter*, comma primo, prima parte, il soggetto che, non avendo concorso alla realizzazione della falsificazione, riceve, da altri, carte di credito o di pagamento contraffatte e faccia uso di tale mezzo di pagamento[92].

Con riferimento, invece, ai rapporti tra il delitto di cui all'art. 493-*ter* c.p. e quello di frode informatica di cui all'art. 640-*ter* c.p., la giurisprudenza ha statuito che integra il primo reato la condotta di colui che, in assenza di frode, utilizzi indebitamente il codice e una tessera *bancomat* per effettuare prelievi di denaro[93].

Sussiste, invece, un contrasto giurisprudenziale in relazione alla qualificazione giuridica dell'utilizzo indebito di supporti magnetici clonati. Per alcuni tali condotte integrano l'illecito di cui all'art. 493-*ter* c.p. – indebito utilizzo di carte di pagamento clonate – per altri quello di cui all'art. 640-*ter* c.p.[94]. Secondo un orientamento giurisprudenziale, infatti, integra il reato di indebita utilizzazione di carte di credito e non quello di frode informatica di cui all'art. 640-*ter* c.p., la condotta del soggetto che attraverso frequenti prelievi presso uno sportello *bancomat* di un istituto bancario, ritiri ripetutamente del denaro contante, attraverso l'utilizzazione indebita di un supporto magnetico clonato: tale orientamento si giustifica alla luce del fatto che tale condotta, sostanziandosi nel ritiro di somme per mezzo di una carta bancomat illecitamente duplicata, configura un'ipotesi di utilizzo indebito di uno strumento di pagamento e di prelievo, che è appunto sanzionato dal predetto art. 493-*ter* c.p., che assorbe la rilevanza penale dell'eventuale alterazione fraudolenta di un sistema informatico[95]. Secondo un altro orientamento, invece, la stessa condotta rientra nell'art. 640-*ter* c.p., poiché si ritiene decisiva la sussistenza dell'utilizzo "fraudolento" del sistema informatico[96].

Tale breve esame è utile al fine di introdurre la tematica concernente il luogo di consumazione della fattispecie. A tal fine è utile ricordare che la fattispecie si

[92] *Ibidem*.

[93] Cfr. Cass. pen., Sez. II, 30.10.2019, n. 50395, in *www.dejure.it*

[94] In tal senso Cass. pen., Sez. II, 14.02.2017, n. 8913, in *www.dejure.it*.

[95] Così Cass. pen., Sez. VI, 04.11.2015, n. 1333, in *www.dejure.it.*

[96] Si veda Cass. pen., Sez. II, del 13.10.2015, n. 50140, in *www.pluris-cedam.utetgiuridica.it*.

consuma nel momento in cui vi è l'utilizzo indebito delle carte, o nel momento in cui avviene la falsificazione o la cessione a terzi.

Si ritiene ostica l'individuazione del *locus commissi delicti* in relazione ai particolari casi in cui venga attuata una compravendita *online* di carte di credito falsificate sul *dark web,* ovvero quando venga attuato un utilizzo indebito della carta mediante servizi *home banking,* o ancora quando siano effettuati acquisti *online*. In tutte queste ipotesi non risulta di diretta evidenza il luogo in cui si consuma la fattispecie, dovrebbe ritenersi applicabile l'autorevole opinione dottrinale che ritiene individuabile il *locus commissi delicti* nel luogo ove si produce il danno.

CAPITOLO IV

LE PROSPETTIVE *DE IURE CONDENDO*

SOMMARIO: 1. Considerazioni introduttive. – 2. Analisi *de iure condito*. – 3. Analisi delle prospettive *de iure condendo*. – 3.1 *(Segue)*. L'esperienza in ambito europeo (cenni) – 3.1.1 *(Segue)*. L'esperienza spagnola. – 3.1.2 *(Segue)*. L'esperienza francese. – 3.1.3 *(Segue)*. L'esperienza tedesca. – 4. Considerazioni conclusive.

1. Considerazioni introduttive

Nel corso della trattazione si è evidenziato come l'attività di individuazione del *locus commissi delicti* possa risultare un'operazione non semplice alla luce delle caratteristiche che l'illecito acquisisce nella realtà cibernetica: si tratta di condotte che assumono una veste transnazionale, aterritoriale e atemporale, su cui è bene spendere ulteriori precisazioni per fare chiarezza sulle posizioni precedentemente prospettate.

Difatti, posto che l'indagine sull'individuazione del *locus commissi delicti* debba essere compiuta seguendo il consueto metodo casistico, bisogna chiedersi se sia, peraltro, possibile rinvenire una linea ermeneutica che sia in grado di plasmare i principi generali al mutato contesto d'azione, in altre parole se sia possibile operare *de iure condito* un'interpretazione evolutiva dei principi tradizionali e prospettare soluzioni *de iure condendo*.

Le tradizionali categorie concettuali spazio-temporali non trovano un efficace riscontro nel *cyberspace* a causa della delocalizzazione e dematerializzazione delle risorse. Difatti, muta nella realtà di Internet la concezione spaziale, che è ora accessibile ai più, ad esclusione delle aree c.d. riservate di pertinenza del singolo utente. Si assiste ad una trasposizione delle attività del singolo in uno spazio nuovo, il quale necessariamente tramuta il *modus esplicandi* delle azioni, che si tradurranno in una serie di operazioni automatizzate consistenti in dati che viaggiano tra i diversi snodi della rete, contribuendo a concepire tale realtà come se fosse fluida e continuamente mutevole. Un "*panta rei*" di informazioni che rende sfuggente la suddetta realtà, che ha avuto il merito di connotare le condotte come transnazionali, consentendo ad un soggetto di trovarsi contemporaneamente in più luoghi virtuali, nonché di pianificare nel tempo operazioni da eseguirsi poi automaticamente, tale da incidere dunque sul

tradizionale modo di intendersi del tempo d'azione. Le condotte dei soggetti spaziano in tale contesto mutevole, che ignora i confini spazio-temporali differentemente dagli ordinamenti giuridici i quali «necessitano di uno spazio sul quale esercitare la propria sovranità esclusiva»[1]. Dunque, non è possibile operare una limitazione in senso spaziale della Rete, la quale è accessibile da ogni dove ad un numero illimitato di utenti, tale da rendere ardua l'individuazione del *locus commissi delicti*[2].

Ebbene tali caratteristiche favoriscono il proliferare della criminalità, che si giova del contrasto nascente tra realtà materiale e virtuale, sfruttando la transnazionalità dell'illecito, la diffusività della condotta e il presunto anonimato che domina la Rete. Queste peculiarità caratterizzano le condotte criminose compiute nel *cyberspace*, vale a dire i reati informatici, che coinvolgono modalità operative a carattere tecnologico o comunque incidono su dati, informazioni e programmi.

Come si è avuto modo di analizzare, però, la questione concerne solamente i reati a evento informatico, i reati di mera condotta commessi *online* e i tentativi di reati di evento commessi *online*: si fa riferimento a condotte che si traducono in una serie di impulsi elettronici tale da rendere ardua l'individuazione del luogo in cui si esplica il risultato di tale azione. Alla luce di queste caratteristiche così menzionate si rende necessaria una rivalutazione circa i criteri generali che permettono di circoscrivere nel tempo e nello spazio l'illecito cibernetico. Si tratta di ipotesi in cui la collocazione spaziale della fattispecie criminosa risulta ontologicamente incompatibile con l'incessante dinamicità che caratterizza la Rete. Occorre, pertanto, istituire nuovi criteri di collegamento tra la condotta criminosa e la legge applicabile, alla luce di un'interpretazione evolutiva dei principi tradizionali che vengono in considerazione.

Il legislatore ha inteso individuare il *locus commissi delicti* seguendo la teoria della ubiquità, per cui rileva sia il luogo ove il soggetto ha compiuto l'azione,

---

[1] Così SEMINARA, Locus commissi delicti, *giurisdizione e competenza nel cyberspazio*, relazione al Convegno "Presi nella rete – Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012, reperibile su www.informaticagiuridica.unipv.it/convegni/2012/SEMINARA.

[2] In tal senso si è espresso SEMINARA, *La pirateria su internet e diritto penale*, in *Riv. trim. dir. pen. ec.*, 1997, 102.

sia quello in cui si è verificato l'evento; così facendo si opera un collegamento tra il fatto e l'evento dagli ampi confini, accogliendo il principio di tendenziale universalità. L'adesione a questa teoria è giustificabile in virtù della volontà di non lasciare impunite condotte illecite, che necessitano di essere represse a livello internazionale e appare utile alla luce delle peculiarità dell'azione che risulta infatti suscettibile di espansione quanto agli effetti. Tale espansione deriva dalla diffusività delle operazioni poste in essere, dalla permanenza dei contenuti nello spazio virtuale, nonché dalla messa a disposizione di informazioni ad un numero indeterminato di utenti: riprendendo un concetto già esplicato, è la stessa automazione a determinare la protrazione nel tempo degli effetti, che possono addirittura sfuggire al controllo del reo che li ha posti in essere tramite le Tecnologie dell'Informazione.

La dimensione ontologicamente aterritoriale degli illeciti impone delle riflessioni concernenti il momento e il luogo di commissione del reato, non essendo sufficiente limitarsi ad un'analisi delle singole fattispecie.

È, pertanto, essenziale svolgere ulteriori considerazioni nell'ottica di prospettare soluzioni ragionate che permettano di far luce sui persistenti dubbi concernenti l'individuazione del *locus commissi delicti* nel *cyberspace*, partendo preliminarmente dall'analisi delle soluzioni suscettibili di adozione *de iure condito* e successivamente facendo leva su prospettive *de iure condendo* che vengono in rilievo osservando casi concreti. Come affermato da autorevole dottrina, tale contesto cibernetico funge da spunto per revisionare taluni concetti fondamentali, ricordando che «il mutare della normativa di riferimento prescinde dal movimento fisico dell'individuo da uno spazio nazionale ad uno estero, dipendendo, invece, dalla navigazione dell'utente lungo le "autostrade telematiche"»[3].

2. Analisi *de iure condito*

Si è ampiamente discusso riguardo la vocazione transnazionale della Rete che rende difficoltosa la tracciabilità di criteri giuridici che permettano di agire prontamente contro i crimini ivi perpetrati. Nonostante il contesto ubiquitario,

[3] V. RUGGIERO, *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002, 256.

dematerializzato e aterritoriale in cui si muove la criminalità informatica, è possibile individuare, *de iure condito*, un punto di sintesi, da rinvenire nell'interpretazione evolutiva del principio di territorialità. Ancorare la condotta *online* ontologicamente immateriale alla fisicità dei comportamenti intesi in senso tradizionale potrebbe consentire di rinvenire dei punti fermi in una realtà dinamica e mutevole, che caratterizza l'incessante evolversi delle tecnologie informatiche.

L'inarrestabile evoluzione tecnologica ha fatto sorgere nel corso degli anni la necessità di adattare, infatti, i tradizionali principi e concetti giuridici al mutato contesto. In tale ottica si è lungamente adoperata la giurisprudenza prospettando, in base al caso concreto, soluzioni confacenti alle nuove tecnologie informatiche, che consentissero di individuare il *locus commissi delicti*.

In tale campo di indagine dovrebbe trovare applicazione *de iure condito* un criterio flessibile, come sottolineato in dottrina, che valorizzi il rapporto tra la persona offesa e il bene giuridico protetto, restando ancorati così al tradizionale principio di territorialità, interpretato in maniera evolutiva[4]. Ebbene si è fatta avanti un'interpretazione tesa a valorizzare il luogo in cui avviene il contatto con il sistema – per i reati di condotta perpetrati *online* – e il luogo in cui si verifica il danno – per i reati di evento – di modo da ancorare l'individuazione del *locus commissi delicti* alla fisicità dei comportamenti tradizionalmente intesi.

Prendendo come riferimento il luogo in cui si instaura il dialogo con il sistema si consente di perseguire il reato nel luogo ove questo sia stato posto in essere, garantendo «un più efficace accertamento del reato e di una appropriata applicazione della pena»[5]. Questo approccio ermeneutico consente di evitare il riferimento al luogo ove è ubicato il *server* in cui transitano le informazioni, che il più delle volte non permette di esprimere appieno il disvalore della condotta e parimenti non aderisce ai principi accolti dalla Carta Costituzionale, quale il principio del giudice naturale.

È bene precisare, ancora una volta, che il *server* consente l'accesso ed offre servizi sempre disponibili all'interno di una Rete per cui non si può prescindere da

[4] Cfr. FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, cit., 1308.

[5] V. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *Dir. pen. cont.*, 2 febbraio 2015.

esso nell'utilizzo della stessa. Alla luce di ciò è doveroso sottolineare che esso può collocarsi in disparate zone del globo e consentire l'accesso indistinto a qualsiasi soggetto dotato di una connessione, da cui emerge il carattere ubiquitario della Rete. Qualora il *server* sia ubicato in un luogo fisico identificabile potrebbe astrattamente accogliersi anche l'orientamento che alloca il luogo di consumazione del reato nel luogo ove è ubicato il *server*, sebbene tale teoria sia stata scongiurata sulla base della valorizzazione della funzionalità della rete stessa, nonché in virtù del principio del giudice naturale precostituito per legge. Tale interpretazione cozzerebbe, infatti, con la struttura stessa della Rete, che si caratterizza per il suo funzionamento delocalizzato, dinamico e accessibile contemporaneamente da parte di una schiera indefinita di utenti. Dunque, il classico concetto di fisicità che lega il risultato della condotta al luogo in cui è allocato il *server* non può essere plasmato ai dettami della Rete in cui, nella maggior parte dei casi, non vi è un risultato fenomenico inteso in senso materiale che si verifica in un dato luogo, alla luce del fatto che nella Rete vi è una circolazione costante di dati contemporaneamente rinvenibili in luoghi disparati.

Ecco per quale motivo in dottrina e in giurisprudenza si è inteso privilegiare il luogo ove è situato il soggetto agente, vale a dire il luogo da cui il soggetto fa partire la condotta, che è il luogo in cui maggiormente si percepisce il disvalore dell'azione criminosa e in cui il diritto necessita di essere riaffermato. Tale soluzione ben si concilia con la realtà fluttuante dello spazio cibernetico alla luce della normativa esistente, dato che si sostanzia in un'interpretazione evolutiva del principio di territorialità che valorizza il luogo in cui è avvenuta l'azione, ma a ben vedere non può assurgere a criterio generale. Difatti, nelle non infrequenti ipotesi in cui il luogo dal quale il soggetto agisce non è rinvenibile o comunque non sia circoscritto ad un unico luogo dovrebbero assumere rilevanza ulteriori criteri. Si fa riferimento per esempio al caso in cui vengano in rilievo dispositivi mobili, *browser* anonimi o sistemi di *cloud computing*.

Tali ultime piattaforme vengono intese come l'insieme delle tecnologie caratterizzate dall'agilità di utilizzo, in quanto consentono la fornitura su richiesta di una serie di risorse preesistenti, che si sostanziano nel memorizzare, archiviare ed elaborare dati, disponibili da remoto nella forma di un'architettura distribuita, in

grado di smaterializzare la consueta fisicità intercorrente tra l'utente e la macchina sulla quale opera. I servizi che vengono offerti dal *cloud* sono gestiti da terzi, per cui tali sistemi sono caratterizzati dalla semplicità di funzionamento che ne consente una estesa fruizione. Vengono forniti, dunque, differenti modelli di *cloud* a seconda della necessità vantata dall'utente, il che consente di assecondare le disparate esigenze dei soggetti, che pertanto saranno portati ad utilizzare tale sistema, in quanto meno oneroso e di semplice utilizzo[6]. In questo tipo di sistema i dati non sono allocati in *server* fisici, ma sul *cloud* del fornitore che può geograficamente espandersi su siti distinti, contemporaneamente accessibile a diversi utenti, da cui ne emerge la forte componente aterritoriale, in quanto permette ai dati e alle informazioni di evadere dalla dimensione fisica e accogliere la caratteristica ubiquitaria. Difatti, il *cloud* costituisce un luogo in cui si determina il fallimento dei limiti temporali e territoriali che consentono di individuare il *tempus e locus commissi delicti,* ponendo così problemi relativi appunto all'accesso da remoto e alla collocazione dei dati[7]. In riferimento a tali sistemi fallisce il tentativo di individuare un unico luogo in cui sono allocati i dati o comunque il luogo dal quale il soggetto agisce per l'interazione tra i diversi soggetti; piuttosto si evidenzia

[6] Per un completo approfondimento riguardante questa nuova sfaccettatura della tecnologia sempre più diffusa si veda IASELLI, Cloud computing *per i professionisti: vantaggi e svantaggi*, in *Quot. giur*., 20 gennaio 2016, via *www.pluris-cedam.utetgiuridica.it*. L'autore evidenzia l'esistenza di diversi modelli di servizio: «Nel caso di servizi *IaaS* (*Cloud Infrastructure as a Service* – infrastruttura *cloud* resa disponibile come servizio), il fornitore noleggia un'infrastruttura tecnologica, cioè server virtuali remoti che l'utente finale può utilizzare con tecniche e modalità che ne rendono semplice, efficace e produttiva la sostituzione o l'affiancamento ai sistemi già presenti nei locali dell'azienda. Tali fornitori sono in genere operatori di mercato specializzati che realmente dispongono di un'infrastruttura fisica, complessa e spesso distribuita in aree geografiche diverse.

Negli *SaaS* (*Cloud Software as a Service* – software erogato come servizio del *cloud*), il fornitore eroga via *web* una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Tali servizi sono spesso offerti in sostituzione delle tradizionali applicazioni installate localmente dall'utente sui propri sistemi, che è quindi spinto ad "esternalizzare" i suoi dati affidandoli al fornitore. Si pensi, ad esempio, ad applicazioni tipiche per l'ufficio erogate in modalità web quali fogli di calcolo, elaborazione dei testi, applicazioni per il protocollo informatico, la rubrica dei contatti e i calendari condivisi, ma anche alle moderne offerte di posta elettronica *cloud*.

Infine, nei *PaaS* (*Cloud platform as a service* – piattaforme *software* fornite via *web* come servizio), il fornitore offre soluzioni per lo sviluppo e l'*hosting* evoluto di applicazioni. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie, allo scopo di assolvere a esigenze interne oppure per fornire a loro volta servizi a terzi. Anche nel caso dei *PaaS* il servizio erogato dal fornitore elimina la necessità per il fruitore di doversi dotare internamente di strumenti *hardware* o *software* specifici o aggiuntivi».

[7] Così ATERNO, MATTIUCCI, Cloud Forensics *e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen*., 3/2013, 877.

come vi sia una continua circolazione in Rete di dati e informazioni, in un continuo flusso che rende ardua l'identificazione degli stessi.

Ebbene in relazione a tali casi particolari emerge la labilità del criterio di individuazione del *locus commissi delicti* nel punto in cui si situa il soggetto che instaura il contatto con il sistema, che sebbene utile alla risoluzione di diverse problematiche – tra cui evitare l'accentramento della competenza esclusivamente nei luoghi ove sono allocati i *server* e rispettare il principio costituzionale del giudice naturale – non appare del tutto confacente alle numerose questioni che si pongono.

Accanto alla problematica mancata individuazione del luogo da cui il soggetto agisce, si farebbe viva l'ipotesi di una strumentalizzazione di tale criterio da parte del reo, agendo in luoghi tecnologicamente arretrati e con carente produzione normativa in un punto di diritto penale dell'informatica. Non è infrequente, infatti, l'ipotesi in cui i criminali informatici privilegino luoghi in cui vi è insufficiente tutela per i sistemi informatici e telematici, nonché limitata repressione di condotte criminose perpetrate ai danni di soggetti attraverso la Rete, riuscendo così a produrre ingenti danni nei confronti di sistemi allocati in Paesi tecnologicamente avanzati e cospicui profitti.

Sia consentito effettuare un'ulteriore digressione con riferimento a quest'ultimo assunto: il divario emergente tra paesi tecnologicamente arretrati e paesi tecnologicamente avanzati consente lo sviluppo dilagante della criminalità informatica, che strumentalizza appunto i luoghi dai quali agire, sovente denominati paradisi cibernetici. Per sfuggire a questa evenienza, la quale mette a repentaglio i numerosi tentativi di intervento volti a scongiurare tale nuova forma di criminalità, emerge sempre più la necessità di una normativa armonizzata e sovranazionale che coinvolga più Paesi possibili, proprio al fine di combattere efficacemente tale fenomeno.

Si fa strada in questo contesto, nell'ottica di adottare soluzioni *de iure condito*, un ulteriore criterio avanzato dalla dottrina, che evita di far riferimento parimenti al luogo dove viene instaurato il dialogo e al luogo ove è ubicato il *server*. Difatti, quando non sia possibile individuare il luogo dal quale il soggetto attivo ha agito, occorre – secondo autorevole dottrina – valorizzare il rapporto tra la persona

offesa e il bene giuridico protetto, su cui ricadono gli effetti dell'azione, per cui verrebbe ad assumere rilevanza il luogo in cui è avvenuta parte dell'azione che corrisponde al luogo ove si rinviene l'area giuridica oggetto di attacco[8]. Tale assunto consente di interpretare in maniera evolutiva il principio di territorialità in conformità con la teoria ubiquitaria di allocazione del *locus commissi delicti*. Parte dell'azione si rintraccia sul sistema destinatario dell'attacco e ciò consente di radicare in Italia la giurisdizione, così come stabilito dall'art. 6 co. 2 del c.p.

Questa interpretazione evolutiva porta con sé dei vantaggi volti a scongiurare una valutazione errata circa il funzionamento della Rete, nel rispetto dei tradizionali principi dell'ordinamento giuridico e supplendo le ipotesi non infrequenti in cui non sia riscontrabile una sorgente di attacco. Tale ultimo criterio sarebbe, inoltre, teso a favorire l'armonizzazione delle legislazioni nazionali che attribuirebbero maggiormente rilevanza alla tutela dei soggetti passivi.

Questa soluzione, come evidenziato da autorevole dottrina[9], trova inoltre conferma nelle fonti europee in materia di giurisdizione, che ai sensi della Direttiva 2013/40/UE statuiscono che uno Stato deve assicurare di avere competenza giurisdizionale qualora, tra le altre ipotesi, il reato sia stato commesso ai danni di un sistema situato nel proprio territorio, al di là del caso in cui l'autore del fatto criminoso fosse fisicamente presente in suddetto territorio al momento della commissione[10], in accordo peraltro con le disposizioni della Convenzione di Budapest inerenti al tema della giurisdizione al fine di scongiurare conflitti tra Stati e favorire la cooperazione.

Tuttavia, anche tale criterio non appare in grado di assurgere a principio generale alla luce delle considerazioni che ci si appresta a puntualizzare. Vi sono, difatti, ipotesi in cui non è possibile individuare una persona fisica determinata

---

[8] In tal senso FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, cit., 1307.

[9] *Ivi*, 1308 s.

[10] V. art. 12 co. 2 lett. b), Direttiva 2013/40/UE, in materia di competenza giurisdizionale, in *www.eur-lex.europa.eu*: Art.12.2 «[...]Nello stabilire la propria competenza giurisdizionale conformemente al paragrafo 1, lettera a), uno Stato membro assicura di avere competenza giurisdizionale qualora: a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato[...]».

offesa dal reato in virtù della costruzione della fattispecie – che potrebbe essere formulata sulla base di un pericolo astratto. Si tratta dei casi in cui il bene compromesso appartiene ad una schiera indeterminata di soggetti o alla generalità dei consociati, vale a dire un bene «la cui integrità rispecchia cioè un interesse diffuso tra tutti i consociati, o comunque fra cerchie ampie e indeterminate di soggetti»[11]. Un esempio concreto può essere rinvenuto nel caso di fattispecie inerenti al *cyber*-terrorismo, la cui direzione offensiva del fatto ha come obiettivo la società civile nel suo complesso[12], in quanto ad essere messi in pericolo sono beni collettivi, a titolarità diffusa, come la sicurezza nazionale e l'ordine pubblico. In altre parole, si tratta di condotte con una soglia di punibilità altamente anticipata, in virtù della rilevanza che assume la protezione del bene giuridico. È opportuno sottolineare che l'anticipazione della tutela, giustificata dall'esigenza di salvaguardare la sicurezza collettiva, deve essere bilanciata con il principio costituzionalmente tutelato della libertà di espressione, ai sensi dell'art. 21 della Costituzione, per cui si richiede la concreta pericolosità della condotta per i rilevanti interessi pubblici che vengono in considerazione[13].

Dinnanzi a queste condotte diviene complesso stabilire, innanzitutto, la giurisdizione applicabile al fine di istituire un collegamento con un ambito territoriale e secondariamente individuare il luogo esatto ove si consuma il reato, per cui il criterio summenzionato fallisce.

Alla luce della complessità della questione emerge che non è possibile trarre un criterio generale e univoco che permetta di individuare in maniera inequivoca il *locus commissi delicti*. Ci si trova di fronte a situazioni in cui le norme tradizionali

[11] Sul punto MARINUCCI, DOLCINI, *Manuale di Diritto Penale. Parte Generale*, cit., 238 s.

[12] In argomento FLOR, Cyber-*terrorismo e diritto penale in Italia*, in FORNASARI, WENIN (a cura di), *Diritto penale e modernità. Nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Napoli, 2017, 325 ss. L'Autore sottolinea come si trovi dinnanzi ad un "diritto penale al limite", in virtù dell'arretramento della soglia di rilevanza penale a condotte meramente prodromiche alla realizzazione del pericolo concreto, per il bisogno di controllare alla radice il rischio, proprio in virtù del rango dei beni giuridici che vengono in questione. Ovviamente, lasciando alle sedi opportune i discorsi in merito, questa politica legislativa deve essere sempre parametrata e bilanciata con principi costituzionali, quale quello di manifestazione del pensiero, che potrebbe risentire della legislazione promulgata nel corso degli anni in materia.

[13] Per un completo approfondimento sulla dubbia compatibilità di una così rilevante anticipazione di tutela in vista di tali beni con la libertà di manifestazione del pensiero, si veda CIRILLO, *Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di Internet*, in *Dir. pen. cont. – Riv. Trim.*, 2/2019, 81 ss.

faticano ad adattarsi al mutato contesto d'azione tipicamente transnazionale, per cui in attesa di un intervento legislativo in materia, si suggerisce – *de iure condito* – la necessità di interpretare in maniera evolutiva i principi tradizionali, in particolare il principio di territorialità, avendo a mente i criteri sopra menzionati: valorizzare ove possibile il rapporto di titolarità del sistema attaccato, privilegiando così la struttura aterritoriale della rete e, ove non sia possibile risalire ad esso, far riferimento al luogo nel quale il reo ha agito, in aderenza ai principi costituzionali.

3. Analisi delle prospettive *de iure condendo*

Le indagini svolte finora hanno permesso di evidenziare l'importanza non secondaria della questione accanto alle necessità di un intervento legislativo volto a regolare la materia. Nell'attesa che il legislatore si adoperi, è possibile prospettare talune soluzioni *de iure condendo*, volte a scongiurare dubbi ermeneutici inerenti a fattispecie concrete.

L'esigenza nascente dall'annosa questione, motore della trattazione in oggetto, riguarda l'individuazione di un criterio di collegamento tra il fatto illecito integrante un crimine informatico e le conseguenze da esso derivanti. Difatti, la disciplina inerente all'individuazione del *locus commissi delicti*, emergente dalle norme nazionali e sovranazionali, non fornisce una risposta risolutiva alla luce delle caratteristiche ontologiche del *cyberspace*. Ci si trova dinnanzi a condotte che si snodano nei diversi punti della rete, che possono essere compiute a distanza mediante operazioni automatizzate, coinvolte in una dimensione transnazionale, che ignora i confini spazio-temporali da cui emerge in tutta evidenza la difficoltà degli ordinamenti nazionali a sviluppare una risposta che sia efficace nel contrastare tali illeciti. Tale difficoltà necessita di essere sanata da interventi tempestivi a livello sovranazionale, di modo da adattare il tradizionale contesto normativo alle nuove esigenze insorgenti dallo spazio cibernetico: dinnanzi ad illeciti transnazionali la cooperazione e armonizzazione si rivelano l'unico modello d'azione in grado di contrastare tale forma di criminalità[14].

[14] In tal senso FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 192.

Alla luce di tali considerazioni è utile, come precedentemente accennato, delineare delle prospettive *de iure condendo*.

L'*input* per l'intervento auspicato potrebbe volgere lo sguardo all'esperienza nazionale di altri settori dell'ordinamento. Il riferimento è alla disciplina speciale in materia di diffamazione commessa a mezzo di trasmissione radiofoniche o televisive di cui all'art. 30 comma 5 della legge n. 223 del 1990 ovvero al disegno di legge in materia di diffamazione mediante Internet, da cui potranno scaturire criteri passibili di adattamento anche per altre fattispecie criminose[15].

La legge del 6 agosto 1990 n. 223 – c.d. legge Mammì – recante la disciplina del sistema radiotelevisivo pubblico e privato, posta la fondamentale importanza di interesse generale circa la diffusione di programmi radiofonici e televisivi, prevede l'estensione delle sanzioni in materia di diffamazione commessa a mezzo stampa ai casi di diffamazione commessa a mezzo di trasmissioni radiofoniche o televisive. Per comprendere il contesto di cui ci si appresta a trattare è necessario attuare delle premesse.

L'art. 30 della legge in esame ha avuto il merito di introdurre nell'ordinamento delle sanzioni penali per il caso in cui taluno commetta reati a mezzo di trasmissioni radiofoniche o televisive, effettuando tra l'altro numerosi riferimenti alla legge sulla stampa n. 47 del 1948. All'art. 30 comma 4 si statuisce l'applicabilità delle sanzioni previste dall'art. 13 della legge n. 47 del 1948 ai soggetti concessionari pubblici e privati. In particolare, la legislazione in tema di stampa contiene una disciplina speciale in tema di diffamazione, stante l'uso privilegiato di tale mezzo ai fini della commissione dell'illecito, che risulta aggravato: l'art. 13 prevede, difatti, una disciplina sanzionatoria maggiormente gravosa rispetto a quella indicata dall'art. 595 co. 3 c.p., nel caso in cui a mezzo stampa sia commessa un'offesa all'altrui reputazione consistente nell'attribuzione di un fatto determinato[16]. A tali gravose sanzioni fa riferimento finanche l'art. 30

[15] Di tale avviso FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite,* cit., 1309, che alla nt. 43 suggerisce tale spunto di riflessione.

[16] V. Art. 13 "Pene per la diffamazione", Legge 8 Febbraio 1948 n. 47, "Disposizioni sulla stampa": «Nel caso di diffamazione commessa col mezzo della stampa, consistente nell'attribuzione

della l. n. 223/1990, che ha esteso l'aggravante anche all'ambito della radio e della televisione, eliminando una possibile disparità di trattamento[17].

L'art. 30 suscita interesse ai fini della trattazione oggetto di analisi per il contenuto di cui al comma 5, difatti risulta un punto di riflessione utile ai fini dell'individuazione del *locus commissi delicti* nella realtà cibernetica. Si statuisce che in caso di diffamazione consistente nell'attribuzione di un fatto determinato commesso attraverso trasmissioni, il foro competente è determinato dal luogo di residenza della persona offesa.

Parimenti ha statuito la Corte di Cassazione, la quale ha stabilito che «In tema di diffamazione commessa a mezzo di trasmissioni radiofoniche e televisive, la competenza territoriale deve essere stabilita applicando l'art. 30 comma 5 della l. 6 agosto 1990, n. 223, e cioè con riferimento al luogo di residenza della parte lesa, chiunque sia il soggetto chiamato a rispondere della diffamazione»[18]. Tale disciplina, con la relativa pronuncia, mira ad assicurare una tutela effettiva al soggetto offeso nella reputazione.

Alla luce delle considerazioni così svolte, è possibile partire da tale criterio che si riferisce ad una realtà prettamente materiale per prospettare, *de iure condendo*, una soluzione valevole in ambito cibernetico. Il criterio da ultimo menzionato, che si riferisce alla residenza del soggetto offeso, ben potrebbe essere adottato nell'ambito dei *cybercrimes*, in quanto si opererebbe così un approccio certo e univoco che consentirebbe di evitare le indefinite difficoltà concernenti l'individuazione del luogo da cui il reo fa partire l'attacco, così come permetterebbe di scongiurare i problemi inerenti alla struttura della Rete e di conseguenza evitare riferimenti alle tecniche di localizzazione dei flussi di dati. Si conferirebbe in tal modo un'ampia tutela al soggetto passivo, per cui verrebbe attribuita maggiore rilevanza al diritto della personalità leso. Tale prospettiva è passibile di adattarsi non solo alle ipotesi di diffamazione perpetrate con il mezzo telematico, ma

di un fatto determinato, si applica la pena della reclusione da uno a sei anni e quella della multa non inferiore a lire 500.000».

[17] Sul punto si veda il *dossier* (serie Disegni di legge) n. 390 dell'ottobre 2012 del Servizio Studi del Senato della Repubblica "Diffamazione a mezzo della stampa o altro mezzo di diffusione AA. SS. 3491 e 3492. Elementi di documentazione e di diritto comparato".

[18] Cfr. Cass. Pen., Sez. I, 13.01.2000, n. 269, in *www.dejure.it*.

parimenti ad ulteriori ipotesi di reati cibernetici che risentono della problematica relativa all'individuazione del *locus commissi delicti*.

Sempre nell'ottica di prospettare soluzioni *de iure condendo*, appare utile disquisire sul tema del progetto di riforma in materia di diffamazione a mezzo Internet, da cui si potrebbe tentare di intravedere un criterio di individuazione del *locus commissi delicti* passibile di estensione per i reati cibernetici. In particolare, si fa riferimento al progetto di legge recante "Modifiche alla legge 8 febbraio 1948, n.47, al codice penale, al codice di procedura penale, al codice di procedura civile e al codice civile, in materia di diffamazione, di diffamazione con il mezzo della stampa o con altro mezzo di diffusione, di ingiuria e di condanna del querelante nonché di segreto professionale, e disposizioni a tutela del soggetto diffamato"[19]. Tale progetto di riforma ha l'obiettivo di garantire una più efficace tutela alla persona lesa nell'onore e parimenti garantire la libertà di stampa, nonché il diritto di cronaca. Inoltre, esso mira ad escludere per la scarsa efficacia deterrente l'applicabilità della pena della reclusione per il reato di diffamazione, irrigidendo piuttosto il trattamento sanzionatorio circa le pene pecuniarie, sia con riferimento alla disposizione concernente le sanzioni di cui alla legge n. 47/1948, sia con riferimento alla disposizione sancita dal codice penale all'art. 595. Fondamentale risulta l'innovazione proposta in relazione all'art. 1 della legge n. 47 del 1948, che introduce un'importante modifica, concernente l'estensione «dell'applicazione delle disposizioni di tale normativa anche alle testate giornalistiche online registrate ai sensi dell'articolo 5, limitatamente ai contenuti pubblicati, trasmessi o messi in rete nonché alle testate giornalistiche radiotelevisive»[20]. A tutela del soggetto leso sono previste, altresì, modalità di rettifica per le testate giornalistiche *online* e per la stampa non periodica.

Passando ora alla modifica che qui interessa, si evidenzia come all'art. 1 comma 1 lett. f) del presente progetto di legge, recante "Modificazioni alla legge 8 Febbraio 1948 n. 47", sia disposta la modifica dell'art. 21 della citata legge a cui è

[19] V. Disegno di legge, d'iniziativa del senatore Caliendo, XVIII Legislatura, n. 812. Il presente progetto è stato presentato in data 20 Settembre 2018. Tale progetto è stato preceduto dal disegno di legge n. 1119 della XVII Legislatura: per un approfondito commento si consenta di rinviare al contributo di GULLO, *La tela di Penelope. La riforma della diffamazione nel Testo unificato approvato alla Camera il 24 giugno 2015*, in *Dir. pen. cont. – Riv. Trim.*, 1/2016, 31 ss.

[20] Ivi, 2.

aggiunto un ulteriore comma, il quale dispone che «Per il delitto di diffamazione commesso mediante comunicazione telematica è competente il giudice del luogo di residenza della persona offesa»[21]. Con tale modifica si porrebbe fine all'annosa questione concernente il *locus commissi delicti* inerente alla diffamazione *online*, in quanto si stabilirebbe così uno specifico riferimento normativo valevole in tale ambito, senza lasciare spazio ai dubbi che hanno lungamente attanagliato dottrina e giurisprudenza circa la consumazione. Ebbene, il criterio menzionato potrebbe assurgere a criterio generale cui far riferimento nel caso in cui vengano in rilievo reati cibernetici commessi *online*.

Sulla scorta di queste brevi soluzioni prospettabili *de iure condendo* non può che auspicarsi un intervento legislativo che ponga fine ai dubbi in merito.

3.1 *(Segue)*. L'esperienza in ambito europeo (cenni)

L'esigenza primaria emergente in relazione alla tematica concernente l'individuazione del *locus commissi delicti* è quella di un intervento normativo che consenta di sopire i numerosi dibattiti dottrinali e giurisprudenziali in materia – stante l'importanza della questione – sempre tenendo a mente la rilevanza del tema a livello internazionale alla luce della "*cross-border nature*" dei reati cibernetici, che necessiterebbero una politica legislativa comune, volta all'armonizzazione delle legislazioni. Tuttavia, in attesa di un passo decisivo da parte del legislatore, è bene volgere lo sguardo alle esperienze europee in merito, per tentare, senza pretesa di completezza, di prospettare brevemente possibili soluzioni *de iure condendo*.

3.1.1 *(Segue)*. L'esperienza spagnola

La lotta alla criminalità informatica è un obiettivo condiviso dei Paesi europei, che evidenziano la necessità di un agire comune in grado di combattere questo dilagante fenomeno. Il problema di individuazione del *locus commissi delicti*, pertanto, si riafferma in ciascuno di essi a causa della natura transnazionale dei reati cibernetici.

In particolare, in Spagna si manifesta la necessità di una lotta comune contro tali illeciti mediante l'istituzione di uno spazio di cooperazione internazionale,

[21] Cfr. Art. 1 comma 1 lett. f) del Disegno di legge n. 812, XVIII Legislatura.

volto a istituire regole comuni nel perseguimento dei suddetti crimini[22]. Si sottolinea, difatti, come si tratti di crimini transnazionali, per cui determinare il luogo del commesso reato è un'operazione di fondamentale importanza alla luce delle caratteristiche del crimine in oggetto, che consente di individuare diversi possibili luoghi fisici in cui localizzare il fatto, come il luogo ove si trova il reo, il terminale, dove si trovano i *server* e i fornitori di servizi, nonché ove viene attivato il dialogo logico con il sistema sul quale si agisce[23].

Nel dettaglio, di significativa rilevanza risulta la riforma in materia di terrorismo del 2015 che, tra le altre modifiche introdotte al codice penale, ha qualificato quali reati terroristici anche i reati informatici di cui agli articoli 197-*bis*, 197-*ter*, inerenti all'accesso abusivo ad un sistema informatico e la diffusione di programmi informatici e codici di accesso atti a commettere il reato di cui sopra e l'intercettazione di telecomunicazioni, e agli articoli 264-264-*quater* del codice penale, inerente ai delitti di danneggiamento, quando questi siano commessi con finalità di terrorismo[24]. Inoltre, la riforma in questione mira a scongiurare qualsiasi forma di propaganda del terrorismo, nonché istigazione commessa con strumenti telematici, per via dell'alta diffusività degli stessi.

Un'altra importante novità, contenuta nella *Disposición final primera*, è costituita dall'estensione della legge penale applicabile, per cui si dispone l'ampliamento della competenza spagnola non più solo ai cittadini spagnoli, ma parimenti agli stranieri che risiedano in Spagna o si trovino sul suo territorio che

---

[22] In tal senso FLORES PRADA, *Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia*, in *Revista Electrónica de Ciencia Penal y Criminología*, 2015, 17-21, in *www.criminet.ugr.es*.

[23] Ivi, in cui l'autore afferma «*La determinación del lugar de comisión del delito juega entonces un papel fundamental en la determinación de la jurisdicción nacional —primero—y en la asignación del tribunal concreto —después—que habrá de asumir la competencia para el conocimiento de los delitos transfronterizos cometidos a través de las redes informáticas. Se trata, sin embargo, de una tarea extraordinariamente difícil, no solo por la propia dificultad de determinar los anclajes físicos de la ciberdelincuencia, sino también porque este tipo de criminalidad presenta por lo general características que favorecen la concurrencia de jurisdicciones, como la posibilidad de duplicidad o multiplicidad de lugares físicos en los que situar la actividad —lugar donde actúa el actor, lugar donde se encuentra su terminal, lugar donde se activan los programas informáticos a través de los que actúa, lugar donde se encuentran los servidores o los proveedores de servicios—, o la multiplicidad de lugares en los que, con frecuencia, cabe situar el resultado de la conducta —delitos contra la propiedad intelectual, delitos contra el honor, estafas múltiples, etc.—.*».

[24] *Artículo único, Ley orgànica* del 30 marzo 2015 n. 2, che modifica l'art. 573 "*Definición de delito de terrorismo*" del *Código Penal*, in *www.eur-lex.europa.eu*.

abbiano commesso un crimine di terrorismo. Si evince, quindi, l'applicazione del principio di territorialità per cui ogni qual volta un simile reato venga commesso in territorio spagnolo si determina l'estensione della legge penale spagnola. In particolare, l'organo competente viene individuato con riferimento al momento in cui il soggetto attivo immette le informazioni in Rete, in cui si radicherà la competenza territoriale.

In generale, qualora la condotta si possa ritenere esplicata nei territori di diversi Stati, la dottrina spagnola attribuisce rilevanza per i "*delitos de mera acción*" al luogo in cui è avvenuta l'azione determinante[25]; per i "*delitos de mera conducta*" si evidenzia che l'azione è ancorata sia al luogo in cui il soggetto agisce, sia al luogo in cui sono situati i sistemi attraverso i quali agisce il soggetto, per cui riconoscendo l'esistenza di un tipo di azione materiale e una virtuale, è necessario attribuire rilevanza al luogo in cui si trovano fisicamente tali sistemi[26].

Da questa breve analisi emergono soluzioni diverse a seconda dei casi che vengono in considerazione. Potrebbero parimenti adottarsi anche nella legislazione italiana diversi criteri a seconda della struttura del reato che viene in luce, tenendo sempre a mente le peculiarità dello spazio cibernetico.

3.1.2 *(Segue)*. L'esperienza francese

L'ordinamento francese, al fine di scongiurare dubbi in merito all'individuazione del *locus commissi delicti* e precisamente in merito ai criteri di collegamento tra il fatto e la legge applicabile, è intervenuto attraverso l'introduzione di una norma, l'art. 113-2-1 nel *Code pénal*, volta a delineare l'ambito giurisdizionale per i reati commessi mediante la rete.

---

[25] FLORES PRADA, *Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia*, cit., «*Para los delitos de mera acción, en los que la conducta pueda entenderse desarrollada en territorios de diversos Estados, se propone el citado criterio de la acción relevante o determinante, entendiendo por tal la que domina la conducta, la controla, la desencadena, la coordina, la que integra la parte sustancial de la acción y localiza la decisión de la acción*».

[26] *Ivi*, «*En los delitos de mera conducta, los criterios deben completarse con una orientación pensada para la ciberdelincuencia: la acción tanto se ancla en el lugar en el que esté físicamente el sujeto, como en el lugar en los que estén los equipos o sistemas a través de los que el sujeto actúe. Se reconoce así el modus operandi en el ciberespacio, en el que hay una conducta física y una acción virtual, o puesta en acción virtual. Se incluye por ello en el lugar de la acción el lugar en el que estén físicamente los equipos, sistemas o terminales a través de los que el sujeto actúe o se sirva —servidores, plataformas, ordenadores, terminales, sistemas etc.—*».

La norma in questione, introdotta con la legge n. 731 del 3 Giugno 2016[27], prevede che, qualora un fatto criminoso sia commesso a danno di una persona fisica residente sul territorio o a danno di una persona giuridica avente sede sul territorio della Repubblica, questo si considera commesso sul territorio della stessa[28]. Si è introdotta, pertanto, una norma *ad hoc* volta a rafforzare la lotta contro la criminalità che trova nella realtà cibernetica uno spazio in cui proliferare, migliorando altresì l'efficienza e le garanzie procedurali. Tale norma adotta, infatti, il principio di personalità passiva – volto a tutelare il soggetto passivo vittima di un attacco – che prevale sull'ubicazione geografica del reo che commette il fatto criminoso.

Il *Code pénal* aderisce alla teoria di ubiquità per cui il fatto si considera commesso nel territorio dello Stato quanto ivi è avvenuto uno dei fatti costitutivi[29]: tale teoria è strettamente connessa al principio di territorialità, in quanto si richiede che sul territorio siano comunque commessi fatti costitutivi del reato, per cui con tale novella legislativa si rafforza ulteriormente la forza attrattiva della legge penale francese, declinando il criterio di applicazione della legge nello spazio sulla scorta del principio di personalità passiva[30]. L'applicazione di questo principio permette di scongiurare dubbi in merito al luogo in cui il reato commesso tramite la Rete viene consumato, alla luce del fatto che non è sempre semplice determinare dove un reato cibernetico viene commesso in virtù dell'universalità della Rete.

Questo criterio di individuazione, che fa leva sul soggetto passivo, viene adoperato parimenti in Italia al fine di individuare il giudice territorialmente competente in relazione a un caso di diffamazione commessa contro un soggetto

[27] V. Art. 28 *Loi* n. 2016-731 del 3 Giugno 2016, in *www.legifrance.gouv.fr*.

[28] Cfr. Art. 113-2-1 *Code pénal*, che dispone quanto segue: «*Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République*».

[29] Cfr. Art. 113-2 *Code pénal*, che dispone quanto segue: «*La loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire*».

[30] V. DELAGE, *Brèves remarques sur l'article 113-2-1 du Code pénal*, 8 settembre 2017, in *www.actu-juridique.fr;* in argomento si veda anche HONNORAT, *Extension de la territorialité des poursuites pénales en matière de cybercriminalité*, in *Réseau Eurojuris France*, 10 gennaio 2017, in *www.eurojuris.fr*.

determinato[31]. Tuttavia, è stato sottolineato come tale principio possa risultare obsoleto dinnanzi alle immense capacità della Rete, che sovente non permettono di identificare un soggetto passivo determinato. Difatti, la giurisprudenza francese è piuttosto orientata verso diversi criteri che permettano di individuare con esattezza il luogo della commissione al fine di stabilire il tribunale competente, ferme restando le particolarità dei *cybercrimes* che vengono in considerazione: in un primo momento si è fatto strada il principio di ricezione di messaggi immessi in Rete; secondariamente il principio di accessibilità dei siti relativi ad Internet; infine il criterio di focalizzazione, che statuisce il principio per cui il crimine deve essere diretto verso il pubblico francese[32].

Malgrado ciò, è bene ribadire che il problema di individuazione del luogo di commissione dei *cybercrimes* pone dubbi interpretativi generalizzati, che in tal caso sono stati parzialmente risolti mediante l'introduzione di un criterio *ad hoc*, consacrando un criterio di collegamento tra il fatto e il soggetto vittima, sebbene tale introduzione normativa non sia andata esente da critiche.

Questa premessa è utile per svolgere una breve analisi comparatistica per identificare *de iure condendo* criteri innovativi suscettibili di applicazione nel territorio italiano. Come è emerso dalle disposizioni nazionali in materia di diffamazione e del relativo progetto di riforma, si evince una tendenza a privilegiare – in tal caso per estendere la giurisdizione sulla scorta della legge applicabile – il luogo di residenza del soggetto passivo o comunque il luogo di appartenenza di quest'ultimo, al fine di garantire maggiori garanzie. Valorizzare il luogo in cui il soggetto passivo risiede comporta inevitabilmente dei vantaggi, in quanto mira ad evitare una strumentalizzazione da parte del soggetto attivo del luogo di commissione del reato – il quale potrebbe privilegiare luoghi con una legislazione maggiormente permissiva – nonché evitare lungaggini derivanti dai problemi legati all'individuazione della sorgente dell'attacco.

3.1.3 *(Segue)*. L'esperienza tedesca

[31] Sul punto CAMPLANI, Locus commissi delicti, *norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Arch. pen.*, 2/2020, 1° settembre 2020.

[32] In tal senso PEREIRA, *La lutte contre la cybercriminalité: de l'abondance de la norme à sa perfectibilité*, in *Revue internationale de droit économique*, 2016, 3, 387 ss., via *www.cairn.info*.

La delimitazione spaziale della criminalità informatica si rivela un problema tangibile per l'applicazione del diritto penale anche nell'ordinamento giuridico tedesco, alla luce delle caratteristiche di suddetta criminalità in grado di intensificare fenomeni transnazionali. Proprio per tale motivo si suggerisce un'armonizzazione del diritto penale, mediante la criminalizzazione reciproca di determinati comportamenti devianti per migliorare il perseguimento di tali condotte criminose a livello internazionale.

Analizzando nel dettaglio la normativa inerente all'applicazione della legge penale tedesca nello spazio, si precisa che il codice penale tedesco – lo *Strafgesetzbuch* – aderisce alla teoria dell'ubiquità per cui un fatto si considera commesso nel luogo nel quale il soggetto attivo ha agito, ovvero in caso di omissione, in quello in cui avrebbe dovuto agire, o nel luogo in cui l'evento del fatto si sia verificato o si sarebbe dovuto verificare[33].

Partendo da questo principio consacrato al § 9 comma 1, nella dottrina tedesca si sono avanzate varie teorie in merito all'individuazione del *locus commissi delicti* ove venga in essere un delitto compiuto mediante le Rete.

La prima teoria estende il concetto del *locus commissi delicti*, fissandolo nel luogo in cui emerge il pericolo o avrebbe potuto verificarsi il pericolo di verificazione l'evento, in quanto in caso di reati di pericolo è in quello spazio che la condotta esplica la propria pericolosità; la seconda teoria fa leva su un collegamento oggettivo tra il fatto e il territorio, riferendosi al luogo a cui la condotta sia finalisticamente indirizzata, in quanto in caso di reati di pericolo non è richiesta la verificazione dell'evento; infine vi è la teoria che privilegia il luogo in cui vengono inseriti i dati[34].

Alla luce di queste considerazioni, si evince che le prime due teorie summenzionate accolgano criteri eccessivamente elastici soggetti ad un'ampia dilatazione e strumentalizzazione. La teoria da ultimo descritta, invece, fa leva sul luogo di immissione dei dati in Rete: tale teoria è ancorata alla fisicità dell'azione, in quanto la dottrina ritiene che i criminali pongano in essere la propria azione nel mondo fisico, vale a dire che ci sarebbe sempre un punto di contatto con il sistema

[33] Cfr. § 9 comma 1 del Codice penale tedesco.

[34] V. CAMPLANI, Locus commissi delicti, *norme di collegamento e reati informatici a soggetto passivo indeterminato*, cit., 22 s.

su cui la persona agisce, per cui il luogo rilevante è quello in cui si trova l'autore che immette i dati e instaura il dialogo con il sistema[35].

Come si può evincere, tale orientamento è parimenti seguito dalla giurisprudenza di legittimità italiana. Tale criterio risulta evidentemente di intuitiva applicazione ove il soggetto attivo sia individuabile e risulta, altresì, vicino alla fisicità dei comportamenti tradizionalmente intesi. Collocare il *locus commissi delicti* nel luogo in cui il soggetto agisce equivale a rispettare il principio di naturalità del giudice, sancito dalla Costituzione italiana, per cui sarebbe astrattamente prospettabile una soluzione in tal senso. Non va sottaciuto che anche quest'ultima soluzione nasconde delle criticità nel caso in cui si tratti di un reato di evento, in quanto tale soluzione anticiperebbe la soglia di rilevanza del fatto. Si sono già evidenziati gli altri aspetti negativi che affliggono questo tipo di soluzione, per cui talvolta il soggetto agente non risulta individuabile per via della manipolazione dell'indirizzo IP ovvero ancora potrebbe strumentalizzare il criterio suddetto facendo partire l'azione in Paesi tecnologicamente arretrati.

4. Considerazioni conclusive

L'evoluzione del diritto penale è strettamente ancorata all'agire umano, per cui all'evolversi delle modalità di aggressione dovrebbe corrispondere un'evoluzione di metodi e tecniche giuridiche al fine di contrastare la criminalità. Ciò è indice del fatto che il diritto non può essere ancorato a formule fisse, ma dovrebbe progredire di pari passo alla società per evitare che determinati comportamenti criminosi restino impuniti. La materia *cyber* è quella in cui, più di ogni altra, presente e futuro hanno un confine largamente labile, per cui si rilevano necessarie capacità inventive in grado di supplire ad eventuali carenze sul piano normativo[36].

Ebbene, la tematica oggetto del presente elaborato evidenzia questa particolare necessità. Difatti, dinnanzi al silenzio del legislatore su un tema che ha

[35] Per un approfondimento si veda il contributo di BRODOWSKI, FREILING, *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft,* in *Forschungsforum Öffentliche Sicherheit*, 2011, 4, 164 ss., in *www.sicherheit-forschung.de*.

[36] Così SEVERINO, *Le leve e le sfide per il rilancio del Paese. Le frontiere della sicurezza informatica e prevenzione del* Cybercrime, Cernobbio, 2017.

suscitato dibattiti dottrinali e giurisprudenziali, occorre adoperarsi al fine di scovare l'interpretazione ermeneutica maggiormente confacente alle caratteristiche della realtà cibernetica. È emerso che tale problematica è particolarmente sentita anche da altri ordinamenti europei, che in modo diverso hanno regolato la disciplina. Il problema di individuazione del *locus commissi delicti* coinvolge la stessa rilevanza penale del fatto e smuove i numerosi dubbi concernenti la nozione stessa di consumazione.

Come prospettato da autorevole dottrina italiana, in tale silenzio bisogna adoperarsi al fine di risolvere potenziali conflitti sorgenti dalle diverse modalità di esplicazione dell'illecito, in grado di coinvolgere diversi Paesi, in virtù della connotazione transnazionale. Tale caratteristica fa emergere le difficoltà degli Stati di sviluppare criteri generali nazionali, in grado di adattarsi ai crimini che vengono in rilievo, per cui si rende necessaria una cooperazione internazionale, volta all'armonizzazione delle legislazioni e che limiti soluzioni strettamente ancorate alla singola realtà territoriale[37].

Alla luce dell'analisi sin qui compiuta, si evince la possibilità di adottare, *de iure condito*, un'interpretazione flessibile che sia in grado di adattarsi alle numerose peculiarità dell'illecito cibernetico, in quanto le norme tradizionali, quale il principio di territorialità, faticano ad adattarsi ad un contesto così mutevole aterritoriale e immateriale. Si sottolinea, quindi, che *de iure condito* potrebbe farsi riferimento al luogo in cui il soggetto passivo possiede il proprio centro di interessi, ponendo in tal senso l'evento nel luogo ove questo si trova, vale a dire ove si produce il danno – soluzione peraltro prospettata dalla Corte di giustizia europea, in caso di lesione dei diritti della personalità, in quanto l'attribuzione della competenza al giudice del luogo ove il soggetto passivo possiede il proprio centro di interessi corrisponderebbe ad una corretta amministrazione della giustizia – adottando così un criterio maggiormente flessibile confacente alle peculiarità del cyberspazio; altrimenti potrebbe adoperarsi l'ulteriore criterio che predilige, quale *locus commissi delicti*, il luogo ove si instaura il dialogo logico con il sistema.

[37] V. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., 192.

Non può che auspicarsi un intervento legislativo *ad hoc* che superi i limiti del principio di territorialità e abbracci le peculiari connotazioni che l'illecito assume nel *cyberspace*, al fine di evitare forzature in ambito ermeneutico. A tal fine può suscitare interesse la precedente analisi svolta la quale, *de iure condendo*, invita a prendere come spunto di riflessione la disciplina prevista in tema di diffamazione commessa mediante trasmissioni radiofoniche o televisive ovvero volgendo lo sguardo al progetto di legge in tema di diffamazione *online*. Ancora utili potrebbero risultare, altresì, le esperienze estere sul tema, da cui si evincono soluzioni disparate e interessanti al fine di individuare il *locus commissi delicti* per un efficace contrasto ai *cybercrimes*.

Concludendo, tali riflessioni sono state svolte nell'ottica di prospettare soluzioni *de iure condendo*, in grado di esaltare le connotazioni dei crimini cibernetici nel *cyberspace*, in cui le classiche nozioni di azione ed evento mutano radicalmente di significato.

CONCLUSIONI

Nella parte iniziale del presente elaborato si è posto in evidenza come l'individuazione del *locus commissi delicti* sia un'operazione imprescindibile in vista della collocazione spaziale della fattispecie criminosa che implica delle conseguenze sia in ottica sostanziale che procedurale.

È emerso che l'attività da ultimo menzionata non risulti di immediata soluzione con riferimento a figure di reato, i *cybercrimes*, connotate da caratteristiche peculiari che pongono problemi di applicazione dei principi tradizionali dell'ordinamento penale.

In virtù di questa premessa, nel tentativo di fornire una risposta esaustiva a tale problematica, si è proceduto ripercorrendo le tappe salienti che hanno caratterizzato l'evolversi della realtà cibernetica, fino a giungere ad un'analisi sufficientemente dettagliata concernente le singole fattispecie, che risentono della tematica in oggetto.

I *cybercrimes* si differenziano, infatti, per la natura tipicamente aterritoriale e atemporale, la quale evidenzia la loro ontologica incompatibilità con le classiche nozioni di collocazione spaziale, tradizionalmente intese. Il *cyberspace*, il luogo ove tali condotte devianti sono poste in essere, mal si concilia con l'idea di delimitazione spaziale delle azioni umane: come più volte sottolineato nel corso della trattazione, esso consente la delocalizzazione delle risorse e delle attività espletate nonché la detemporalizzazione di queste ultime.

Proprio nel cyberspazio si è rinvenuto il punto di partenza dell'analisi svolta, teatro di innovative modalità di aggressione, che hanno condotto il legislatore a reagire dinnanzi alle nuove minacce cibernetiche mediante interventi legislativi di portata nazionale e internazionale, posta la necessità di una cooperazione volta a disincentivare il dilagante propagarsi della nuova forma di criminalità. Si è avuto modo di notare che il continuo progredire della Rete è stato considerato un terreno fertile per i cybercriminali, i quali hanno declinato a proprio favore le caratteristiche tipiche della nuova dimensione, lontana dai concetti di fisicità e materialità, con cui l'individuo era solito rapportarsi.

Gli interventi legislativi volti a sopire il fenomeno hanno condotto all'incriminazione di nuove tipologie di condotte, mancando però di considerare le problematiche relative alla particolare modalità di esplicazione delle stesse, che rendono ostica l'applicazione dei tradizionali principi dell'ordinamento. Le condotte si traducono, difatti, in una serie di operazioni automatizzate, che si snodano nei diversi punti della rete e ciò rende problematica la collocazione spaziale del punto in cui il reato si considera consumato.

A tal proposito è risultata utile la digressione svolta sulla nozione di consumazione del reato e sui principi di applicazione della legge penale nello spazio, volta ad analizzare il principio di territorialità, universalità, di personalità attiva e passiva e individuare i limiti degli stessi. In particolare, si è avuto modo di verificare che l'individuazione dei limiti di operatività della legge penale nello spazio possa avvenire mediante la combinazione di tali principi, che vanno temperati tra loro così da ricomprendere la vastità delle situazioni che possono manifestarsi nella realtà fisica. Inoltre, giova ricordare la teoria utilizzata dallo stesso legislatore al fine di individuare il *locus commissi delicti*, vale a dire la teoria dell'ubiquità, per cui il reato si considera commesso nel territorio dello Stato tanto se ivi è avvenuta parte dell'azione tanto se ivi si è verificato l'evento.

Da questo svincolo si è intrapresa l'analisi concernente il diverso atteggiarsi delle condotte esplicate in rete, per cui si è evidenziato come il fatto venga polverizzato in diversi luoghi, così da ritenere opportuno un intervento internazionale che emendi i criteri di collegamento tra il fatto commesso *online* e l'ordinamento giuridico. Se ne è dedotto che è proprio il particolare *modus operandi* dell'azione che rende doverosa l'individuazione di peculiari criteri, date le caratteristiche sottolineate in grado di scardinare i principi cardine dell'ordinamento penale. A ciò va premesso che tale problematica si è posta non per tutte le categorie di illecito che coinvolgono sistemi informatici o telematici, bensì solamente per i reati a evento c.d. informatico, i reati di mera condotta commessi *online*, nonché per le ipotesi di tentativo di reati di evento commessi *online*, per cui la condotta o l'evento realizzatosi in Rete e, in particolare, le tecniche di automazione, determinano la circolazione e la permanenza dei dati nello spazio cibernetico, tale da non rendere identificabile il luogo esatto in cui il reato si è

consumato. Questo ha portato alla nascita di autorevoli voci che hanno evidenziato la necessità di un diritto giudiziale flessibile[361], alla luce del contesto transnazionale, immateriale e aterritoriale in cui i *cybercrimes* operano.

Le considerazioni qui brevemente riportate hanno condotto la giurisprudenza a farsi carico della questione, con l'intento di fornire soluzioni che potessero risultare confacenti alla luce della struttura atipica che l'illecito acquisisce nel *cyberspace*. Sono stati avanzati diversi orientamenti nel tentativo di fornire una risposta adeguata alle caratteristiche della Rete. Da un lato, un orientamento legato alla fisicità dei comportamenti intesi in senso materiale, legando il luogo di consumazione all'allocazione spaziale del *server* centrale; dall'altro, un orientamento volto a privilegiare la struttura della Rete, individuando il luogo del commesso reato nel luogo ove l'agente fa partire il dialogo logico con il sistema.

Dinnanzi a tali soluzioni la giurisprudenza di legittimità ha privilegiato la struttura unitaria della Rete e il principio del giudice naturale precostituito per legge, prediligendo il luogo ove è allocato il *client*. Tuttavia, tale risposta ermeneutica non risulta pienamente soddisfacente in virtù delle peculiarità delle azioni criminose commesse nel cyberspazio che talvolta non consentono di individuare il luogo da cui parte il dialogo logico con il sistema – si pensi ai dispositivi mobili – o ancora potrebbe favorire il fenomeno del *forum shopping*, consentendo al reo di scegliere il luogo da cui far partire l'azione. Peraltro, questa soluzione non è l'unica prospettata in virtù del fatto che il principio espresso dalla giurisprudenza di legittimità non risulta applicabile a tutte le fattispecie criminose perpetrabili nel *cyberspace*, per cui si è evidenziato come la questione debba essere affrontata adottando un metodo casistico per comprendere le incompatibilità con i principi tradizionali, in quanto le soluzioni avanzate dipendono dalla struttura della fattispecie che di volta in volta viene in essere e dal momento consumativo.

Date le criticità poste in luce, in dottrina si è sottolineato come una soluzione maggiormente flessibile e in linea con le caratteristiche tipiche dell'illecito cibernetico potrebbe sopire i problemi attinenti all'individuazione del *locus commissi delicti*: si è, infatti, proposto di valorizzare il luogo ove si produce il

[361] FLOR, *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 10/2015.

danno, al fine di offrire effettiva tutela al bene giuridico protetto dalla norma incriminatrice, quale soluzione adottabile *de iure condito*. Con tale proposta si ha l'intento di distanziarsi dalla classica interpretazione del principio di territorialità, per abbracciare un approccio flessibile che sia compatibile con le peculiarità dello spazio cibernetico, così da valorizzare il luogo ove il bene giuridico tutelato dalla norma incriminatrice subisce un danno.

Merita di essere rilevato che con questo innovativo criterio, peraltro adottato finanche in seno alla giurisprudenza europea in sede civile, si consente di tutelare adeguatamente la vittima, che collocherà il proprio centro di interessi nei Paesi che offrono maggior protezione sul piano della cybersicurezza e offre dei vantaggi dal punto di vista processuale ed in particolare per l'attività di indagine, che si svolgerà dapprima sul luogo di produzione del danno per poi individuare il luogo da cui l'azione è partita.

Nelle more di un intervento *ad hoc* volto a sopire le molteplici problematiche delineate, si sono prospettate soluzioni *de iure condendo*, che mirano a valorizzare il particolare contesto di azione dell'illecito cibernetico al fine di recepire un criterio comune, applicabile ogni qual volta ci si trovi dinnanzi ad un comportamento deviante perpetrato nel *cyberspace*: si fa riferimento alle proposte avanzate dai diversi settori dell'ordinamento nazionale, nonché ai modelli adottati dai paesi europei, che fanno leva sul luogo in cui si trova il soggetto passivo o sul luogo di immissione dei dati in Rete.

Alla luce del quadro di analisi così prospettato, a parere di chi scrive, non può che auspicarsi un intervento del legislatore, finalizzato a recepire una connotazione evolutiva dei principi tradizionali, tali da permettere di valorizzare le peculiari caratteristiche che assume il concetto di individuazione del *locus commissi delicti* nei *cybercrimes.*

INDICE BIBLIOGRAFICO

AGNINO F., Computer crime *e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*, in *Corr. merito*, 3/2009, 285.

ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Milano 1983.

AMATO G., DESTITO V.S., DEZZANI G., SANTORIELLO C., *I reati informatici*. Padova, 2010.

ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, Vol. I, Milano, 2016.

ATERNO S., MATTIUCCI M., Cloud Forensics *e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.*, 3/2013, 865.

ATERNO S., *Aspetti problematici dell'art. 615-quater c.p.*, in *Cass. pen.*, 4/2000, 535.

BALLONI A., BISI R., SETTE R., *Principi di criminologia applicata*, Padova, 2015.

BARGIS M., CONSO G., GREVI V., ET AL., *Compendio di procedura penale*, IX ed., Milano, Padova, 2018.

BELLACOSA M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni unite*, in *Dir. pen. cont.*, 2 febbraio 2015.

BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 9/1995, 1463.

BONAVOGLIA P., *Cifrari a chiave pubblica*, in *www.crittologia.eu.*

BORRUSO R., BUONOMO G., CORASANITI G., D'AIETTI, *Profili penali dell'informatica*, Milano, 1994.

BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in LUPÁRIA (a cura di), *Sistema penale e criminalità informatica, Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 Marzo 2008, n. 48)*, Milano, 2009, 181.

BRASCHI S., *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Padova, 2020.

BRODOWSKI D., FREILING F., *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, in Forschungsforum Öffentliche Sicherheit,* 4/2011, 164 ss., in *www.sicherheit-forschung.de.*

CAJANI F., COSTABILE G., MAZZARACO G., Phishing *e furto d'identità digitale: indagini informatiche e sicurezza bancaria*, Milano, 2008.

CAMPLANI F., Locus commissi delicti, *norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Arch. pen.*, 2/2020, 1° settembre 2020.

CAPONE F., *Gli attacchi di ingegneria sociale*, 8 marzo 2018, in *www.cyberlaws.it*.

CASSANO G., SCORZA G., VACIAGO G. (a cura di), *Diritto dell'Internet. Manuale operativo: casi, legislazione e giurisprudenza*, Padova, 2012.

CIRILLO P., *Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di Internet*, in *Dir. pen. cont. – Riv. Trim.*, 2/2019, 81.

CONIGLIARO S. C., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. pen. cont.*, 30 ottobre 2013.

CONSOB, *Le criptovalute: che cosa sono e quali rischi si corrono*, in *www.consob.it.*

CORRIAS LUCENTE G., *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in Il *diritto dell'informazione e dell'informatica*, 1/1987, 167.

CUOMO L., RAZZANTE R., *La nuova disciplina dei reati informatici*, Torino, 2009.

D'AGOSTINI D., D'ANGELO S., VIOLINO L., ATTANASIO A., *Diritto Penale Dell'Informatica: Dai* Computer Crime*s Alla* Digital Forensic, Forlì, 2007.

DAL CHECCO P., *Il* ransomware Wannacry *infetta PC non aggiornati: ospedali ed enti pubblici a rischio*, 12 maggio 2017, in *www.ransomware.it*.

DE MARTINO P., *Rimessa alle Sezioni Unite una questione in tema di competenza territoriale del delitto di accesso abusivo ad un sistema informatico* (Nota a Cass. Pen. Sez. I, ord. 28.10.2014, n. 52575), in *Dir. pen. cont.*, 20 gennaio 2015.

DE MARTINO P., *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico,* in *Dir. pen. cont.*, 11 maggio 2015.

DE PAOLIS M., *I reati informatici nell'ordinamento nazionale ed europeo: profili generali*, in CASSANO G., SCORZA G. (a cura di), *Diritto Dell'internet. Manuale Operativo. Casi, Legislazione, Giurisprudenza*, Padova, 2012, 509.

DEL NINNO A., *Il furto di identità*, in CENDON P. (diretto da), *Trattato breve dei nuovi danni. Figure emergenti di responsabilità*, Vol. 3, Padova, 2014, 537.

DELAGE P.J., *Brèves remarques sur l'article 113-2-1 du Code pénal*, 8 settembre 2017, in *www.actu-juridique.fr*.

DESTITO V. S., DEZZANI G., SANTORIELLO C., *Il diritto penale delle nuove tecnologie*, Padova, 2007.

DI GIORGIO C., *Melissa, virus velenoso come un serpente a sonagli*, in *la Repubblica*, 29 marzo 1999.

DI PAOLO E., Cyber crime. *Il* phishing*: prospettive di un delitto*, in *Arch. pen.*, 2/2017, 18 maggio 2017.

DI PRISCO A., *Truffe* online *e* PostePay*: quando e dove si consuma il reato?*, 29 gennaio 2018, in *www.iusinitinere.it.*

DI VIZIO F., Phishing*: le operazioni del prestaconto possono integrare il delitto di riciclaggio*, in *Web&Tech*, 27 marzo 2017.

FALLETTA P., *La diffamazione* online, in MENSI M., FALLETTA P., *Il diritto del web*, Padova, 2018, 157.

FARINA M., *Elementi di diritto dell'informatica*, Padova, 2019.

FIANDACA G., MUSCO E., *Diritto Penale Parte Speciale, I delitti contro il patrimonio*, Bologna, 2002.

FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo* jus excludendi alios, in *Dir. pen. proc*., 2005, 81.

FLOR R., Phishing, Identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente,* in *Riv. it. dir. proc. pen*., 2007, 2-3, 899.

FLOR R., *Art. 615*-ter *c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto,* in *Dir. pen. proc*., 1/2008, 106.

FLOR R., Phishing *e profili penali dell'attività illecita di "intermediazione" del cd.* financial manager, in *Dir. pen. proc.*, 1/2012, 55.

FLOR R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet,* in *Dir. pen. cont.*, 20 settembre 2012.

FLOR R., *I limiti del principio di territorialità nel* cyberspace. *Rilievi critici alla luce del recente orientamento delle Sezioni Unite,* in *Dir. pen. proc.*, 10/2015, 1291.

FLOR R., Cyber-terrorismo *e diritto penale in Italia,* in FORNASARI G., WENIN R. (a cura di), *Diritto penale e modernità. Nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Napoli, 2017, 325.

FLOR R., Cyber-criminality*: le fonti internazionali ed europee*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 98.

FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 141.

FLOR R., *Cybersecurity ed il contrasto ai* cyber-attacks *a livello europeo:* dalla CIA-Triad protection *ai più recenti sviluppi*, in *Riv. dir. Internet*, 3/2019, 453.

FLORES PRADA I., *Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia*, in *Revista Electrónica de Ciencia Penal y Criminología*, 2015, 17-21, in *www.criminet.ugr.es*.

FONDAROLI D., *Osservazioni intorno ad alcune delle norme contenute nella recente normativa italiana sui computer crimes*, in SOLA L., FONDAROLI D., *La nuova normativa in tema di criminalità informatica: alcune riflessioni*, Bologna, 1995, 19.

FREDIANI C., *Guerre di rete*, Bari, 2017.

FREDIANI, *10 cose da sapere dell'infezione* NotPetya, *e perché è più insidiosa di Wannacry*, 28 giugno 2017, in *www.lastampa.it*.

GALLUZZO F., *Competenza sulla diffamazione a mezzo Internet*, in *Dir. pen. proc.*, 10/2011, 1233.

GERCKE M., *Impact of the Lisbon Treaty on Fighting Cybercrime in the EU. The redefined role of EU and the change in approach from patchwork to comprehensiveness*, in *Cri*, 3/2010, 75.

GIBSON W., *Neuromante*, Milano, 1986.

GIORDANO M. T., *Le principali fattispecie in materia di crimini informatici*, in CASSANO G., CIMINO I.P. (a cura di), *Diritto dell'internet e delle nuove tecnologie telematiche*, Padova, 2008, 587.

GIORDANO M. T., DAL CHECCO P., *Le nuove fattispecie di reati informatici:* identity theft, phishing, in CASSANO G., SCORZA G. (a cura di), *Diritto Dell'internet. Manuale Opertivo. Casi, Legislazione, Giurisprudenza*, Padova, 2012, 587.

GORI U., *Le nuove minacce* cyber, in *Informazioni della Difesa*, Periodico dello Stato Maggiore della difesa, supplemento al n. 6/2014, 5.

GRIFFITH S., *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem, in Vanderbilt Law Review*, 1990, 454.

GULLO A., *La tela di Penelope. La riforma della diffamazione nel Testo unificato approvato alla Camera il 24 giugno 2015*, in *Dir. pen. cont. – Riv. Trim.*, 1/2016, 31.

HONNORAT F., *Extension de la territorialité des poursuites pénales en matière de cybercriminalité*, in *Réseau Eurojuris France*, 10 gennaio 2017, in *www.eurojuris.fr*.

IASELLI M., Cloud computing *per i professionisti: vantaggi e svantaggi*, in *Quot. giur.*, 20 gennaio 2016.

LANA A., I love You*, venti anni fa il primo virus informatico che ha messo il mondo in ginocchio*, in *www.corriere.it*, 4 maggio 2020.

LEVY S., Hackers*: Gli eroi della rivoluzione informatica*, Milano, 1996.

LEANDRO A., Rootkit*: cosa sono, come individuarli e come rimuoverli*, in *www.cybersecurity360.it*, 10 luglio 2019.

LOMBARDO S., Spyware*: cosa sono, come si diffondono e come eliminarli*, in *www.cybersecurity360.it*, 16 maggio 2019.

LOMBARDO S., Pharming*: cos'è, come funziona e i consigli per difendersi dalla truffa dei "siti-trappola"*, in *www.cybersecurity360.it*, 28 gennaio 2020.

LUBERTO M., *"*Sex-Torsion*" via web e minaccia a mezzo ransomware: la nuova frontiera del delitto di estorsione*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Cybercrime*, Torino, 2019, 724.

LUPÀRIA L., *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (l. 18 Marzo 2008, n. 48). I profili processuali.*, in *Dir. pen. proc.*, 6/2008, 717.

MALGIERI G., *La nuova fattispecie di "indebito utilizzo di identità digitale". Un problema interpretativo*, in *Dir. pen. cont. – Riv. Trim.*, 2/2015, 143.

MANICCIA A., *Gli incerti "confini" del principio di territorialità* (nota a Cass. Pen. Sez. VI, 21.09.2017), n. 56953, in *Cass. pen.*, 11/2008, 3717.

MANTOVANI F., *Diritto penale parte speciale I*, "*Delitti contro la persona*", Padova, 2008.

MANTOVANI F., *Diritto penale, parte generale*, Padova, 2017.

MARINELLI A., voce "*Internet e web*", in *Enciclopedia Treccani online, www.treccani.it*.

MARINI G., *Condotte in alterazione del reale aventi ad oggetto nastri ed altri supporti magnetici e diritto penale,* in *Riv. it. dir. proc. pen.*, 2/1986, 381.

MARINI G., *Delitti contro la persona*, II ed., Torino, 1996.

MARINUCCI G., DOLCINI E., *Costituzione e politica dei beni giuridici*, in *Riv. it. dir. proc. pen*., 2/1994, 333.

MARINUCCI G., DOLCINI E., *Manuale di Diritto Penale. Parte Generale*, Milano, 2017.

MARKOFF J., *Worm Infects Millions of Computers Worldwide*, in *The New York Times*, 22 gennaio 2009.

MARTINO L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica&Società*, 1/2018, 61.

MASI A., *Frodi informatiche e attività bancaria,* in *Riv. pen. econ.,* 4/1995, 427.

MENSI M., *La sicurezza cibernetica*, in MENSI M., FALLETTA P., *Il diritto del web*, Padova, 2018, 281.

MEZZALAMA M., LIOY A., METWALLEY H., *Anatomia del* malware, in *Mondo Digitale*, 47/2013, settembre 2013.

MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ.*, 1992, 365.

MIRTI M., *La disciplina giuridica del* cyberspace*. Una panoramica sulle problematiche attuali e le principali linee evolutive*, in *Opinio Juris*, 23 novembre 2016.

MUCCIARELLI F., *Commento all'art. 10 della legge n. 547 del 1993*, in *Leg. Pen.*, 1996, 136.

NERI G., *Criminologia e reati informatici: profili di diritto penale dell'economia*, Roma, Bari, 2014.

PAGLIARO A., voce Tempus commissi delicti, in *Enc. dir.*, XLIV, 1992, Milano, 82.

PAGLIARO A., *Principi di diritto penale, Parte speciale, Delitti contro il patrimonio*, Milano, 2003.

PALMAS F., *Spazio cibernetico: atout e vulnerabilità di una nuova dimensione strategica*, in *Rivista di Studi Politici Internaz*ionali, 4/2008, Vol. 75, 534.

PANADA F., UNTERBRINK H. (a cura di), Ransomware*: un flagello che prende di mira privati e aziende*, in *Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia*, in *www.clusit.it.*, 2017.

PANATTONI B., Compliance, cybersecurity *e sicurezza dei dati personali*, Assago, 2020.

PECORELLA C., *Diritto penale dell'informatica*, Ristampa con aggiornamento, Padova, 2006.

PECORELLA C., *Truffe* on-line*: momento consumativo e competenza territoriale,* in *Dir. pen. cont.*, 10 maggio 2012.

PECORELLA C., *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico* (nota a Cass. Pen., Sez. I, sent. 27.05.2013 n. 40303), in *Dir. pen. cont.*, 11 ottobre 2013.

PEREIRA B., *La lutte contre la cybercriminalité: de l'abondance de la norme à sa perfectibilité*, in *Revue internationale de droit économique*, 2016, 3, via *www.cairn.info.*

PERRI P., *Lo* smishing *e il* vishing*, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. Internet*, 3/2008, 261.

PETRINI D., *La responsabilità penale per i reati via internet*, Napoli, 2004.

PICA G., *Diritto penale delle tecnologie informatiche*, Torino, 1999.

PICA G., Computer crimes *e uso fraudolento delle nuove tecnologie*, Seminario di studi, Roma, 15 dicembre 2000.

PICOTTI L., *Studi di diritto penale dell'informatica,* Verona, 1992.

PICOTTI L., voce *Reati informatici*, in *Enc. giur.*, Agg., VIII, Roma, 2000, 1.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21.

PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. Internet*, 2/2005, 189.

PICOTTI L., *Ratifica della Convenzione* Cybercrime *e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. Internet*, 5/2008, 437.

PICOTTI L., *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (l. 18 Marzo 2008, n. 48). Profili di diritto penale sostanziale,* in *Dir. pen. proc.*, 6/2008, 700.

PICOTTI L., *Reati informatici, riservatezza e identità digitale*, report presentato al VII Convegno Nazionale dei Professori di Diritto Penale sul tema "*Il diritto penale tra recenti modifiche e progetti di riforma*", Torino, 9-10.11.2018.

PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (diretto da), *Cybercrime*, Torino, 2019, 35.

PICOTTI L., con il contributo di SALVADORI I. e FLOR R., *Reati informatici, riservatezza, identità digitale*, Convegno Nazionale dell'Associazione Italiana dei Professori di Diritto Penale, 2019.

RESTA F., Cybercrime *e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. Merito*, 9/2008, 2147.

RIJTANO R., Keylogger*: cos'è, come eliminarlo, i migliori per Windows, Mac e cellulare*, 24 maggio 2018, in *www.cybersecurity360.it.*

RIJTANO R., SBARAGLIA G., WannaCry*, cos'è, come funziona e come difendersi dal ransomware che ha fatto piangere il mondo*, 28 giugno 2018, in *www.cybersecurity360.it.*

RUGGIERO F. P., *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002, 254.

SARZANA DI S. IPPOLITO C., *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. proc.*, 4/2002, 509.

SARZANA DI S. IPPOLITO C., *Informatica, Internet e diritto penale.* (3. Riv., corretta ampliata ed.), Milano, 2010.

SANTORO F., *Il progetto internazionale "No more ransom" alla luce dell'attacco* WannaCry, in *Web&Tech Sicurezza informatica,* 1° giugno 2017.

SCARCELLA A., *Il* phishing *è punibile come frode informatica,* in commento alla sentenza Cass. pen., Sez. II, 24.10.2018, n. 48553, *in Quot. Giur.*, 13 novembre 2018.

SEMINARA S., *La pirateria su Internet e diritto penale,* in *Riv. trim. dir. pen. ec*., 1-2/1997, 71.

SEMINARA S., Locus commissi delicti, *giurisdizione e competenza nel cyberspazio,* relazione al Convegno "Presi nella rete – Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012, reperibile su www.informaticagiuridica.unipv.it/convegni/2012/SEMINARA.

SEMINARA S., voce *Internet (diritto penale)*, in *Enc. dir.*, Annali VII, Milano, 2014, 567.

SEVERINO P., *Le leve e le sfide per il rilancio del paese. Le frontiere della sicurezza informatica e prevenzione del Cybercrime*, Cernobbio, 2017.

SEVERINO P., *Standard globali in difesa della trasformazione digitale*, in *www.ilsole24ore.com*, 29 marzo 2019.

SINISCALCO M., *Locus commissi delicti*, in *Enc. dir.*, 1974, XXIV, Milano, 1051.

SILVETTI V., *I crimini informatici più frequenti degli ultimi anni: tabella riepilogativa e profili giuridici*, in *Quot. giur.*, 4 ottobre 2019.

STALLA G., *L'accesso abusivo ad un sistema informatico o telematico*, in *www.penale.it,* 2003.

TARSITANO P., Ginp, il trojan Android *che finge di segnalare i contagiati da Coronavirus*, 25 marzo 2020, in *www.cybersecurity360.it*.

TESTAGUZZA A., Digital forensic. *Informatica giuridica e processo penale*, Padova, 2014.

TRUNFIO E., CRISAFI M., *Il phishing*, in CENDON P. (diretto da), *Trattato breve dei nuovi danni. Figure emergenti di responsabilità*, Vol. 3, Padova, 2014, 515.

VIACIAGO G., GIORDANO M. T., *La qualificazione giuridica del* Phishing *in una delle sue prime applicazioni giurisprudenziali*, in *Dir. Internet*, 1/2007, 62.

VIGNERI F., *I nuovi scenari criminali: introduzione al fenomeno del* cybercrime, in *Salvis Juribus*, 17 dicembre 2018.

VINCIGUERRA S., *Diritto penale italiano. Vol. I. Concetto, fonti, validità, interpretazione*, Padova, 1999.

VULPIANI D., *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in *Riv. di criminologia, vittimologia e sicurezza*, 2007, I, (1), 46.

ZENO ZENCOVICH V., *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, 1/2003, 89.

INDICE DELLA GIURISPRUDENZA

Cass. Pen., Sez. V, 16.10.1972, n.811.

Corte Costituzionale, 25.07.1994, n. 341, in *Giur. cost.*, 1994.

Cass. Pen., Sez. V, 28.02.1995, n.3247, in *www.dejure.it.*

Cass. Pen., Sez. V, 02.07.1998, n. 4389, in *www.dejure.it.*

Cass. Pen., Sez. Un., 16.12.1998, in *Giur. it.*, 2000.

Cass. Pen., 04.10.1999, n. 3065, *www.dejure.it.*

Cass. Pen., Sez. VI, 04.10.1999, n. 3067 in *Cass. Pen.*, 11/2000, 2990.

Cass. Pen., Sez. I, 13.01.2000, n. 269, in *www.dejure.it.*

Cass. Pen., Sez. V, 17.11.2000, n.4741, in *www.dejure.it.*

Cass. Pen., Sez. V, 27.06.2002, n. 24847, in *www.dejure.it.*

Cass. Pen. Sez. V, 20.05.2003, n. 22319, in *www.avvocato.it.*

Cass. Pen., Sez. V, 19.11.2003, n. 44362, in *www.avvocato.it.*

Cass. Pen., Sez. V, 24.11.2003, n. 4576, via *www.ius-web.it.*

Cass. Pen., Sez. II, 17.12.2004, n. 5688, in *www.dejure.it.*

Cass. Pen., Sez. V, 19.05.2005, n. 4011, in *www.dejure.it.*

Corte costituzionale, 5.04.2006, n. 168, in *www.giurcost.it.*

Cass. Pen., Sez. V, 21.06.2006, n. 25875, in *www.penale.it.*

Cass. Pen. Sez. V, 31.07.2007, n. 31135, in *www.avvocato.it.*

Cass. Pen. Sez. V, 14.12.2007, n. 46674, in *www.pluris-cedam.utetgiuridica.it.*

Cass. Pen., Sez. II, 21.02.2008, n. 10085, in *www.exeo.it.*

Cass. Pen., Sez. V, 04.04.2008, n. 16262, in *www.penale.it.*

Cass. Pen., Sez. V, 01.07.2008, n. 31392, in *www.diritto.it.*

Trib. Milano 19.10.2008, in *Corr. merito*, 2009, 3, 285.

Cass. Pen., Sez. I, 5.02.2009, n. 8513, in *www.penale.it.*

Corte Appello, Torino del 3 luglio 2009, in *www.dejure.it.*

Cass. Pen., Sez. Un., 29.09.2009, n. 21661, in *www.aduc.it.*

Cass. Pen., Sez. II, 12.11.2010, n. 44929, in *www.exeo.it.*

Cass. Pen., Sez. I, 21.12.2010, n. 2739, in *www.dejure.it.*

Cass. Pen., Sez. I, 15.03.2011, n. 16307, in *www.dejure.it.*

Cass. Pen, Sez. II, 08.04.2011, dep. 21.04.2011, n. 15834, in *www.dejure.it.*

Cass. Pen., Sez II, 15.04.2011, n. 17748, in *www.pluris-cedam.utetgiuridica.it.*

Corte di Giustizia UE, 25 ottobre 2011 (C-509/09, C161-10), in *www.pluris-cedam.utetgiuridica.it*.

Cass. Pen. Sez. VI, 24.04.2012, n. 16115, in *www.pluris-cedam.utetgiuridica.it.*

Cass. Pen., Sez. V,17.05.2012, n. 30329, in *www.dejure.it.*

Cass. Pen., Sez. III, 24.05.2012, n. 23798, in *www.dejure.it.*

Cass. Pen. Sez. II, 04.07.2012, n. 26613, in *www.dejure.it.*

Cass. Pen., Sez. I, sent. 27.05.2013 n. 40303, in *www.dirittopenalecontemporaneo.it.*

Cass. Pen. Sez. II, 26.11.2013, n. 47021, in *www.dejure.it*.

Cass. Pen., Sez. V, 12.12.2013, n. 13350, in *www.penalistiassociati.net.*

Cass. Pen., Sez. I, 22.01.2014, n. 16712 in *www.penale.it.*

Cass. Pen., Sez. I, 07.10.2014, n. 46101, in *www.dejure.it*.

Cass. Pen., Sez. I, ord. 28.10.2014, n. 52575.

Cass. Pen., sez. II, 04.11.2014 n. 7749, in *www.dejure.it.*

Cass. Pen., Sez. V, 18.12.2014, n. 10121, in *www.pluris-cedam.utetgiuridica.it.*

Cass., Sez. Un., sent. 26.03. 2015 n. 17325, in *www.pluris-cedam.utetgiuridica.it*.

Cass. Pen., Sez. II, 13.10.2015 n. 50140, in *www.pluris-cedam.utetgiuridica.it.*

Cass. Pen., Sez. VI, 04.11.2015, n. 1333, in *www.dejure.it*.

Cass. pen., Sez. V 18.12.2015, n.4059, in *www.pluris-cedam.utetgiuridica.it*.

Cass. Pen. Sez. VI, 12.02.2016, n. 11442, in *www.pluris-cedam.utetgiuridica.it.*

Cass. Pen., Sez. V, 25.02.2016, n. 12536, in *www.giurisprudenzapenale.com*.

Cass. Pen., Sez. II, 9.06.2016, n. 41435, in *www.studiolegaleramelli.it*.

Cass. Pen., Sez. V, 14.07.2016, n. 54946, in *www.giurisprudenzapenale.com*.

Cass. Pen., sez. II, 20.10.2016 n. 48027, in *www.penale.it.*

Cass. Pen., Sez. I, 02.12.2016, dep. 02.01.2017, n. 50, in *www.dejure.it*.

Cass. Pen., Sez. II, 14.02.2017, n. 8913, in *www.dejure.it.*

Cass. Pen., Sez. V, 22.02.2017, n. 8482, in *www.dejure.it*.

Cass. Pen., Sez. II, 1.03.2017, n. 10060, in *www.pluris-cedam.utetgiuridica.it.*

Cass. Pen., Sez. V, 06.06.2017, n. 52572, in *www.dejure.it*.

Cass. Pen, Sez. Un., 08.09.2017, n. 41210, *www.giurisprudenzapenale.it*.

Cass. Pen. Sez. VI, 21.09.2017, n.56953, in *www.dejure.it.*

Cass. Pen., Sez. V,12.01.2018, n. 17923, in *www.dejure.it.*

Cass. Pen., Sez. V, 23.10.2018, n. 1275, in *www.archiviodpc.dirittopenaleuomo.org*.

Cass. Pen., Sez. II, 24.10.2018, n. 48553, in *www.pluris-cedam.utetgiuridica.it.*

Cass. Pen., Sez. V, 11.02.2019, n. 5692, in *www.dejure.it.*

Cass. Pen, Sez. V, 11.03.2019, n. 15665, in *www.dejure.it.*

Cass. Pen., Sez. II, 20.05.2019, n. 21987, in *www.pluris-cedam.utetgiuridica.it*.

Cass. Pen. Sez. II, 18.09.2019, n. 46652, in www.pluris-cedam.utetgiuridica.it.

Cass. Pen., Sez. II, 30.10.2019, n. 50395, in *www.dejure.it.*

Cass. Pen., Sez. II, 05.02.2020, n. 10354, in *www.dejure.it.*

SITOGRAFIA

www.actu-juridique.fr

www.aduc.it

www.aipdp.it

www.archiviodpc.dirittopenaleuomo.org

www.archiviopenale.it

www.avvocato.it

www.cairn.info

www.canestrinilex.it

www.cisco.com

www.clusit.it

www.consob.it

www.corriere.it

www.criminet.ugr.es

www.cyberlaws.it

www.cybersecurity360.it

www.dejure.it

www.diritto.it

www.dirittopenalecontemporaneo.it

www.eur-lex.europa.eu

www.eurojuris.fr

www.exeo.it

www.giurcost.it

www.giurisprudenzapenale.com

www.informaticagiuridica.unipv.it/convegni/2012/SEMINARA

www.ilsole24ore.com

www.iusexplorer.it

www.iusinitinere.it

www.ius-web.it

www.lastampa.it

www.legifrance.gouv.fr

www.niccs.us-cert.gov

www.nomoreransom.org

www.penale.it

www.penalistiassociati.net

www.pluris-cedam.utetgiuridica.it

www.ransomware.it

www.sicherheit-forschung.de

www.studiolegaleramelli

www.treccani.it