DIPARTIMENTO DI GIURISPRUDENZA

CATTEDRA DI DIRITTO PENALE 2

IL SISTEMA DEI DELITTI DI DANNEGGIAMENTO INFORMATICO:

EVOLUZIONE, ANALISI E PRASSI APPLICATIVA

Relatore
Chiar.mo Prof. Antonio Gullo

Candidato
Francesco Pioppi
Matr. 142903

Correlatore
Chiar.ma Prof.ssa Maria Lucia Antonietta Di Bitonto

Anno Accademico 2021-2022

INDICE

INTRODUZIONE III

CAPITOLO I: INQUADRAMENTO ED EVOLUZIONE NORMATIVA

1. *Cybersecurity* e *cyberlaw*: introduzione alla disciplina 1

2. Tecniche di *cyber-attacks* e reati informatici: questioni definitorie 10

3. Evoluzione della disciplina 20

3.1. Consiglio d'Europa: la raccomandazione 9 settembre 1989 n. R (89) 9 e la Convenzione di Budapest (2001) 22

3.2. Unione Europea: Decisione Quadro 2005/221/GAI e Direttiva UE 2013/40 29

3.3. Disciplina nazionale: dalla prassi giurisprudenziale all'attuale normativa: Legge 3 dicembre 1993 n. 547 e Legge 18 marzo 2008 n. 48 35

CAPITOLO II: DANNEGGIAMENTO DI DATI E SISTEMI INFORMATICI PRIVATI

1. Le nuove disposizioni dei delitti contro l'integrità di dati e sistemi informatici "privati": gli artt. 635-*bis* e 635-*quater* c.p. 41

2. Soggetto attivo e bene giuridico tutelato: tesi tradizionale e tesi moderna 44

3. Gli oggetti materiali: dati, informazioni e programmi informatici 46

3.1. ... (segue) I sistemi informatici e telematici 49

3.2. ... (segue) Il nuovo concetto di "altruità" 51

4. Le condotte incriminate: definizioni e contenuto 53

4.1. Gli eventi dell'art. 635-*quater* c.p. 58

4.2. Qualificazione delle fattispecie e questioni interpretative 60

4.3. Il *locus commissi delicti* 63

5. L'elemento soggettivo, il momento consumativo e il tentativo 68

6. Le circostanze aggravanti speciali 68

7. Il trattamento sanzionatorio e la procedibilità 72

8. Il rapporto tra reati 74

CAPITOLO III: DANNEGGIAMENTO DI DATI E SISTEMI INFORMATICI PUBBLICI E DI PUBBLICA UTILITÀ

1. Le nuove disposizioni dei delitti contro l'integrità di dati e sistemi informatici pubblici e di pubblica utilità gli artt. 635-*ter* e 635-*quinquies* c.p. 78

2. Soggetto attivo e bene giuridico tutelato: tre possibili orientamenti 81

3. Gli oggetti materiali e la peculiare "qualificabilità" pubblica 84

4. Le condotte incriminate e struttura dei delitti 88

4.1. I delitti a consumazione anticipata e il principio di offensività. Brevi cenni 91

5. L'elemento soggettivo: il problema della compatibilità tra tentativo e dolo eventuale 98

6. Gli eventi "aggravatori" e le altre circostanze aggravanti specifiche 102

7. Il trattamento sanzionatorio e la procedibilità 108

8. Il rapporto tra reati 110

CAPITOLO IV: LA TUTELA DELL'INTEGRITÀ DEI DATI E DEI SISTEMI INFORMATICI QUALE IMPRESCINDIBILE ESIGENZA DEGLI ENTI SOVRANAZIONALI, NAZIONALI E PRIVATI

1. Cyberterrorismo: definizione e contrasto sovranazionale 113

1.1. Cyberterrorismo e diritto penale nazionale 122

2. Reati informatici e responsabilità degli enti: D.Lgs. 231/2001 127

2.1. Misure di prevenzione e *compliance* aziendale 133

3. Tutela della *Privacy*: Regolamento (UE) 679/2016 (GDPR) 140

3.1. *Data breach* e reati informatici 147

CONCLUSIONI 153

BIBLIOGRAFIA 157

INDICE DELLE SENTENZE 168

INTRODUZIONE

Lo sviluppo delle tecnologie informatiche e telematiche ha determinato profondi cambiamenti nel tessuto sociale e nelle dinamiche del rapporto umano. Attraverso la sempre più estesa applicazione ad ogni settore economico e sociale, l'accesso e l'uso di tali strumenti è divenuto, da specifica competenza professionale di pochi, ad indispensabile conoscenza di base alla portata di chiunque. L'era informatica, anche e sopratutto attraverso la creazione e la diffusione del *web*, ha ridisegnato la fisionomia dei territori, abbattendo i confini fisici, a favore di uno spazio virtuale in continua espansione, che consente la delocalizzazione delle risorse e la loro raggiungibilità, da parte dell'utente, da ogni luogo e da qualsiasi distanza. In una siffatta realtà le ambizioni e le istanze dell'essere umano trovano terreno fertile e rapide risposte.

Le trasformazioni sociali, che qui ci si limita ad introdurre, hanno avuto e conservano l'evidente portata di una rivoluzione copernicana, favorendo e accelerando il passaggio da un modo diretto e analogico di gestire i fatti, gli oggetti ed i processi, a un modo discontinuo e indiretto, mediato dalla logica che governa i nuovi strumenti, vale a dire dalla logica digitale. Già nel lontano 1981 il "padre dell'informatica giuridica", Vittorio Frosini, si esprimeva affermando che «come la rivoluzione industriale moltiplicò l'energia fisica dell'uomo e ne diminuì la fatica, abituando l'uomo a convivere con le macchine […] così la rivoluzione informatica allarga e potenzia le capacità della mente umana, obbligando la nostra intelligenza ad avvalersi di una protesi intellettuale»[1].

È vero che la tecnologia e l'informatizzazione hanno aperto la porta a nuovi spazi di applicazione per i pensieri e le attività dell'uomo, rendendo disponibili una serie di strumenti volti alla creazione di nuove opportunità in ogni campo dell'agire. Parimenti, però, si deve riconoscere che tali strumenti hanno favorito la creazione di nuove e varie possibilità criminose; anche la mente dei soggetti criminali, infatti, al pari di ogni ambito dello scibile umano, ha potuto sfruttare i nuovi mezzi informatici, trovando modi e spazi innovativi per "sfogare" inediti comportamenti illeciti.

[1] FELLUGA, *I Computer crimes: definizioni ed elementi principali*, in *Tigor: rivista di scienze della comunicazione e di argomentazione giuridica*, IV, 2012, Trieste, 27.

La dottrina e la giurisprudenza, nazionale e sovranazionale, che rappresentano il primo fronte d'impatto di ogni mutamento nei comportamenti, nelle relazioni e nelle condizioni sociali, rilevanti per l'applicazione del diritto, da meno di mezzo secolo, hanno rivolto l'attenzione anche ai rapporti tra il diritto penale e la c.d. ICT ("tecnologia dell'informazione e della comunicazione"). Allo stesso modo, tali cambiamenti hanno interessato i più autorevoli organismi internazionali e, in un secondo momento, anche i legislatori di quasi tutti i paesi occidentali, che sono progressivamente intervenuti sulla questione, spesso in modo disorganico, a seconda delle diverse urgenze o condizioni politiche se non anche dello sviluppo tecnologico.

Questi mutamenti, che in una prima fase avevano portato i settori della dottrina penale tradizionalista a mostrarsi indifferenti, se non apertamente scettici, circa la rilevanza ed autonomia di questo nuovo ambito giuridico, oggi fanno emergere un esteso riconoscimento del merito di, non solo specifiche analisi ermeneutiche, ma anche un'adeguata elaborazione teorica e sistematica.

Proiettati verso il suddetto scopo bisognerebbe, in primo luogo, superare un approccio c.d. "minimalista", che individua nella "rivoluzione cibernetica" un mero ramo "speciale" del diritto penale, per adottarne uno che si dimostri, invece, consapevole di una prospettiva necessariamente nuova e diversa, riguardante, cioè, l'intero sistema penale. In altre parole, a quella che si definisce "rivoluzione informatica" si dovrebbe riconoscere *tout court* un'importanza strutturale per l'evoluzione del diritto universalmente considerato.

Operando un'estrema schematizzazione, si può affermare che il rapporto tra le moderne novità tecnologiche ed informatiche ed il diritto penale stimola il costante adeguamento del diritto, affinché questo abbracci i nuovi fenomeni *cyber* e perpetui la capacità regolatrice, ricorrendo a tutti gli strumenti dogmatici di cui dispone, dall'interpretazione evolutiva, passando per «l'applicazione analogica, seppur indicibile e necessariamente mascherata nella materia penale»[2], fino alla creazione di nuove norme ovvero di nuove categorie concettuali. D'altra parte, al pari di ogni realtà strutturale che condizioni altre sovrastrutture, la rivoluzione cibernetica ridetermina il suo stesso rapporto con il diritto, modificandone

[2] PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, Milano, 2019.

profondamente le funzioni e, sopratutto, il modo di operare, giacché la tecnologia informatica sembrerebbe in grado di porsi in concorrenza con la primaria funzione normativa − come brillantemente segnalato dalla dottrina internazionale[3].

È esattamente in questo contesto che ci si muoverà nel corso delle pagine che seguiranno. L'analisi che avrà luogo nel presente elaborato avrà ad oggetto il c.d. "microsistema dei delitti di danneggiamento informatico", un complesso di quattro norme contenute nel codice penale − gli artt. 635 *bis*, *ter*, *quater* e *quinquies* c.p. − che positivizzano altrettante fattispecie criminali delittuose. Non si vuole, però, offrire una sterile analisi normativa, quanto piuttosto dipingere − senza pretesa di esaustività − un quadro d'insieme della disciplina che i delitti in parola rappresentano. In questo modo si vogliono cogliere appieno le difficoltà e le criticità che scaturiscono dall'integrazione, ed il conseguente e reciproco condizionamento, tra la realtà *cyber* ed il diritto penale, individuando le ragioni poste alla base delle scelte di politica criminale effettuate dal legislatore, per essere poi in grado di comprendere e valutare la concreta attuazione delle stesse.

A tal fine, l'analisi trarrà le mosse da una necessaria panoramica generale ed introduttiva della materia della *Cyber security* e della sua rispettiva disciplina normativa − vale a dire la c.d. *Cyber Security law*, ovvero anche solo *cyber law* − delineandone i caratteri essenziali, i principi e le criticità ermeneutiche. Nella prima parte del primo capitolo, infatti, si tenterà di ricostruire una − quanto più possibile − completa definizione della nozione stessa di *Cyber security*, attingendo ai maggiori contributi della dottrina nazionale ed internazionale; nel perseguire tale obiettivo non ci si potrà esimere dal volgere l'attenzione al principio cardine che ha condizionato le legislazioni nazionali e sovranazionali nel fronteggiare i rischi derivanti dalla "rivoluzione informatica", vale a dire l'*accountability*, le cui dirette conseguenze pratiche saranno oggetto di valutazione nell'ultimo capitolo. Parimenti, in funzione della suddetta panoramica generale, si analizzeranno le diverse posizioni dottrinali, nonché i vari orientamenti della giurisprudenza, relativamente alla identificabilità di una posizione di garanzia degli *Internet Service Providers*, tema che ha alimentato un acceso dibattito nella comunità giuridica nazionale.

[3] LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, *in Harvard Law Review*, 1999, 113. Nel presente elaborato verrà ripreso il contributo dell'autore; si veda *infra* Cap. I, par. 1.

Nel prosieguo dell'elaborato, pur rimanendo in una prospettiva introduttiva, si circoscriverà la ricerca alle più note forme di attacchi informatici, effettuando una breve e sintetica enucleazione delle stesse, attraverso l'ampio sfruttamento delle elaborazioni della comunità scientifica informatica, accompagnandola ad una ricostruzione delle possibili definizioni e categorizzazioni delle fattispecie penali volte alla repressione delle prime − i c.d. *ciber crimes*. In questo modo sarà possibile cogliere, già in apertura dell'elaborato, l'archetipo del rapporto, estremamente condizionante, tra la realtà informatica ed il diritto penale − in questo specifico caso − sostanziale, poiché, come si sottolineerà, la difficoltà intrinseca di ricostruire una completa nozione di reato informatico deriva proprio dalla ampia eterogeneità dei fenomeni criminali a cui questi si rivolgono.

Il primo capitolo si concluderà, poi, con una dettagliata indagine dell'*iter* normativo che ha portato all'adozione dell'attuale disciplina penale nazionale relativa ai *cyber crimes, ivi* incluso il "microsistema dei delitti di danneggiamento informatico". Tale ricostruzione, oltre che seguire l'ordinario criterio cronologico dei provvedimenti adottati, sarà suddivisa sulla base delle diverse autorità, internazionali o nazionale, che li hanno emananti; dapprima il Consiglio d'Europa con la raccomandazione R(89) 9 del 1989 e la Convenzione di Budapest del 2001, proseguendo per l'Unione Europea mediante la Decisione Quadro 2005/221/GAI e la direttiva UE 2013/40, concludendo con il legislatore nazionale, analizzando i due provvedimenti principali in materia di reati informatici, vale a dire la legge 3 dicembre 1993 n. 547 e la legge 18 marzo 2008 n.48. Le ragioni di suddetta scelta metodologica risiedono nell'evidente influenza, diretta o mediata, dei provvedimenti internazionali sulla legislazione nazionale.

I due capitoli centrali del presente lavoro saranno dedicati alla approfondita analisi delle fattispecie codificate dagli artt. 635 *bis*, *ter*, *quater*, e *quinquies* c.p.; si seguirà un metodo di trattazione "tradizionale", seppur prevedendo una suddivisione metodologica delle quattro norme sulla base di elementi qualificanti che verranno analizzati in seguito. Rispetto a tale trattazione, sarà d'obbligo segnalare e − laddove risulti possibile − sciogliere delicate e controverse questioni ermeneutiche, le quali trascenderanno il sistema di delitti di

danneggiamento informatico, potendosi estendere funzionalmente all'intera categoria dei reati informatici. Ci si soffermerà, in modo particolare, sulle criticità derivanti dall'identificazione dei bei giuridici tutelati dalle norme in esame; operando una sintesi della questione, si individuerà come la dottrina è ancora oggi divisa sul possibile riconoscimento di una nuova categoria di beni giuridici c.d. informatici, meritevoli di tutela, elaborando, di conseguenza, diversi possibili profili ermeneutici. Allo stesso modo si tratterà un tema di assoluta rilevanza per l'intera categoria dei *cyber crimes*: la determinazione del *locus commissi delicti*, reso particolarmente arduo dalle peculiarità strutturali degli stessi; sul punto si riporteranno anche i diversi orientamenti della Corte di Cassazione, la quale ha avuto modo di pronunciarsi sull'argomento in diverse occasioni.

Con particolare riferimento ai delitti di cui agli artt. 635 *ter* e *quinquies*, a cui sarà interamente dedicato il terzo capitolo dell'elaborato, si dovranno prendere ad oggetto anche le numerose problematicità derivanti dalla scelta di politica criminale del legislatore − ampiamente dibattuta dalla dottrina − di mutuare la struttura delle norme in parola a quella dei delitti a consumazione anticipata; si osserverà come tale soluzione abbia determinato l'insorgere della necessità di interventi chiarificatori da parte degli interpreti, nonché come abbia alimentato nella dottrina aspri dibattiti che esulano dalla selettiva categoria dei reati informatici, essendo propri della generale disciplina di diritto penale sostanziale.

Per completare il quadro, l'ultimo capitolo verrà dedicato alla valutazione dell'attuazione della politica di contrasto alla criminalità informatica, operata anche attraverso la repressione delle condotte criminose mediante il ricorso alle fattispecie penali previste dall'ordinamento. In particolare, si prenderanno ad oggetto tre diverse discipline settoriali, rispetto alle quali, premessa una breve panoramica sulla normativa, si cercherà di individuare i metodi attraverso i quali la regolamentazione, propria di ambiti diversi rispetto alla specifica materia dei *cyber crimes*, si integra con la specifica disciplina dei reati informatici. Tali materie riguarderanno: in primo luogo, la repressione dei fenomeni terroristici perpetrati attraverso lo sfruttamento di strumenti informatici − il c.d. "*cyber* terrorismo" – in secondo luogo, la disciplina della responsabilità degli enti dipendente da reato − *ex* d.lgs. 231/2001 – ed infine, la normativa riguardante la

tutela del diritto alla riservatezza e sulla protezione dei dati personali, disciplinata dal regolamento generale sulla protezione dei dati (reg. UE n. 679/2016).

L'obbiettivo ultimo dell'elaborato è, quindi, quello di fornire una visione d'insieme delle premesse teoriche, dell'elaborazione normativa e della concreta attuazione della tutela operata dal legislatore, specificamente, attraverso le norme contenute nel c.d. "microsistema dei delitti di danneggiamento informatico" e, più in generale, mediante l'ampia materia della *Cyber security*, nelle sue declinazioni legate indissolubilmente al diritto penale.

CAPITOLO I

INQUADRAMENTO ED EVOLUZIONE NORMATIVA

1. *Cybersecurity* e *cyberlaw*: introduzione alla disciplina

Nel complesso panorama della modernità la *Cyber Security* può essere considerata come la risposta degli ordinamenti giuridici alla progressiva, e ad oggi pervasiva, digitalizzazione[1] e informatizzazione[2] della vita della società. A più livelli e mediante diversi strumenti, gli enti nazionali, sovranazionali e privati si interfacciano quotidianamente con i rischi dell'universo informatico. La continua dialettica tra società e diritto, in ragione della quale il secondo trasforma in disposizioni le istanze e le esigenze della prima, ha determinato la nascita e lo sviluppo di una nuova branca della giurisprudenza.

Lo spazio virtuale ha caratteristiche peculiari che renderebbero inefficace una disciplina ancorata alle categorie dogmatiche tradizionali o che, più precisamente, vanificherebbero l'efficacia general-preventiva tipica della sanzione penale. Già alla fine dello scorso millennio, si era giunti a individuare l'avvenuto passaggio dalla *rule of law* alla *rule of code*[3]: nell'universo digitale non è più la norma a consentire o disciplinare i comportamenti ma il limite diventa solo il "tecnicamente possibile". In questo panorama, è quindi necessario che anche il diritto − in particolare, il diritto penale − si adatti alle nuove realtà nelle quali si trova ad operare. L'applicazione degli istituti giuridici tradizionali si rivelerebbe inadeguata rispetto alle richieste di sicurezza digitale che, al di là della specificità della materia, si estendono non solo nella direzione della prevenzione dei *cyber attack* ma anche in quella successiva di intervento.

La *cyberlaw*, o con maggiore precisione la *Cyber Security law*, è quindi un fenomeno di diritto che pianta le sue radici nella trasversalità dei temi e delle

[1] Voce DIGITALIZZAZIONE in *Enciclopedia Treccani online, «conversione di grandezze analogiche in informazioni digitali»*.
[2] Voce INFORMATIZZAZIONE in *Enciclopedia Treccani online, «L'introduzione dei sistemi informatici in uno o più settori di attività»*.
[3] Sul punto v. LESSIG, *The Law of the Horse: what cyberlaw might teach* cit., 113. «*code regulates behavior in cyberspace. The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave. [...] They are experienced as conditions on one's access to areas of cyberspace*».

competenze, rendendosi necessariamente flessibile rispetto agli interessi coinvolti e dinamico rispetto ai cambiamenti della realtà digitale[4].

Si intuisce, quindi, come fornire una definizione omnicomprensiva della materia sia un'operazione quantomeno difficoltosa. Di recente, parte della comunità scientifica e giuridica ha definito la *Cybersecurity* come «quella pratica che consente a una entità (ad esempio, organizzazione, cittadino, nazione ecc.) la protezione dei propri *asset* fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal *cyber space*»[5]. Il contributo fornito dalla predetta definizione risiede nella sua capacità di porre in rilievo non solo agli aspetti tecnico-economici, ma soprattutto i diversi profili significativi per il diritto penale della sicurezza informatica. Sono dunque identificati, in via ancora preliminare, i beni giuridici verso i quali è indirizzata la tutela della *Cybersecurity*, vale a dire il patrimonio («*asset* fisici») e l'integrità dei dati («confidenzialità, integrità e disponibilità delle proprie informazioni»)[6].

In secondo luogo, la definizione in commento rivela il ruolo centrale del c.d. *cyber-risck*[7] che si pone in rapporto "genetico" rispetto alla disciplina della sicurezza informatica. In altri termini, gli strumenti di tutela degli interessi sono individuati alla stregua dei rischi provenienti dallo spazio virtuale.

Nel sistema della *Cybersecurity* il rischio legato al trattamento delle informazioni dei sistemi informatici assume una funzione focale non solo

---

[4] Per approfondimenti sul tema v. LIVI, ONORATI, *La "Cybersecurity Law"* in *Telsy*, *https://www.telsy.com/it/la-cybersecurity-law/* In particolare gli Autori rilevano come «la *cyber security law* sia proprio rappresentativa di un diritto che si sviluppa e si evolve all'evolversi della società, captando le istanze economico-sociali di coloro che vi operano e traducendole in disposizioni atte a regolare rapporti ed attività. In ragione della natura sperimentale e all'avanguardia dei sistemi digitali, l'attivo coinvolgimento di legali specializzati in *cybersecurity* risponde alle crescenti richieste del mercato che cerca figure in grado di coniugare le competenze giuridiche con la conoscenza delle tecnologie digitali. Per raggiungere questi obiettivi, è necessario puntare alla multidisciplinarietà della professione forense poiché, oltre alla classica formazione giuridica, va aggiunta anche quella di natura più strettamente tecnologica».

[5] BALDONI, MONTANARI (a cura di), *2015 Italian Cyber Security Report. Un Framework Nazionale per la Cyber Security*, 2016.

[6] V. *infra* Capitolo II, par. 2.

[7] Per approfondimenti sul tema cfr. IASELLI, *Le nuove frontiere del cyber risk*, in *Altalex*, 2017, *https://www.altalex.com/documents/news/2017/09/06/le-nuove-frontiere-del-cyber-risk*, L'Autore approfondisce il concetto di *Cyber risk*, individuando preliminarmente le "5 grandi famiglie del rischio": operativi, finanziari, strategici, organizzativi, di pianificazione aziendale e *reporting*; segnalando come la peculiarità del rischio informatico sia quella di essere in grado di abbracciare indifferentemente ciascuna delle "5 famiglie". In oltre l'Autore qualifica come "rischio di natura esogena" il *Cyber risk*, in contrapposizione al "rischio di natura endogena" proprio degli eventi naturalistici.

relativamente alla costruzione ed identificazione delle fattispecie penali, volte a reprimere e sanzionare condotte illecite svolte per mezzo o avverso strumenti informatici[8]; invero la regolazione pubblica, nazionale e sovranazionale, per far fronte ai possibili illeciti legati al mondo *digital* si fonda, prevalentemente, sul generale principio di *accountability*[9], cioè, la tendenza legislativa volta a responsabilizzare e vincolare al raggiungimento di determinati obbiettivi.

Si richiede alle strutture organizzative di effettuare una previa valutazione dei rischi derivanti dalla loro attività e, di conseguenza, adottare le misure ritenute più idonee in base agli esiti dell'analisi. Il processo brevemente descritto si inserisce nell'annovero delle operazioni relative alla *compliance*[10] aziendale, che si articola proprio sul modello *risk assesment - risk managment*[11].

Nella loro gestione ed organizzazione, gli enti sono, dunque, vincolati sia da obblighi derivanti da leggi nazionali o norme sovranazionali, che impongono l'adozione di misure preventive, sia da fonti di autoregolazione interne, mediante le quali vengono adottate le menzionate misure. In violazione delle prime sono

---

[8] V. *infra* par. 2.

[9] Lett. principio di "responsabilizzazione" o "autoregolazione" dei titolari e responsabili dei trattamenti dei dati personali, trova numerosi riferimenti in diversi atti normativi di fonte europea. Il Regolamento (UE) n. 679/2016 (GDPR), volto a rafforzare la protezione dei dati personali e della *privacy* dei cittadini dell'Unione Europea, pone con forza l'accento sulla *accountability* (artt. 23 − 25 Capo I), ovverosia sull'adozione di comportamenti proattivi tali da dimostrare la concreta attuazione delle prescrizioni del regolamento. Si affida in questo modo ai titolari il compito di decidere autonomamente le modalità e i limiti del trattamento dei dati, alla luce dei criteri imposti dallo stesso GDPR. Altra fonte normativa di particolare importanza è la Direttiva UE 1148/2016 (NIS), rivolta, a livello europeo, alla protezione delle infrastrutture critiche rispetto alle minacce del mondo *cyber*. In via generale, il provvedimento identifica gli Operatori di Servizi Essenziali (OSE) e i Fornitori di Servizi Digitali (FSD), alla stregua dei criteri individuabili all'interno della direttiva, imponendo ai destinatari l'adozione di misure tecniche ed organizzative adeguate a proteggere le informazioni. «Per poter individuare le misure tecniche ed organizzative occorre che ogni destinatario della normativa effettui un *assessment* di rischio e di impatto della propria situazione concreta, individuando così le misure necessarie a seconda dei sistemi usati ed andandole ad implementare e a monitorare». Per approfondimenti v. *https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili;* MARTINI, MOSCA, SPECCHIO, *Sfida accountability, così la normativa spinge il business*, 2020, in *https://www.agendadigitale.eu/sicurezza/privacy/__trashed-24/*

[10] Voce COMPLIANCE in *Dizionario Garzanti online*, *«aderenza alle norme e alle prescrizioni di autoregolamentazione»*.

[11] Per approfondimenti cfr. QUARANTA, *Compliance risk: come gestire il rischio in modo efficace*, in *Teknoring*, 2020. L'Autore effettua un'analisi volta a sottolineare le differenze pratiche dei fenomeni in parola; in estrema sintesi afferma: «Il *Risk Assessment* è un'attività preliminare al vero e proprio *Risk Managment*: se la prima consiste nell'individuare e analizzare le diverse tipologie di rischio a cui una società potrebbe essere esposta, la seconda indica tutto l'insieme delle operazioni che un'azienda dovrebbe intraprendere per proteggere il proprio equilibrio economico e finanziario»; sul punto v. *infra* Cap. IV, par. 2.1.

previste sanzioni amministrative dirette, predeterminate dagli stessi atti normativi che disciplinano il settore di riferimento, attraverso le quali il legislatore fornisce effettività all'*accountability*. La violazione delle misure organizzative autoimposte ha, invece, rilevanti riflessi sul piano della responsabilità penale.

La fissazione di *standard* organizzativi e la previsione di obblighi di protezione divengono parametri per la commisurazione della responsabilità dell'ente. Si parla, in proposito, di "efficacia conformativa della prevenzione del rischio" che si muove nello spazio che il legislatore ha lasciato all'autonomia privata per autoregolamentarsi[12]. L'effetto della realizzazione di modelli organizzativi, e quindi, il raggiungimento degli *standard* di sicurezza minimi, può incidere su singoli elementi "flessibili" delle fattispecie penali (efficacia conformativa indiretta) ovvero, se previsto da norme di settore, può determinare la totale esclusione della responsabilità (efficacia conformativa diretta).

Da ultimo, in questa breve e sintetica disamina della disciplina della sicurezza informatica, resta da trattare un altro tema centrale che ha suscitato un acceso dibattito in dottrina: l'individuabilità di una posizione di garanzia nel *cyber* spazio. Al fine di inquadrare meglio la questione, è necessario porre attenzione su alcuni aspetti caratterizzanti l'ambito operativo oggetto di analisi.

Il *cyberspace* è, per definizione[13], un ambiente del tutto privo di confini territoriali e distanze fisiche, in cui sussiste la c.d. "ubiquità informatica", cioè la contemporaneità tra condotta ed evento[14]; nella rete, infatti, «i dati [...] raggiungono ogni parte del mondo e il loro autore non è in grado né di controllarne l'accesso, né di prevedere quali percorsi essi seguiranno per ricongiungersi infine sullo schermo degli altri utenti»[15] Quanto ora affermato

[12] L'esempio più chiaro e rilevante di questo meccanismo giuridico consiste nella disciplina della responsabilità amministrativa degli enti dipendente da reato *ex* d.lgs. 231/2001. In estrema sintesi, la disciplina prevede l'esclusione della responsabilità, dipendente da reato, dell'ente che, rientrando nei criteri per l'applicazione della disciplina, dimostri di aver adottato un modello organizzativo idoneo rispetto alle esigenze della struttura organizzativa. Per esaustiva trattazione cfr. LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti: diritto sostanziale*, Vol 1, Torino, 2020.

[13] Voce in CIBERSPAZIO in *Enciclopedia Treccani online*, «*Lo spazio virtuale nel quale utenti (e programmi) connessi fra loro attraverso una rete telematica, possono muoversi e interagire per gli scopi più diversi*».

[14] Sul punto cfr. MIRTI, *La disciplina giuridica del cyberspace*, in *Opinio Juris*, 2016, *https://www.opiniojuris.it/la-disciplina-giuridica-del-cyberspace/*.

[15] Così SEMINARA, *La pirateria su internet e il diritto penale*, in *Rivista trimestrale di diritto penale dell'economia*, 1997, 111.

giustifica l'espressione, spesso utilizzata per riferirsi allo spazio virtuale, di "non luogo", che ne evidenzia in maniera sintetica la tipicità. Sfumano, quindi, i concetti di azione ed evento, perdendo ogni connotazione naturalistica e venendo meno la dimensione temporale e spaziale dell'offesa.

In qualità di "non luogo", il *cyber* spazio è un moltiplicatore esponenziale di possibilità di comunicazione e scambi tra utenti, a prescindere dal contatto umano, attraverso strumenti assai diffusi, consentendo, potenzialmente, di agire nel completo anonimato. Si colgono facilmente, in questo quadro, le considerevoli possibilità criminali e criminogene, insite, appunto, nell'efficacissimo meccanismo di realizzazione dei reati. Tali proprietà del *cyberspace* hanno reso determinate categorie di delitti − ad esempio la diffamazione *ex* art. 595, co. 3, c.p., o la diffusione di materiali coperti dal diritto d'autore *ex* artt. 171 e seg. l. n. 633, 1941 − veri e propri reati di massa, con conseguente e sensibile diminuzione della percezione del disvalore delle condotte da parte dei consociati.

In questo complesso panorama, l'individuazione di una responsabilità in capo all'*Internet Service Provider* (d'ora in avanti anche solo ISP)[16] investe delicate scelte di politica criminale da parte dell'ordinamento giuridico, rispetto al necessario bilanciamento tra contrapposti diritti fondamentali: la piena esplicazione della libertà di manifestazione e comunicazione del pensiero in contrapposizione con i diritti fondamentali di altri individui della società, quali l'onore, la pubblica sicurezza ovvero la riservatezza e la protezione dei minori. Il "se" e il "come" individuare una posizione di garanzia in capo agli ISP ruota necessariamente intorno a questi elementi.

Il dibattito dottrinale che si è sviluppato con riguardo al tema in esame ha elaborato tre diversi paradigmi di responsabilizzazione penale, cui corrispondono

[16] Sul punto cfr. IASELLI, *Internet Service Provider. Guida all'ISP: cos'è, regime e tipologie di responsabilità*, in *Altalex*, 2019. *https://www.altalex.com/guide/internet-service-provider*. L'Autore definisce L'*Internet Service Provider* come "quel soggetto che esercita un'attività imprenditoriale che offre agli utenti la fornitura di servizi inerenti *Internet*, in sostanza è colui che fornisce ai terzi l'accesso alla rete, utilizzando una connessione remota tramite linea telefonica o banda larga". L'ISP mette quindi l'utente in connessione con la rete; si tratta di un vero e proprio intermediario. In prassi il ruolo di ISP è svolto da imprenditori, per cui si applica la generale disciplina civilistica *ex.* art. 2195 c.c., qualificandone l'attività come "esercizio d'impresa". Quanto poi alla categorizzazione, l'A. distingue due principali tipologie: l'*access provider*, che mette a disposizione agli utenti un punto di accesso alla rete, generalmente mediante specifico contratto, e il *content provider* che non si limita a garantire l'accesso, ma produce i suoi contenuti e offre una possibile e vasta gamma di servizi ulteriori.

parallelamente tre sistemi di bilanciamento di diritti fondamentali in conflitto e tre distinti ruoli sociali attribuiti agli ISP[17].

Il primo modello idealtipico è improntato alla massimizzazione della libertà di espressione e comunicazione in *Internet*. Si ritiene, in quest'ottica, che il legislatore debba astenersi dal dettare regole di prevenzione dei reati, poiché il rischio di commissione degli stessi non giustificherebbe l'adozione di meccanismi di censura preventiva. L'intervento del diritto penale è eventuale e successivo rispetto la commissione di fattispecie criminose, prestando il presidio sufficiente, determinato dall'effetto general-preventivo della sanzione, senza limitare preventivamente la libertà degli utenti. Il vivere sociale si basa sull'auto-responsabilità dei consociati.

L'ISP è posto sul medesimo piano degli altri utenti, senza obblighi di controllo delle condotte altrui o di denuncia di reati di cui viene a conoscenza. Il paradigma della responsabilità penale è limitato alle ipotesi di commissione delle fattispecie, o di concorso commissivo doloso[18] nelle condotte altrui. Si parla, in questo caso, di ISP "cittadino".

Il secondo modello idealtipico, diametralmente opposto al precedente, sposta l'attenzione sulla tutela dei soggetti terzi e della comunità, considerando la rete come un fattore di rischio per la garanzia di diritti rilevanti. L'informatizzazione, sempre più diffusa, dei processi decisionali e informativi manifesta la necessità di individuare preventivamente centri di filtraggio, controllo ed eventualmente di intervento. Difatti, a sostegno di questa posizione, si rileva come la funzione del diritto penale non sia, solamente, quella di punire condotte criminali, ma anche, e soprattutto, quella di prevenirle.

Quando vi è un fattore di rischio, l'attribuzione di una posizione di garanzia è funzionale alla tutela della posizione giuridica esposta al pericolo. Questa tutela può, quindi, assicurarsi solo attraverso la designazione di soggetti

---

[17] Per approfondimento sul tema v. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, in *Diritto Penale contemporaneo*, 2012.

[18] Sul concorso di persone nel reato si vedano, tra gli altri, INSOLERA, *Profili di tipicità del concorso: causalità, colpevolezza e qualifiche soggettive nella condotta di partecipazione*, in *Rivista italiana di diritto e procedura penale*, 1998, 440 ss.; FIANDACA, MUSCO (a cura di), *Diritto penale. Parte generale*, 7ª ed., 2015, Bologna, 509 ss.; SPERA, *Il concorso di persone nel reato* , in *Altalex*, 2020.

controllori – vale a dire gli ISP – cui spetterebbe l'obbligo di attivarsi, laddove risulti concretamente possibile, per prevenire la commissione di reati.

L'ISP assume, in questo caso, il ruolo sociale di "controllore" e il modello di responsabilità penale si struttura come reato omissivo improprio[19], muovendo il rimprovero di non aver impedito un reato altrui.

Il terzo modello idealtipico offre una posizione intermedia rispetto ai due appena descritti. I sostenitori, adottando un approccio più realista, rilevano elementi di verità in ambedue gli estremi, sottolineando come *internet* sia contemporaneamente vettore di libertà e fattore di rischio. La restrizione della libertà degli utenti deve essere limitata e predeterminata dal legislatore in maniera puntuale e precisa, evitando che ciò si trasformi in un generale strumento di censura.

Si vogliono valorizzare modelli di *compliance* e di controllo successivo. Il coinvolgimento degli ISP è, in questo caso, *ex post*: a questi non si attribuiscono più obblighi di verifica e filtraggio del materiale presente in rete, per così dire "all'ingresso"; si dovranno, invece, attivare per eliminare le conseguenze del reato e agevolare la punizione degli autori.

Il concetto ontologico alla base della sicurezza informatica è proprio quello della "libertà nella rete"[20]; il controllo esercitato deve essere mirato a fronteggiare determinate situazioni di rischio, e non generalizzato. Un meccanismo di prevenzione preventiva ad ampio raggio comprimerebbe eccessivamente non solo la libertà degli utenti, ma anche quella dei titolari dei fornitori di servizi in rete, rispetto ai quali una responsabilità per omesso controllo troppo rigorosa ostacolerebbe il libero esercizio di attività dell'iniziativa economica privata.

---

[19] Per tutti, si veda FIANDACA, MUSCO (a cura di), *Diritto penale. Parte generale*, 7ª ed., 2015, Bologna, 624 ss.; IAGNEMMA, *Il reato omissivo improprio nel quadro di un approccio sistematico all'evento offensivo*, in *Criminalia*, 2020, 309 ss.

[20] Sul punto v. DE MINICO, *Libertà in rete. Libertà nella rete*, 2ª ed., 2020, Torino. Il concetto di "libertà nella rete" si contrappone a quello di "liberta della rete", coinvolgendo, tra le altre, delicate questioni di diritto pubblico. L'Autrice analizza le due filosofie appena indicate, la prima improntata alla *self-regulation* degli imprenditori digitali, mentre a seconda adotta il sistema di eteronomia derivante dalla dialettica democratica parlamentare. La prima si affida alle c.d. "autorità private", mentre la seconda alle Autorità Pubbliche.

In questa prospettiva l'ISP assume il ruolo sociale di "tutore dell'ordine", e il paradigma della responsabilità penale è quello del reato omissivo proprio[21] muovendo il rimprovero di non aver tenuto condotte atte a garantire la punizione dell'autore e l'eliminazione delle conseguenze del reato.

Quanto poi alla questione centrale, cioè l'individuabilità di una vera e propria posizione di garanzia in capo agli ISP, bisogna necessariamente valutarne gli elementi costitutivi sul piano penalistico. Senza entrare nel merito della questione[22], l'esistenza di una posizione di garanzia postula: una fonte, normativa o fattuale, che attribuisca una responsabilità di controllo o protezione; l'effettiva esigibilità di una determinata condotta dal garante; l'accertamento in concreto di poteri impeditivi specifici.

Quanto al primo punto, non si rinviene alcuna norma, nazionale o sovranazionale, che imponga obblighi generali di vigilanza nella rete o dalla quale si possa desumere la responsabilità per la protezione dei beni sottoposti a rischio nel *Cyber-space*[23].

---

[21] Per approfondimento cfr. FIANDACA, MUSCO, *Diritto penale* cit., 621 ss.; MARINUCCI, DOLCINI, GATTA (a cura di), *Manuale di Diritto Penale. Parte Generale*, 11ª ed., Milano, 2022, 288 ss.

[22] Sul tema v. OCCHIPINTI, *Reato omissivo, posizioni di garanzia e casistica giurisprudenziale*, in *Cammino diritto*, 2015, n.15; FACCIOLINI, *Rapporto di causalità e posizione di garanzia*, in *Diritto.it*, 2022, *https://www.diritto.it/rapporto-di-causalita-e-posizione-di-garanzia/*.

[23] La fonte che sembrerebbe introdurre una disciplina normativa della posizione di garanzia in *internet* è la direttiva 31/2000/CE, attuata in Italia con d.lgs. n. 70/2003, che si occupa di disciplinare in via generale il commercio elettronico. Per quanto interessa ai fini del discorso in parola, la direttiva dedica alcuni articoli a delineare un regime di responsabilità penale degli intermediari *web* dai contorni ben definiti. Per approfondimento sul punto cfr. SCUDERI, *La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea*, in *Diritto Mercato Tecnologia*, 2018. L'Autrice afferma: «Riconoscere in capo all'ISP una responsabilità per tutti gli illeciti commessi in Internet sino a ricomprendere quelli posti in essere da soggetti terzi, ovvero gli utenti della rete, attribuiva, indubbiamente, una natura oggettiva alla responsabilità del provider, considerato che questi, lungi dal porre in essere materialmente l'illecito, avrebbe risposto del fatto dannoso solo in quanto fornitore di un servizio di accesso ad Internet. Per tale ragione, attesa l'impossibilità di negare una responsabilità dell'ISP in caso di illeciti *online*, la dottrina maggioritaria rinveniva il fondamento della responsabilità degli intermediari *web* nel criterio di imputazione della colpa». Il legislatore europeo ha configurato una responsabilità sussidiaria e colposa rispetto l'autore del reato, da individuare alla stregua della attività svolta dal *provider*. Da qui la previsione degli artt. 12, 13, 14 della direttiva, che categorizzano diversi tipi di ISP (*mere conduit, access, caching, hosting)*, diversificando il profilo di responsabilità colposa da reato altrui. Per quanto possa sembrare che la direttiva funga da fonte normativa per la posizione di garanzia dei *provider*, l'art. 15, n.1, statuisce che «Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite». Nonostante l'attenuazione di quanto affermato, per opera del secondo comma del medesimo articolo, prevedendo che «Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di

Circa la concreta esigibilità di una determinata condotta del *provider*, l'ambiente virtuale permette che anche solo su un singolo *server* possano circolare quantità tali di informazioni da non poter concretamente pretendere di sottoporre tutto il materiale a controllo preventivo.

Non è riscontrabile, infine, un potere impeditivo riconosciuto in capo agli ISP: a norma degli artt. 14, 15 e 16 d.lgs. 70/2003[24], si ricava che i *provider* sono tenuti a impedire l'accesso ai dati, o eventualmente a rimuoverli, solo a seguito di richiesta della pubblica autorità, o di fronte a materiale palesemente illecito. Per queste ragioni, la dottrina maggioritaria conviene per negare la sussistenza di una posizione di garanzia in capo agli ISP.

Alla medesima conclusione perviene, infine, la giurisprudenza. Nel noto caso *Google vs Vivi Down*[25], si è evidenziato l'impossibile esigibilità di una condotta di controllo preventivo, in ragione della mole di informazioni che ogni secondo transitano sui *server*. Allo stesso tempo, la Corte di Cassazione, chiamata a pronunciarsi sulla questione, ha affermato che nessuna disposizione «prevede che vi sia in capo al *provider* [...] un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito», e ha parimenti sottolineato che nessuna norma incriminatrice punisce «un ipotetico obbligo dei *provider* di ricordare agli utenti di rispettare la legge».

La mancanza di obblighi generali di controllo è frutto di un'accurata scelta legislativa, basata sul bilanciamento tra la libertà ed efficienza delle comunicazioni in *internet* e le garanzie dei diritti individuali. Non è, tuttavia, da escludersi in maniera assoluta la rilevanza dell'art. 40 cpv c.p. per l'omissione di determinati doveri giuridici; sono le discipline di settore che, dotate di particolare incisività, possono prevedere profili di responsabilità per gli ISP per omesso

---

presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati», resta pacifico che la direttiva in parola non sia fonte normativa di alcuna posizione di garanzia nel *cyberspazio*.

[24] Decreto attuativo della direttiva 2000/31CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.

[25] Cass. pen., Sez. III, 17.12.13, n. 5107, che conferma l'esito del giudizio di merito come deciso da App. Milano, 21.12.12, n. 8611. Per approfondimento cfr. INGRASSIA, *Le sentenze della Cassazione sul caso Google*, in *Diritto penale contemporaneo*, 2014.

impedimento[26]. Si tratta comunque di ipotesi residuali rispetto all'impostazione generale della disciplina, in cui non si riscontra alcuna posizione di garanzia.

2. Tecniche di *cyber-attacks* e reati informatici: questioni definitorie

Dopo aver offerto un'analisi sintetica della disciplina, sembrerebbe opportuno volgere l'attenzione verso un'ulteriore questione introduttiva, funzionale ad un corretto approccio alla materia oggetto di ricerca.

Prima ancora di valutare l'evoluzione normativa in materia[27], si vuole, in questo spazio, individuare le tecniche più diffuse nella prassi criminale di *cyber-attacks* e cercare di fornire le relative definizioni, così da intendere in maniera più corretta le strategie di politica criminale adottate dagli enti nazionali e sovranazionali.

Si segnala preventivamente che, di frequente, per ragioni di convenienza linguistica, si tende a far coincidere il concetto di *cyber-attack* con quello di reato informatico. Parrebbe più corretto, tuttavia, comprendere gli elementi distintivi dell'uno e dell'altro: i reati informatici – ovvero anche *computer crimes* – sono fattispecie penali, introdotte nell'ordinamento giuridico mediante apposita norma, frutto di precise scelte di politica criminale da parte del legislatore, atte a contrastare, prevenire e sanzionare condotte criminali tipiche del *cyberspace*, segnatamente della rete *internet.* Gli attacchi informatici consistono, invece, nelle suddette condotte criminali, evolutesi nella prassi e caratterizzate nei singoli elementi dall'ambiente in cui si sono sviluppate.

Si è già evidenziato come la rivoluzione tecnologica abbia reso disponibile una serie di strumenti in grado di creare nuove opportunità in numerose attività della società; parallelamente, però, i medesimi mezzi si sono rivelati altrettanto idonei a porre in essere nuove e pericolose condotte criminose.

Per potersi concentrare inizialmente sul delineare gli elementi distintivi e categorizzanti dei reati informatici, è utile partire dall'assunto secondo cui «individuare e definire compiutamente il fenomeno dei *computer crimes* è

[26] A titolo esemplificativo si segnalano artt. 14-*ter* e *quater* l. 269/1998, che prevedono obblighi di collaborazione per i *provider* con il Centro nazionale per la lotta alla pedopornografia in *internet*.
[27] V. *infra* par. 3.

obiettivamente un compito arduo e complesso»[28]. Le cause di questa intrinseca difficoltà di delineare una completa cornice descrittiva di queste fattispecie sono riconoscibili nell'ampia eterogeneità delle modalità attraverso cui è possibile compiere un'azione riconducibile alla categoria in parola, sia dal ruolo che lo strumento informatico può ricoprire nell'azione stessa.

Bisognerebbe effettuare in via preventiva una scelta di metodo. In dottrina si è rilevato che «la difficoltà di definire il concetto di crimine informatico si pone in tutta la sua evidenza se si osserva che, né a livello di legislazioni nazionali, né in ambito internazionale è stato possibile elaborare una definizione unitaria»[29]. Ne deriva incertezza anche e soprattutto attorno all'esistenza di un bene giuridico c.d. "informatico" da tutelare, costringendo i penalisti a estendere forme di tutela tradizionali a fatti che vertono su oggetti informatici. Non dovrà, quindi, ricercarsi una definizione unitaria di *cyber crimes* in una sequenza statica di parole, ma chiarirne il significato effettuando opportune distinzioni, adottando il più efficace metodo delle classificazioni.

Una prima classica distinzione tra due categorie di reati prende ad oggetto il ruolo che lo "strumento" informatico ricopre all'interno della fattispecie. Alcuni autori hanno rilevato come il *computer* può assumere diverse funzioni nella perpetrazione delle condotte criminali, potendo esserne oggetto, soggetto, strumento e simbolo[30].

Da questa preliminare classificazione è quindi possibile distinguere i *cyber* crimini tra "reati eventualmente informatici", ovvero *computer crimes* in senso lato, e "reati necessariamente informatici", ovvero *computer crimes* in senso

---

[28] Così POMANTE, *Internet e criminalità*, 1989, Torino, 437 ss.

[29] Sul punto cfr. FAGGIOLI, *Computer crimes*, 1998, Napoli, 10.

[30] Per approfondimento sul tema v. FELLUGA, *I Computer crimes: definizioni ed elementi principali*, in *Tigor: rivista di scienze della comunicazione e di argomentazione giuridica*, IV, 2012, Trieste, 31. Come afferma l'Autore, nel primo caso, essendo il *computer* "oggetto", la condotta include «la distruzione, la manipolazione, la manomissione o l'inservibilità dell'elaboratore, dei dati e dei programmi in esso contenuti e delle relative apparecchiature di supporto»; nel secondo caso, inteso come "soggetto", l'elaboratore consiste nel luogo, il motivo o la fonte del crimine; nella terza ipotesi il *computer* diviene strumento del reato quando ciò che avviene, rispetto all'elaboratore, non è di per sé illegale, ma è strumentale alla commissione di fattispecie criminose; nell'ultimo caso lo strumento informatico diventa elemento di circonvenzione fraudolenta della vittima, in ragione «dell'immagine di straordinaria efficienza tecnologica che il *computer* come simbolo esprime». Per una generale ricostruzione dello sviluppo del fenomeno riguardante i reati informatici, le difficoltà ermeneutiche e le diverse tecniche di formulazione si segnala anche PEORELLA, *Reati informatici*, in AA. VV., *Enciclopedia del diritto. Annali X*, 2017, Milano, 707 ss.

stretto. Il distinguo, nel dettaglio, risiede nella considerazione che la tecnologia informatica abbia solo ampliato le forme di manifestazione di un reato già esistente, o abbia determinato la configurazione di nuove fattispecie, precedentemente neppure ipotizzabili.

I reati c.d. "necessariamente informatici" sono stati specificamente formulati dal legislatore, con l'introduzione di fattispecie *ad hoc*, includendo cioè, nei loro elementi costitutivi, modalità di condotta, mezzi o effetti caratterizzati da un imprescindibile contenuto informatico[31]. L'introduzione di nuove ipotesi di reato si è resa necessaria per colmare lacune giuridiche che non sarebbe stato possibile superare in via interpretativa per il divieto di analogia in *malam partem*, derivante dal fondamentale principio di legalità in materia di diritto penale.

I reati c.d. "eventualmente informatici", al contrario, consistono in fattispecie tradizionali che, in ragione delle modalità con cui vengono poste in essere, si prestano ad implicazioni di carattere informatico, seppure in maniera accidentale e non caratterizzante. In questo caso le norme "comuni", per la loro struttura e formulazione, già si prestano a sussumere le nuove forme di commissione nel *cyber space*, senza la violazione del sopracitato divieto di analogia in *malam partem*, potendosi ricomprendere i nuovi comportamenti *cyber* nel loro ambito, anche se non concepiti al momento dell'originale stesura[32].

Un'ulteriore classificazione si basa sullo scopo che il soggetto agente intende perseguire. Trova qui spazio la suddivisione operata da autorevole dottrina più di un quarantennio addietro e, ciò nonostante, ancora attuale[33].

Si identificano tre gruppi di *cyber crimes*: fattispecie correlate all'uso del *computer* con lo scopo di realizzare un profitto per l'autore e/o la produzione di un

---

[31] Si segnalano a titolo esemplificativo i delitti di accesso abusivo a un sistema informatico *ex* art. 615 *ter* c.p., il reato di frode informatica *ex* art. 640 *ter* c.p., le falsità in documenti informatici pubblici *ex* art. 491 *bis* c.p., e in maniera particolare il sistema dei delitti di danneggiamento informatico *ex* artt. 635 *bis, ter, quater, quinquies* c.p., oggetto di approfondita analisi v. *infra* cap 2 e 3. Sul tema v. PICOTTI, *Cybercrime e tutela penale dei diritti della persona e della privacy nel web*, in *AIAF*, n, 1, 2020.

[32] Gli esempi più chiari sono il reato di diffamazione *ex* art. 595 c.p., per cui l'offesa alla reputazione può essere commessa «comunicando con più persone» certamente anche con messaggi *web*; ovvero altro esempio è il reato di estorsione *ex* art. 629 c.p., a seguito di criptaggio di dati e sistemi informatici altrui. Per approfondimento sul tema cfr. PICOTTI, *Cybercrime e tutela penale* cit.

[33] Cfr. SARZANA, *Criminalità e tecnologia: il caso dei computer crimes*, *in Rassegna penitenziaria e criminologica*, n. 1, 1979, 59 ss.

danno per la vittima; fattispecie dirette contro il *computer* inteso come entità fisica; fattispecie correlate all'uso del *computer* dirette a cagionare un danno fisico a individui o alla collettività.

Con riferimento, infine, al *modus operandi*, sebbene sia costantemente necessario aggiornare il novero delle possibili condotte, di pari passo con l'incalzante sviluppo tecnologico, è possibile effettuare un'ulteriore classificazione, individuando due categorie. La prima include i reati commessi per mezzo del *computer*, immettendo istruzioni fraudolente nella memoria del *device*, modificando i dati già presenti o aggiungendone di nuovi. La seconda include reati che sfruttano l'uso di un computer, che di per sé non esegue nulla di irregolare ma attraverso il quale sono perpetrati illeciti di penale rilevanza[34].

Dal tenore di suddette definizioni e distinzioni appare evidente che l'unico dato unificante dei *computer crimes* consiste nel coinvolgimento di strumenti informatici attraverso diverse modalità. Tuttavia è essenziale sottolineare come non tutte le condotte correlate all'uso del *computer*, ancorché penalmente rilevanti, possono essere annoverate nella categoria in parola. Tale qualifica è da limitarsi ai soli casi in cui il sistema informatico costituisca l'oggetto della condotta, in riferimento a quelle ipotesi in cui il coinvolgimento di particolari beni giuridici – informatici – comporti problemi di applicazioni delle norme tradizionali e la necessità di nuove fattispecie.

Si volge adesso l'attenzione all'ampia categoria dei *cyber-attacks*, partendo, come di consueto, dal tentare di fornire una prima definizione generica del fenomeno: tanto in dottrina quanto nella comunità scientifica si rintraccia più di un tentativo di circoscrivere le peculiarità in un'unica espressione definitoria; una prima, offerta da esperti del settore, si pronuncia nel seguente modo: «un attacco informatico è un tentativo malevolo e intenzionale da parte di un individuo o di un'organizzazione di violare il sistema informativo di un altro individuo o azienda. Di solito, l'*hacker* viola la rete della vittima per ottenere qualche tipo di vantaggio»[35].

---

[34] Per approfondimento v. FELLUGA, *I computer crimes* cit., 31 s.

[35] Si guardi a *definizione di attacco informatico*, in *cos'è un attacco informatico?*, *https://www.cisco.com/c/it_it/products/security/common-cyberattacks.html*.

Più attenta agli aspetti tecnici è invece la definizione fornita dalla *National Initiative for Cybersecurity Careers and Studies* (NICCS), secondo cui per *cyber-attack* si intende «*The intentional act of attempting to bypass one or more security services or controls of an information system* [...] *to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity*»[36].

Ovviamente le definizioni ora riportate non esauriscono gli aspetti tipici e vari dei *cyber-attacks*, che dovranno essere individuati nella prassi criminale, ma contribuiscono ad un inquadramento introduttivo e dimostrano, ancora una volta, come circoscrivere la *Cybersecurity* e le sue declinazioni in categorie dogmatiche generali sia un'operazione impossibile.

Ciò che, tuttavia, risulta possibile è prendere a riferimento aspetti specifici del fenomeno in parola che manifestano specifiche prerogative e, conseguentemente, elementi categorizzanti. A tal fine si considereranno ora le articolate tipologie di attacco informatico riscontrabili nella prassi criminale.

Sebbene il costante sviluppo tecnologico determini la continua evoluzione delle possibili minacce cibernetiche, si può preliminarmente effettuare una distinzione. Si intende *cyber-attack* "semplice" quello che consiste in un'unica operazione che, sul piano penalistico, identifica una singola condotta la quale configura uno dei reati previsti dall'ordinamento. Si parla invece di *cyber-attack* "complesso" intendendo più operazioni tra loro collegate, configurando, anche in tempi diversi, più fattispecie penali, in realizzazione del medesimo disegno criminoso, secondo la figura del reato continuato[37] *ex* art. 81, comma 2, c.p.

Le specifiche modalità di attacchi informatici sono numerose, da individuare, come anticipato, nella prassi criminale che, nel corso degli anni, ha subito grandi e complesse evoluzioni; seguirà una sintetica enucleazione delle principali tipologie dei *cyber-attacks*.

---

[36] Voce *attack* in *A Glossary of Common Cybersecurity Words and Phrases*, *https://niccs.cisa.gov/cybersecurity-career-resources/glossary*. Per approfondimento ed analisi della definizione cfr. TORRINI, *Cos'è un attacco informatico e quali sono le diverse tipologie*, in *UniversIT*, 2021, *https://universeit.blog/attacchi-informatici/*. Secondo l'Autore la definizione in parola è puntuale nel rimandare ad atti malevoli, da parte di singoli o di vere e proprie aziende, finalizzati al furto danneggiamento o distruzione di obbiettivi specifici.

[37] Per approfondimento si rimanda a FIANDACA, MUSCO (a cura di), *Diritto penale. Parte generale* cit., 704 ss.; MARINUCCI, DOLCINI, GATTA (a cura di), *Manuale di Diritto Penale. Parte Generale*, cit., 644 ss.

Rientrano nella categoria degli attacchi "semplici" quelli perpetrati mediante l'utilizzo di *malware*[38], ossia un'ampia gamma di programmi informatici che hanno in comune la capacità di introdursi, senza il consenso del proprietario, nei sistemi informatici, con finalità delittuose. Si ratta di applicazioni indesiderate, che possono nascondersi in codici o programmi legittimi o, più facilmente, in rete.

La prima tipologia specifica di *malware* è il *virus*, nella sua accezione particolare[39]: consiste in un *software*, di per sé non autonomamente eseguibile, che, in prima battuta, infetta un programma "ospite" che, una volta avviato, permette la proliferazione del *virus* infettando altri *files* con compiti dannosi – cancellazione, modifica degli stessi, formattazione etc.

Altra tipologia inclusa nei *malware* sono i c.d. programmi *worms*, ossia *software* che, diversamente dai *virus*, non necessitano del contributo materiale dell'utente attaccato, essendo dotati di autonomia funzionale, i quali diffondendosi nella rete infettano altri programmi, perseguendo finalità dannose.

Altro esempio ancora sono i programmi *trojan*, *software* all'apparenza legittimi ma con celate finalità malevole – furto, cancellazione o blocco di dati, *password* etc. − che non hanno necessità di infettare altri programmi per perseguire il loro obbiettivo, non propagandosi autonomamente, ma inducendo l'utente all'installazione; in questi casi gli *hacker* utilizzano tecniche di c.d. "ingegneria sociale"[40].

Sempre nella macro categoria dei *malware* si riscontrano gli *spyware*, programmi utilizzati per prelevare informazioni sensibili nei sistemi in cui sono occultamente installati, trasmettendo queste ultime al destinatario che poi le

---

[38] Letteralmente "programma cattivo", è un termine coniato nel 1990 da Yisrael Radai, noto ricercatore informatico israeliano che ha, tra le altre cose, analizzato approfonditamente la macrocategoria dei *virus* informatici; cfr. FOX, *The Israeli Who Put Your Virus Under the Microscope*, in *Jewis Telegrafic Agency*, 2014, *https://www.jta.org/jewniverse/2014/the-israeli-who-put-your-virus-under-the-microscope.* con il termine *malware* si vuole identificare una macro categoria di programmi informatici "malevoli", in grado di introdursi nei *devices* altrui, per danneggiare, rubare o spiare le vittime; per approfondimento sul tema v. IANESE, *Attacchi Malware, Ransomware e DDOS: quando sono*, in *SmartIUS*, 2021, *https://www.smartius.it/data-it-law/malware-ransomware-ddos-quando-sono-reato/.*

[39] Prima dello sviluppo di una "cultura" degli attacchi informatici si era soliti identificarli con il generale termine di *virus.*

[40] Anche *Social Engineering Techniques*, consistono in tecniche finalizzate all'ottenere informazioni per l'accesso alle infrastrutture informatiche dell'obbiettivo e dei loro contenuti, mediante lo studio dei comportamenti dei soggetti nell'uso della rete. Cfr. *CISCO, Che cos'è il social engineering?*, in *https://www.cisco.com/c/it_it/products/security/what-is-social-engineering.html*

utilizzerà, presumibilmente, per la preparazione di attacchi informatici o per trarne direttamente profitto. Sono programmi installati inconsapevolmente dall'utente-obiettivo che spiano i comportamenti e le abitudini nell'utilizzo del *computer* e nella navigazione in rete. Anche per questo genere di condotte l'*hacker* utilizza le sopracitate tecniche di ingegneria sociale.

Ultimo sottogruppo di *malware* consiste nei c.d. *adware*, ossia programmi progettati per proiettare annunci pubblicitari sul *computer* o reindirizzare l'utente verso siti pubblicitari, raccogliendo dati *marketing* e inviandoli verso *server* remoti. In questi casi il consenso viene comunque fornito dall'utente, sebbene, solitamente, carpito con dolo.

Ulteriore categoria compresa negli attacchi c.d. "semplici" sono i *ransomware*. Si tratta di programmi "malvagi" (volendo ancora *malware)* che, dopo aver infettato un *computer*, ne bloccano l'utilizzo mediante la criptazione dell'*hard-drive*, per il cui ripristino il soggetto attivo avanza una richiesta di riscatto. Si tratta di una condotta mediante la quale i dati di un utente vengono tenuti in ostaggio, se non anche minacciati di cancellazione o divulgazione, salvo pagamento del riscatto per ottenere la chiave di decriptazione. Sovente l'*hacker* richiede di essere pagato in criptovalute[41].

Si definisce, invece, *spamming* la pratica che consiste nell'invio insistente di posta indesiderata – per l'appunto chiamata *spam* – volta a indurre subdolamente gli utenti a connettersi a siti malevoli, determinando la diffusione di programmi *virus*. «Lo *spammer* – cioè colui che invia lo *spam* – utilizza riferimenti (*e-mail*, numeri telefonici, etc.) per l'invio di messaggi promozionali spesso raccolti in modo non lecito o in maniera automatica via Internet (su gruppi *Usenet*, *newsgroups*, *forum*, etc.), mediante speciali programmi (*spambot*, etc.) o, più semplicemente, facendo invii massivi a caso ad indirizzi *e-mail* basati sull'uso di nomi comuni»[42].

[41] Per approfondimento sul tema si veda OODRIVE TEAM, *I principali 10 tipi diversi di attacchi informatici*, in OODRIVE, 2021, *https://www.oodrive.com/it/blog/sicurezza/principali-10-tipi-diversi-di-attacchi-informatici/;* GDPD, *Ransomware*, in *Garante per la protezione dei dati personali*, *https://www.garanteprivacy.it/temi/cybersecurity/ransomware*.

[42] A riguardo v. GDPD, *Spam*, in *Garante per la protezione dei dati personali*, *https://www.garanteprivacy.it/temi/spam*

Ulteriore tecnica d'attacco è il c.d. *Man-in-the-middle*, consistente in una pratica di pirateria informatica attraverso la quale l'aggressore intercetta scambi di dati codificati tra due utenti o due *computer* per decodificarne e manipolarne i contenuti. L'*hacker* si inserisce tra due sistemi interconnessi in rete, spacciandosi per uno di essi e recependo le informazioni destinate al corrispondente. L'intruso può non limitarsi alla mera ricezione ma intervenire attivamente sui dati trasmessi, modificandoli o cancellandoli, finanche sostituendosi nel corso della comunicazione ad uno dei due *client*. Gli utenti che risiedono agli estremi del collegamento non sono in grado di accorgersi dell'intrusione, che avviene sfruttando la vulnerabilità dei codici di identificazione delle schede di rete[43].

Altro, ancora, gruppo di attacchi sono i *Domain Name System*[44] (anche solo DNS) *poisoning*. Consistono nell'inserire nelle *cache* di un DNS informazioni sbagliate, sostituendole alle originali, in modo da alterare l'associazione indirizzo *IP-server*. Di conseguenza, quando un utente inoltra una richiesta al *server* infettato viene, senza accorgersene, reindirizzato verso un altro *server*. Solitamente questo genere di attacco è prodromico ad altri *cyber-attacks*[45].

Ultima tipologia di *cyber-attack* c.d. "semplice" consiste negli attacchi *Denial of Service* (anche solo DoS). Si configurano come aggressioni mirate volte a rendere inutilizzabile un sistema o un servizio, per finalità meramente dimostrative, ovvero per perseguire scopi criminosi, causando interruzioni di servizi e perdite economiche. In altre parole l'obiettivo è quello di "ingolfare" le risorse di un sistema informatico che fornisce determinati servizi ai *computer*

---

[43] Per approfondimento v. *Attacco Man-in-the-middle, tutti i modi possibili e come difenderci*, in *Cybersecurity360, https://www.cybersecurity360.it/nuove-minacce/attacco-man-in-the-middle-tutti-i-modi-possibili-e-come-difenderci/*; si rilevano le diverse sottocategorie degli attacchi *Man-in-the-middle*, che si diversificano sulla base del "contesto" informatico in cui vengono perpetrati. In sintesi: *Man-in-the-wi-fi* se l'attacco avviene attraverso la compromissione di una rete *wi-fi*; *Man-in-the-mobile* se oggetto o mezzo dell'intrusione consiste in uno *smartphone*, solitamente al fine di *by*-passare l'autenticazione a due fattori tipica dei *browser* finanziari e bancari; *Man-in-the-browser*, conosciuto anche come *banking trojan*, che installando un programma su un dispositivo della vittima è in grado di modificarne le operazioni; *Man-in-the-lot*, in riferimento all'ormai attuale fenomeno dell'*internet of things*, a riguardo degli attacchi aventi come obbiettivo i numerosi oggetti connessi alla rete; da ultimo i *Man-in-the-app*, nel caso di attacchi svolti falsificando i certificati di sicurezza delle applicazioni usate anche quotidianamente dagli utenti.

[44] Si intende per *Domain Name System* un sistema che traduce nomi comprensibili, come i nomi di un dominio *web*, in indirizzi *IP* utilizzati dal *computer*, cioè in stringhe numeriche utilizzate dai *devices* informatici per comunicare tra loro.

[45] Sul tema v. *Che cos'è il DNS cache poisoning?*, in *Cloudfare*, *https://www.cloudflare.com/it-it/learning/dns/dns-cache-poisoning/*.

connessi. Ciò avviene, solitamente, inondando il sito *web*, obbiettivo dell'attacco, con numerose false richieste di accesso, a cui non riesce a far fronte[46].

Gli attacchi DoS sono sicuramente tra i più diffusi nella prassi criminale informatica, tanto da aver subito un'efficace evoluzione in breve tempo, potendosi, soprattutto manifestare come forme di *cyber-attack* "complessi". In questi casi si parlerà di *Distributed Denial of Service* (d'ora in avanti anche solo DDoS).

I DDoS funzionano allo stesso modo delle loro versioni "semplici" ma su scala molto più ampia. In questo caso, infatti, le domande fasulle arrivano nello stesso momento da più fonti, determinando di conseguenza una maggior efficacia dello strumento d'attacco, che, per funzionare, richiede minore tempo, mentre gli effetti perdurano più a lungo. Gli obbiettivi solitamente sono interi *datacenter*, cioè reti di distribuzione di dati o servizi, che divengono, così, irraggiungibili o completamente inutilizzabili[47]. Per questo genere di operazioni gli *hacker* si dotano di un vasto numero di *computer*, distribuiti su un'ampia area geografica o su più *providers*.

Uno strumento particolarmente efficace per svolgere questa funzione è il c.d. *botnet*[48], un insieme di *computer* infettati da *malware* che permette all'*hacker* di assumerne il controllo e fargli eseguire determinate operazioni. Quello del *botnet* è un fenomeno di sempre maggiore diffusione, registrandosi tra l'altro l'esistenza di grandi reti di *computer* infettati, sottoposti al controllo di un "amministratore malevolo", ovvero *bot-operator*, che affittano queste capacità ad elementi criminali.

Si può quindi volgere l'attenzione sulle principali manifestazioni di attacchi informatici "complessi", di cui i DDoS ne costituiscono un esempio.

Vi si inserisce, inoltre, il particolare fenomeno criminologico ad ampissima diffusione[49], identificato con il generico termine di *phishing*. In

---

[46] Per approfondimento si veda *Attacchi DoS, cosa sono e come proteggersi*, in *NEXSYS*, *https://www.nexsys.it/attacchi-dos-cosa-sono-e-come-proteggersi/*.

[47] Sul tema si veda *Attacco DDoS (Distributed Denial of Service): Cos'è, come fare, come difendersi*, in *Cybersecurity360*, *https://www.cybersecurity360.it/nuove-minacce/ddos-cosa-sono-questi-attacchi-hacker-e-come-stanno-evolvendo/*.

[48] Per ulteriori approfondimenti v. *LA BOTNET*, in *Telsy*, *https://www.telsy.com/it/le-botnet/*.

[49] Secondo un rapporto di *Zscaler* solo nel 2021 il bilancio registrato è di oltre 873 milioni di attacchi informatici di questo genere (*phishing*) con un aumento del 29% rispetto l'anno

estrema sintesi, si tratta di una serie di operazioni volte al furto di dati personali contenuti nello spazio *web*, per lo svolgimento di operazioni *online*, al fine di sottrarre, a soggetti terzi inconsapevoli, ingenti somme di denaro dalle aree riservate dei conti correnti o dei sistemi di pagamento.

Si configura come una modalità di commissione della truffa *online*, svolta attraverso una serie precisa di attività in sequenza, che costituisce il paradigma tipico di commissione del *phishing*[50]; in prima battuta l'utente-obbiettivo viene adescato e raggirato mediante l'invio, di frequente, di una *email* fraudolenta, apparentemente spedita da un mittente affidabile, come ad esempio un istituto di credito, che induce l'utente a connettersi, attraverso un collegamento ipertestuale ingannatorio, ad un sito-clone, grazie al quale vengono sottratti i codici di accesso alla vittima. L'operazione successiva comporta l'utilizzo dei dati o la loro commercializzazione, allo scopo di trarne profitto[51].

Si tratta, come si è evidenziato, di un *iter criminis* complesso e articolato, suscettibile di numerose categorizzazioni, a seconda delle specifiche modalità di esecuzione. Si segnala, a titolo esemplificativo, il *pharming*, in cui la fase ingannatoria avviene attraverso la manipolazione degli indirizzi DNS, al fine di reindirizzare l'utente-vittima verso un sito *web* creato appositamente dall'*hacker* per perseguire i suoi scopi criminosi.

Da ultimo resta da analizzare una pratica di attacco informatico che, negli ultimi anni, ha subito una sensibile crescita e diffusione e che viene considerata, da molti, come l'evoluzione del *phishing* e del *social engineering*[52]: il c.d. *watering hol*e. In sintesi, consiste nella pratica di attirare un gruppo definito di

---

precedente; *https://www.zscaler.com/press/new-zscaler-research-shows-over-400-increase-phishing-attacks-retail-and-wholesale-industries.*

[50] Cfr. LAVECCHIA, *Phishing attack: Significato, utilizzo e fasi del Phishing informatico,* in *Informatica e Ingegneria Online*, *https://vitolavecchia.altervista.org/phishing-attack-significato-utilizzo-e-fasi-del-phishing-informatico/*; l'Autore identifica 6 distinte fasi dell'attaco di *phishing* tipico: *planning*, cioè la pianificazione, *setup*, la preparazione tecnica, *attack*, la fase operativa nella quale l'attaccante instaura un contatto con la vittima, *collect*, cioè la materiale sottrazione delle credenziali di accesso, *fraud*, la vendita o il diretto utilizzo dei dati sottratti, e *post attack*, cioè la disattivazione dei meccanismi precedentemente attivati e la "fuga".

[51] Per approfondimento sul tema v. IASELLI, *Il Phishing*, in *Altalex*, 2020, *https://www.altalex.com/guide/phishing; Phishing, cos'è e come proteggersi: la guida completa*, in *Cybersecurity360*, *https://www.cybersecurity360.it/nuove-minacce/ransomware-cose-come-rimuoverlo-e-come-difendersi/*,

[52] Cfr. RIGONI, *Attacco Watering hole: tutto quello che devi sapere*, in *Cyberment*, *https://cyberment.it/cyber-attacchi/attacco-watering-hole-tutto-quello-che-devi-sapere/.*

utenti su siti *web* compromessi, sfruttando la loro stessa curiosità, avendo studiato le loro abitudini. In altri termini l'*hacker* verifica attentamente quali siti *web* normalmente vengono visitati dal gruppo di vittime designato e, solo successivamente, li colpisce mentre, sfruttando eventuali vulnerabilità, li "infetta".

Da ciò si evince quella che può dirsi la principale peculiarità degli attacchi *watering hole*, e cioè fare in modo che sia la stessa vittima a cercare l'agente malevolo presente sul *server*, e non più l'*hacker* a sollecitarne la visita. Per questo motivo, è particolarmente difficile da identificare l'attacco, a maggior ragione se l'aggressore riesce ad individuare e sfruttare vulnerabilità delle pagine *web* non ancora note al momento della condotta[53].

La sintetica enucleazione e descrizione delle principali manifestazioni delle fattispecie criminose riscontrabili nell'ambiente *cyber* non si può definire esaustiva. L'evoluzione delle pratiche che il *web* e le infrastrutture digitali permettono di compiere è in costante accelerazione, tanto da costringere gli ordinamenti giuridici e le strutture organizzative, private o pubbliche, ad inseguire il progresso della criminalità informatica, ogni qual volta lo stesso assuma nuove e differenti configurazioni.

In conclusione, il contributo definitorio qui brevemente riportato, oltre che funzionale ad una, quanto più possibile, completa conoscenza della materia della *Cybersecurity*, risulta strumentale al fine di cogliere, in maniera più approfondita, le ragioni del grande rilievo offensivo e dell'allarmante impatto sociale che, sin dalle sue origini, ha suscitato in dottrina ma anche nella società informatica che quotidianamente si interfaccia con il *web* e, di conseguenza, con le sue criticità.

3. Evoluzione della disciplina

Le strutture tecnologiche, in continua evoluzione ed innovazione, sono state − sin dagli albori dello sviluppo informatico − e continuano ad essere oggi, un fattore di trasformazione della comunicazione e delle relazioni tra gli uomini. Le regole giuridiche che seguono l'evoluzione di questo sistema si devono necessariamente aprire a nuove prospettive di tutela e disciplina.

[53] Per approfondire il tema v. PAGANINI, *Phishing, spear phishing e watering hole: quali differenze?*, in *Techeconomy2030*, 2014, *https://www.techeconomy2030.it/2014/03/11/phishing-spear-phishing-e-watering-hole-quali-differenze/*.

Tale fenomeno di modernizzazione, che ha generato una radicale trasformazione del sistema dei servizi informatici e telematici, offerti dagli apparati burocratici, economici ed amministrativi, non è, ovviamente, passato inosservato dinanzi agli occhi della criminalità, richiedendo anche al diritto penale una costante operazione di aggiornamento ed adattamento ai pericoli che progressivamente emergono dal mondo *digital*.

Nei paragrafi precedenti si sono analizzati i diversi metodi di manifestazioni aggressive della criminalità informatica al c.d. "bene informatico", perpetrate, in origine, grazie alla complicità di un evidente vuoto di tutela negli ordinamenti giuridici nazionali e sovranazionali[54]. Nelle pagine che seguiranno, invece, l'analisi avrà ad oggetto proprio la risposta normativa che gli enti pubblici hanno fornito, nel corso del tempo, all'incalzante richiesta di adeguata tutela e prevenzione, per arginare e scoraggiare i comportamenti illeciti di matrice informatica.

Il legislatore italiano ha manifestato l'intenzione di prevenire e reprimere la criminalità informatica − ad eccezione di alcuni sporadici interventi settoriali[55] − attraverso un'*iter* che risulta condizionato in maniera significativa dall'azione propulsiva di alcuni organismi internazionali, ai quali il nostro Stato appartiene.

Per questo motivo l'analisi dell'evoluzione normativa avanzerà, in questo elaborato, seguendo un criterio non esclusivamente cronologico, ma prendendo in considerazione, dapprima, le singole organizzazioni internazionali e i provvedimenti da loro emanati, per poi volgere l'attenzione sulla recezione degli stessi da parte del legislatore nazionale.

[54] Cfr. MAZZA, *Computer Crimes e Tecnologie informatiche*, in *Rivista di Polizia*, 2007, 353.

[55] Per quanto una disciplina nazionale generale relativa alla categoria dei reati informatici non si vedrà nel nostro paese prima della legge 547/1993, si segnalano alcuni interventi legislativi settoriali precedenti l'*iter* che prende propulsione dagli organismi internazionali; i primi progetti, infatti, sono stati presentati al Parlamento a partire dalla fine degli anni '70. A riguardo gli unici tre provvedimenti approvati dal legislatore nazionale sono: legge 19/1978, che introduce nel codice penale l'art. 420 che, prevedendo e sanzionando l'attentato agli impianti di pubblica utilità, fa espressa menzione anche degli impianti di elaborazione di dati; legge 121/1981, che istituisce il Centro elaborazione dati preso il ministero dell'interno; legge 76/1983, in tema di manomissione ed alterazione degli apparecchi misuratori fiscali, prevede all'art. 2, com. l'alterazione del dato di rilievo fiscale contenuto nello strumento elettronico. In aggiunta si segnala la presentazione di numerose proposte di legge non approvate. Sul tema si veda MAZZA, *Prevenzione e repressione in tema di reati informatici*, in *Osservatorio Penale*, 2016.

3.1. Consiglio d'Europa: la raccomandazione 9 settembre 1989 n. R (89) 9 e la Convenzione di Budapest (2001)

Il primo lavoro organico avente a oggetto il settore della criminalità informatica è stato compiuto da un gruppo di esperti, riuniti a Parigi, ad opera del Comitato per la Politica dell'Informazione, dell'Informatica e delle Comunicazioni dell'OCSE[56]. Recependo gli stimoli derivanti dalla comunità internazionale e dai singoli paesi, il gruppo di esperti compilò tra il 1984 e il 1985 un ampio rapporto[57], analizzandovi i principali orientamenti normativi dei singoli paesi membri dell'organizzazione, riguardanti la frode informatica e le concrete soluzioni adottate nell'ambito del diritto penale.

Le indagini casistiche svolte dimostrarono, fin da subito, la realtà e la sensibilità dei fenomeni, rilevanti sul piano dei rapporti economici e giuridici, che i legislatori «avrebbero dovuto prendere seriamente in considerazione»[58].

A seguito di tale lavoro, nel settembre del 1989, il Comitato dei Ministri[59] degli Stati membri del Consiglio d'Europa approvò la Raccomandazione n. R (89)-9 relativa al «*Computer-related Crime*»[60].

Tale raccomandazione si apre con il riconoscimento della necessità di un'adeguata e rapida risposta normativa al crescente fenomeno della criminalità informatica, in considerazione, tra l'altro, della sua peculiare natura transfrontaliera. Il Comitato non voleva fornire una generale ed univoca definizione del *cyber-crime*, ma si poneva l'obbiettivo di incentivare uno sviluppo uniforme della prospettiva europea, individuando le possibili scelte di tutela normativa che avrebbero potuto consentirlo. Si limitò quindi a dettare alcune

---

[56] Cfr. Informativa del Ministero di economia e delle Finanze *https://www.dt.mef.gov.it/it/attivita_istituzionali/rapporti_finanziari_internazionali/organismi_internazionali/ocse/*: Organizzazione per la Sicurezza e la Cooperazione in Europa; si tratta di «un'organizzazione internazionale di studi economici per i paesi membri, paesi sviluppati aventi in comune un sistema di governo di tipo democratico ed un'economia di mercato. L'organizzazione svolge prevalentemente un ruolo di assemblea consultiva che consente un'occasione di confronto delle esperienze politiche, per la risoluzione dei problemi comuni, l'identificazione di pratiche commerciali ed il coordinamento delle politiche locali ed internazionali dei paesi membri». Istituita nel dicembre del 1960 con il trattato di Parigi, città dove attualmente risiede, contando 36 paesi membri, prevalentemente, ma non esclusivamente, europei.

[57] V. OCSE, *Computer-related crime: analysis of legal policy*, Parigi, 1986.

[58] A riguardo si veda MAZZA, *Prevenzione e repressione in tema di reati informatici* op. cit.

[59] Il Comitato dei Ministri è l'organo decisionale del Consiglio d'Europa, composto dai Ministri degli Affari esteri di tutti gli stati membri o dai loro rappresentanti diplomatici permanenti presso Strasburgo.

[60] Cfr. *Council of Europe Committee of Ministers*, *Recommendation R (89) 9*, Strasburgo, 1989.

direttive rivolte ai legislatori degli Stati membri, lasciando, a ciascuno di essi, la possibilità di formulare le proprie disposizioni e, quindi, di disciplinare autonomamente il proprio sistema giuridico nazionale.

L'inefficienza degli strumenti giuridici offerti dal diritto penale vigente all'interno dei singoli ordinamenti giuridici, congiuntamente con la necessità di rispettare l'alto valore general-preventivo che dovrebbe avere l'intervento penale − nonostante le evidenti difficoltà di accertamento di questo tipo di condotte criminose − aveva rilegato i *computer-crimes* in una forma di "isolamento normativo"; si inserivano in una zona di interesse non compiutamente formalizzata, a metà tra una difficile interpretazione della normativa in vigore e la necessità di creare nuove fattispecie in grado di sussumere le nuove condotte criminali informatiche, non sanzionabili attraverso le disposizioni già presenti negli ordinamenti[61].

Per questa ragione, il Consiglio d'Europa, nel suo lavoro, si è limitato ad indicare l'ambito di estensione del diritto penale informatico, raccomandando ai legislatori dei paesi membri di inserire nel proprio ordinamento una c.d. "lista minima" di infrazioni, prevedendo poi una c.d. "lista facoltativa", all'interno della quale vennero inserite altre figure criminose di cui ere già nota la portata afflittiva e che rischiavano di divenire, in un momento successivo, particolarmente diffuse[62].

Con particolare riguardo al sistema dei delitti di danneggiamento informatico − tema centrale del presente elaborato − non pare superfluo evidenziare il contributo fornito dalla Raccomandazione n. R (89)-9, primo atto ad indicare espressamente i predetti delitti − inseriti nella c.d. "lista minima" −

---

[61] Sul tema si è espresso MAZZA, *Prevenzione e repressione in tema di reati informatici* cit.

[62] Cfr. *Council of Europe Committee of Ministers, Recommendation R (89) 9,* cit., 36 ss.; nell'annovero della "lista minima" si inseriscono: la frode informatica, il falso informatico, danneggiamento di dati e programmi informatici, sabotaggio informatico, l'accesso non autorizzato a sistema informatico, l'intercettazione non autorizzata, la riproduzione non autorizzata di programma informatico protetto e la riproduzione non autorizzata di una topografia; nella "lista facoltativa", invece, sono inserite: l'alterazione di un programma o dato informatico, lo spionaggio informatico, l'utilizzo non autorizzato di un computer e l'utilizzo non autorizzato di un programma protetto (traduzione letterale della versione ufficiale in lingua inglese). L'Italia ratificò la raccomandazione, dandone seguito con l'inserimento delle fattispecie previste dalla "lista minima" con la legge 547/1993. Per approfondimento del tema v. TADDEI ELMI (a cura di), *La Raccomandazione del Consiglio d'Europa del 9 settembre 1989 n. R (89)-9 e la Legge 23 dicembre 1993 n. 547 in materia di computer crimes: una analisi comparativa*, in *Informatica e Diritto*, vol. V, 1995, 113 ss.

successivamente introdotti nell'ordinamento penale italiano, con la Legge 3 dicembre 1993 n. 547[63].

In termini generali, la Raccomandazione R (89)-9 ha acceso i riflettori su un tema − quello della *cybersecurity* − fino a quel momento, trascurato dalle legislazioni. Non solo ne sono conseguiti interventi e riforme normative nazionali, ma la comunità internazionale ha iniziato, più di prima, a sentire la necessità di una collaborazione comune per individuare una linea strategica condivisa e strumenti comuni di tutela e prevenzione.

Nella società che si è nel tempo sviluppata, in cui si fa sempre più affidamento sulla tecnologia e sull'informazione, la risposta più chiara al sempre maggiore rischio derivante dai *cyber-crimes* viene offerta dalla Convenzione sulla criminalità informatica, approvata dal Consiglio d'Europa nel novembre del 2001 a Budapest.

La Convenzione − anche nota semplicemente come Convenzione di Budapest − è uno strumento di primaria importanza nonché, innegabilmente, il maggiore sforzo finora effettuato a livello internazionale nella lotta alla criminalità informatica; consiste infatti, ad oggi, nell' unico documento normativo internazionale vincolante in questo ambito. L'esigenza, propria della comunità giuridica, non solo europea, di giungere ad un tale esito è stata già più volte segnalata: la natura transfrontaliera delle condotte tipiche del *cybercrime*, congiuntamente con il crescente e, ormai, positivizzato bisogno di armonizzare i diversi quadri normativi, nel tentativo di uniformare il più possibile le legislazioni[64].

In via ancora preliminare, due sono le principali caratteristiche della Convenzione che hanno garantito efficacia e fortuna al provvedimento: uno è l'innovazione, che trae fonte dai numerosi riferimenti, e conseguenti contributi definitori, forniti dal testo stesso, a sistemi informatici, telematici, dati, rete e informazioni; l'altro consiste nella flessibilità, determinata dalla natura di c.d.

[63] V. *infra* par 3.3.
[64] Così correttamente segnalato da MANZARI, *La convenzione di Budapest, l'alba di una normativa di contrasto al* cyber crime, in *bptmavvocati*, *https://www.bptmavvocati.it/portfolio/i-reati-informatici-e-la-convenzione-di-budapest/*.

"disciplina quadro" della Convenzione[65], tale per cui le parti hanno regolamentato gli elementi su cui sono state in grado di trovare un accordo, lasciando spazio per successivi aggiornamenti sulle problematiche sopra le quali non si è raggiunta un'intesa[66]. In altre parole, può affermarsi che la Convenzione sia costantemente in fase evolutiva, grazie alla continua possibilità di aggiungere note di orientamento e protocolli.

Con riguardo alle concrete finalità che hanno portato il Consiglio d'Europa all'emanazione della Convezione in parola, autorevole dottrina si è espressa nel seguente modo: «L'obiettivo primario della Convenzione sulla criminalità informatica risiede nell'esigenza di introdurre un *minimum target* di tutela dei beni giuridici offesi dai *cyber-crimes* ed un livello minimo essenziale comune di strategie di contrasto a tali illeciti, soprattutto in ragione della loro natura tendenzialmente transnazionale, che comporta chiaramente la necessità dell'armonizzazione della relativa normativa di contrasto nell'ambito dei vari ordinamenti»[67].

Altro indice degli scopi della Convenzione è il preambolo introduttivo della stessa. La chiara questione primaria, consolidata nelle intenzioni del Consiglio d'Europa, è quella di creare una politica comune della prevenzione e contrasto ai reati informatici[68]. I mezzi messi a disposizione dal Consiglio

[65] Per approfondimento di veda ILARDA, MARULLO, *Cybercrime: conferenza internazionale : la Convenzione del Consiglio d'Europa sulla criminalità informatica*, in *Osservatorio permanente sulla criminalità organizzata*, Milano, 2004, 24 ss.

[66] Dall'emanazione della Convenzione già sono stati due i protocolli aggiuntivi: uno del 2003 che include nella Convenzione i reati legato alla propaganda a sfondo razzistico e xenofobo; un altro nel 2021 per rafforzare la cooperazione internazionale nella raccolta e divulgazione delle prove elettroniche. Cfr, DI GIACOMO, *Protocollo addizionale alla convenzione di Budapest sulla criminalità informatica: l'Italia che guarda al futuro*, in *diritto.it*, 2022, *https://www.diritto.it/protocollo-addizionale-alla-convenzione-di-budapest-sulla-criminalita-informatica-litalia-che-guarda-al-futuro/*; OCCHIPINTI, *Criminalità informatica, il secondo protocollo addizionale alla Convenzione di Budapest*, in *Altalex*, 2022, *https://www.altalex.com/documents/news/2022/05/26/criminalita-informatica-secondo-protocollo-addizionale-convenzione-budapest.*

[67] Cfr. RESTA, Cybercrime *e cooperazione internazionale nell'ultima legge della legislatura*, in *Corriere del merito*, 2008, n. 9, 2147 ss.

[68] Nel preambolo gli stati membri e gli altri stati firmatari si affermano, infatti, «convinti della necessità di perseguire, come questione prioritaria, una politica comune in campo penale finalizzata alla protezione della società contro la criminalità informatica, adottando una legislazione appropriata e sviluppando la cooperazione internazionale»; v. *Convenzione di Budapest sulla criminalità informatica, Preambolo.*

d'Europa per perseguire quanto detto sono l'armonizzazione delle procedure nazionali[69] e il potenziamento dell'assistenza giudiziaria.

Per quanto riguarda il contenuto della Convenzione, in via preliminare è possibile suddividerla in tre macro aree: la criminalizzazione di condotte criminose (Capitolo II, Sezione I); strumenti di diritto processuale (Capitolo II, Sezione II) e norme per una cooperazione internazionale efficiente (Capitolo III). Si aggiungono poi due elementi non meno importanti, cioè il Capitolo I, dedicato alle definizioni utili al fine della Convenzione[70], e il Capitolo IV, contenente le disposizioni finali.

Più nel dettaglio, il Capitolo II, relativo a «provvedimenti da adottare a livello nazionale», dedica la prima Sezione al profilo di diritto sostanziale; sono qui inserite tutte le fattispecie, suddivise in 4 Titoli[71], previste dalla Convenzione e che i singoli Stati firmatari hanno dovuto criminalizzare nell'ordinamento interno. I crimini previsti da suddetto elenco sono, per la maggior parte, quelli indicati dalla Raccomandazione R (89)-9, avendo avuto come riferimento proprio le linee guida derivanti dal documento emanato dal Consiglio d'Europa nel 1989.

Appena successive all'elenco di reati vi sono alcune significative disposizioni ad esso collegate. Si segnala tra queste l'Art. 11, paragrafo 2, che prevede la punibilità del tentativo per la maggior parte delle fattispecie criminose, ai sensi del quale le Parti devono definire, nelle loro legislazioni interne, come reato «il tentativo di commettere ogni tipo di reato in base agli articoli da 3 a 5, 7, 8, 9.1 a. e c. della presente Convenzione»[72]. Come si evince dalla disposizione in

[69] Si intende per "armonizzazione delle procedure" la creazione di una regolamentazione comune di un fenomeno globale, nel rispetto delle differenti tradizioni giuridiche nazionali. È un fattore fondamentale laddove, in ragione della trans-nazionalità di un fenomeno, un controllo statale non è possibile. In ambito europeo, in specie nel contesto dell'Unione Europea, il termine "armonizzazione" viene adoperato per indicare il processo di progressivo ravvicinamento delle legislazioni degli Stati membri, al fine di eliminare ogni ostacolo, normativo, tecnico o burocratico, nelle relazioni dell'Unione. Per approfondimento *Armonizzazione*, in *Dizie*, *https://www.dizie.eu/dizionario/armonizzazione/;* ARENA, *La Convenzione come modello di armonizzazione*, in *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*, 2021, 11 ss.

[70] Nel dettaglio si offrono le definizioni di: "sistema informatico", "dati informatici", "*service provider"* e "trasmissione dei dati". Cfr. Art. 1 *Convenzione di Budapest*.

[71] Titolo I "reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici", Titolo II "reati informatici", Titolo III "reati relativi al contenuto", Titolo IV "reati contro la proprietà intellettuale e diritti collegati".

[72] Art. 11, par. 2, *Convenzione di Budapest sulla criminalità informatica*.

esame, non tutti i reati vengono puniti a titolo di tentativo, ma solo quelli *ivi* segnalati.

La seconda Sezione del Capitolo II è, invece, dedicata alle misure processuali, prevedendo, in conformità con le esigenze di armonizzazione e cooperazione rafforzata, un vero e proprio statuto processuale, destinato ad essere implementato negli Stati aderenti. La redazione della parte processuale della Convenzione ha richiesto un maggiore controllo e un delicato esercizio di bilanciamento tra la necessità di migliorare le capacità di contrasto al crimine informatico, tramite strumenti processuali adatti e la tutela di libertà individuali e della *privacy*[73].

In estrema sintesi è possibile affermare che gli Artt. 14-22 della Convenzione di Budapest − dedicati al profilo di diritto processuale − introducono, oltre che le misure procedurali tradizionali della perquisizione e del sequestro adattate al nuovo contesto tecnologico, una disciplina volta all'ottenimento ed alla conservazione dei dati e delle informazioni, in vista di procedimenti penali[74].

Il Capitolo III è dedicato alla cooperazione internazionale e contiene principi generali e disposizioni specifiche. L'obbiettivo è quello di ridurre gli ostacoli, a livello internazionale, al flusso di informazioni e consentire lo svolgimento di indagini per conto di altri Stati trasmettendo le risultanze probatorie con maggiore rapidità.

---

[73] Per approfondimento sul tema cfr. ARENA, *La Convenzione di Budapest del Consiglio d'Europa*, op. cit., 27 ss.

[74] Di particolare interesse e meritevole di brevi ed ulteriori cenni è l'Art. 14 della Convenzione, relativo all'ambito di applicazione delle disposizioni procedurali. Si tratta di una norma che attiene al piano dei principi, stabilendo regole generali. Al paragrafo 1 prevede che «Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire i poteri e le procedure previste in questa Sezione per indagini o procedimenti penali specifici». Nel Paragrafo 2, invece, viene circoscritto l'ambito di operatività delle norme procedurali: esse trovano applicazione nei reati stabiliti dalla Convenzione, agli Artt. 2-11, a tutti i reati comunque commessi attraverso un sistema informatico e nella raccolta di prove in forma elettronica per un reato. A questa regola sono previste due eccezioni, una da ricondurre alla clausola di riserva «Salvo contraria disposizione risultante all'articolo 21», posta in apertura del Paragrafo II, Art. 14, l'altra è relativa alla raccolta di dati in tempo reale sul traffico, prevista dall'Art. 20 della stessa Convenzione; essendo considerata una possibile invasione della sfera della *privacy*, suddetta raccolta può essere limitata a discrezione dello Stato membro, tramite apposita riserva di legge che indichi gli specifici reati verso i quali non sarà possibile usufruirne. Per l'esercizio di questa facoltà è, tuttavia, posta una condizione: «purché l'ambito di tali reati o categorie di reato non sia più ristretto di quello dei reati ai quali la Parte applica le misure di cui all'articolo 21».

La norma cardine è l'Articolo 23 della Convenzione, rubricato «Principi generali relativi alla cooperazione internazionale». Il Consiglio d'Europa si è qui posto l'obbiettivo di estendere i rapporti di cooperazione ed agevolare lo scambio della c.d. *digital evidence*[75].

L'Articolo in questione contiene tre principi generali: la cooperazione deve essere favorita «nella misura più ampia possibile», richiedendo alle Parti di ridurre al minimo gli ostacoli alla collaborazione internazionale; la cooperazione deve essere poi estesa a tutti i reati relativi a dati o sistemi informatici, quindi non solo reati commessi mediante lo strumento informatico, ma anche reati c.d. "ordinari", rispetto ai quali acquistano rilevanza prove elettroniche; infine, lo scambio di informazioni, a norma della Convenzione, deve avvenire comunque nel rispetto dei trattati internazionali in materia penale, nonché delle norme e dei regolamenti propri degli ordinamenti interni, sancendo il principio secondo il quale le disposizioni della Convenzione non devono sostituire quelle degli altri strumenti internazionali[76].

In conclusione di questa breve analisi della Convenzione di Budapest, resta da segnalare la grande diffusione che ha avuto, non solo tra i membri del Consiglio d'Europa, ma anche tra numerosi Stati esterni all'organizzazione, come previsto dall'Articolo 36, inserito nel Capitolo IV, destinato alle disposizioni finali: esso sancisce infatti che «la Convenzione è aperta alla firma degli Stati membri del Consiglio d'Europa e degli Stati non membri che hanno partecipato alla sua elaborazione»[77].

È sicuramente corretto affermare che la presente Convenzione sia uno strumento di guida e un modello di normativa per tutta la comunità internazionale; la sua influenza non si è limitata agli Stati che hanno ratificato il documento, e ciò trova conferma in un recente sondaggio, terminato nel febbraio del 2020, che ha evidenziato come molti Stati, non firmatari, si sono dotati di adeguate normative

[75] Per esaustiva trattazione dell'argomento si veda VACIAGO, *Digital evidence e libertà fondamentali*, in *Nexa Center for Internet & Society*, 2012; l'Autore definisce in apertura la *digital evidence* come «una qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale».
[76] Sul tema v ARENA, *La Convenzione di Budapest del Consiglio d'Europa*, op. cit., 41.
[77] Ad oggi gli Stati firmatari sono 68, 65 dei quali hanno proceduto alla ratifica, e di questi solamente 45 sono membri del Consiglio d'Europa

in materia di criminalità informatica, prendendo a modello proprio la Convenzione di Budapest[78].

Una ragione di questa così ampia fortuna del documento del Consiglio d'Europa − che si è avuto già modo di segnalare − è sicuramente la flessibilità e la capacità adattiva dello stesso. Il Comitato della convenzione sulla criminalità informatica, che rappresenta le Parti firmatarie della Convenzione, ha progressivamente emanato diverse linee guida − nel dettaglio 12 − a contenuto definitorio e descrittivo delle principali e complesse forme di manifestazione delle condotte criminose informatiche tipiche, con lo scopo di semplificare e incentivare l'attuazione e l'effettivo uso della Convenzione da parte degli Stati firmatari[79].

La diretta conseguenza della ratifica della Convenzione sulla criminalità informatica da parte dello Stato italiano, è stata l'emanazione della Legge 48/2008, con cui si è dato seguito alle disposizioni imposte dal Consiglio d'Europa, riformando parzialmente, seppur in maniera significativa, la disciplina precedente dei reati informatici, come si avrà modo di analizzare nelle pagine che seguiranno.

3.2. Unione Europea: Decisione Quadro 2005/221/GAI e Direttiva UE 2013/40

L'Unione Europea ha da sempre avvertito la necessità di offrire soluzioni alle sfide che la c.d. "rivoluzione digitale"[80] ha portato. Difatti l'attenzione dell'UE alle questioni ed alle problematiche attinenti alla *cyber security* non è mai venuta meno e l'obbiettivo generale, in linea con l'ideologia dell'Organizzazione, è stato, sin dall'inizio, quello di realizzare un *cyberspace* aperto e sicuro, per contribuire a creare una maggiore fiducia dei cittadini negli strumenti e nei servizi digitali.

Recentemente l'Unione, per il tramite delle sue Istituzioni, ha avuto modo di esprimere, nuovamente, i punti focali della propria linea rispetto alla sicurezza

[78] I dati del sondaggio sono riportati in *The Budapest Convention on Cybercrime: benefits and impact in practice*, in *https://www.coe.int/it/web/portal/home*

[79] Le 12 linee guida sono consultabili presso la pagina *web* del Consiglio d'Europa, *https://www.coe.int/en/web/cybercrime/guidance-notes.*

[80] Voce RIVOLUZIONE DIGITALE in *Enciclopedia Treccani online*, «*La grande trasformazione della società conseguente all'adozione di strumenti digitali di calcolo automatico*» *https://www.treccani.it/enciclopedia/rivoluzione-digitale.*

informatica, affermando che «la *cyber security* è parte integrante della sicurezza degli europei. [...] i cittadini devono avere la garanzia di essere protetti dalle minacce informatiche. L'economia, la democrazia e la società dell'UE dipendono [...] da strumenti digitali e connettività sicuri e affidabili. La *cyber*-sicurezza è quindi fondamentale per creare un'Europa digitale, verde e resiliente»[81].

Il quadro normativo a supporto della strategia della *cyber security* dell'Unione Europea si articola in numerose norme sia di portata generale che specifiche e settoriali[82].

Con particolare riguardo alla criminalità informatica, filo conduttore della presente analisi, si può affermare, in via introduttiva, che anche l'UE ha recepito la necessità di offrire una risposta chiara al crescente allarmismo della comunità internazionale, dovuto al fenomeno dei *cyber-crimes* − in linea con quanto si è già avuto modo di evidenziare nei paragrafi precedenti. Di conseguenza, consapevole delle potenzialità offensive derivanti da un'uso distorto di *internet*, il Consiglio dell'Unione Europea, in rappresentanza degli Stati membri adotta, come primo atto volto ad arginare la diffusione delle pratiche dei *cyber-crimes*, la Decisione Quadro 2005/222/GAI del febbraio 2005.

Si tratta di un atto giuridico che si inserisce nella fase storica dell'Unione precedente al trattato di Lisbona[83]; il quadro istituzionale di riferimento consisteva

[81] Premessa alla relazione congiunta della Commissione UE e l'Alto rappresentante dell'Unione per gli affari esteri di presentazione della nuova strategia dell'Unione Europea in materia di *cyber security*, 2020. si specifica l'obbiettivo che si pone l'Organizzazione, quello cioè di «rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e garantire a tutti i cittadini e imprese di poter beneficiare appieno di servizi e strumenti digitali sicuri e affidabili»; cfr. GIUSTI, *Strategia UE per la cyber security e armonizzazione normativa: obiettivi e possibili conflitti*, in *Cybersecurity360*, 2022, *https://www.cybersecurity360.it/legal/strategia-ue-per-la-cyber-security-e-armonizzazione-normativa-obiettivi-e-possibili-conflitti/.*

[82] Come evidenziato da un parere del Garante per la protezione dei dati europeo (EDPS); cfr. TARSITANO, *Sicurezza comune europea, positivi gli impatti sulla protezione dei dati personali: il parere EDPS*, in *Cybersecurity360*, 2022, *https://www.cybersecurity360.it/legal/privacy-dati-personali/sicurezza-comune-europea-positivi-gli-impatti-sulla-protezione-dei-dati-personali-il-parere-edps/.*

[83] Noto anche come trattato di riforma, viene firmato a Lisbona nel dicembre 2007 ed entra ufficialmente in vigore nel medesimo mese del 2009. Modifica il Trattato sull'Unione Europea (TUE) e il Trattato che istituisce la Comunità Europea, che diventerà da quel momento il Trattato sul Funzionamento dell'Unione Europea (TFUE), riformando in maniera sensibile l'assetto istituzionale e giuridico dell'Organizzazione.

ancora in quello introdotto dal trattato di Maastricht[84], in cui la "cooperazione di polizia e giudiziaria in materia penale" costituivano il c.d. "terzo pilastro"[85].

La decisione quadro 2002/222 è, difatti, espressione del "metodo intergovernativo", proprio delle materie non delegate dagli Stati membri all'esclusiva competenza dell'UE − non potendo quindi utilizzare gli strumenti ed i meccanismi istituzionali tipici previsti dai trattati, propri dell'opposto "metodo comunitario" − ma perseguite mediante una collaborazione a livello, per l'appunto, intergovernativo, utilizzando come principale strumento, nonché unico effettivamente vincolante, quello della convenzione internazionale − sebbene poi la gestione veniva affidata agli stessi organi comunitari − salvo la possibilità di "comunitarizzare" la procedura[86].

A livello contenutistico, la decisione quadro oggetto di analisi contiene un ristretto numero di articoli − nel dettaglio 13 − nei quali vengono brevemente e genericamente descritte tre ipotesi delittuose, rispetto alle quali gli Stati membri hanno dovuto adottare necessarie misure punitive e preventive[87], nonché una serie

[84] Firmato nel febbraio 1992, anche noto come trattato sull'Unione Europea, istituisce la Comunità Europea e, più specificatamente, il "sistema dei 3 pilastri".

[85] Il "sistema dei 3 pilastri" costituiva il modello di organizzazione istituzionale delle competenze dell'Unione Europea prima dell'entrata in vigore del trattato di Lisbona. Questo quadro venne introdotto dal trattato di Maastricht, e poi successivamente modificato dal trattato di Amsterdam. Consisteva nell'individuazione di 3 aree che si differenziavano per i poteri che i trattati attribuivano all'Unione per disciplinare le singole competenze. Il primo "pilastro" era costituito dalle Comunità europee, nel cui quadro le competenze erano state interamente deferite dagli Stati membri all'Unione, ed esercitate direttamente dalle Istituzioni dell'Organizzazione; il secondo ed il terzo "pilastro" erano, rispettivamente, "politica estera e di sicurezza comune (PESC), e "cooperazione nei settori di giustizia e affari interni" (GAI), rispetto ai quali era prevista una cooperazione intergovernativa, che si avvaleva delle istituzioni comuni, usufruendo di determinati strumenti sovranazionali, come la Commissione o i pareri del Parlamento europeo. Per approfondimenti sul tema si veda SOKOLSKA, *I trattati di Maastricht e di Amsterdam*, in *https://www.europarl.europa.eu/factsheets/it/sheet/3/the-maastricht-and-amsterdam-treaties;* si veda anche DANIELE, *Diritto dell'Unione Europea*, 6ª ed., 2018, Milano, 26.

[86] Per approfondimento si rimanda a *Metodo intergovernativo*, in *Dizionari Simone*, *https://dizionari.simone.it/11/metodo-intergovernativo.* Si segnala che la procedura di "comunitarizzazione" delle materie disciplinate nell'ambito della cooperazione intergovernativa, attraverso il meccanismo noto come "passerella comunitaria", permetteva di applicare i meccanismi tipici del metodo comunitario; per potersi eseguire suddetta procedura, prevista dall'Art 40 TUE, si richiedeva l'iniziativa della Commissione o di uno stato membro, la consultazione del Parlamento europeo e la delibera unanime del Consiglio. La decisine Quadro 2002/222 rientra in questa ipotesi procedurale; v. *Comunitarizzazione*, in *Dizionari Simone, https://dizionari.simone.it/11/comunitarizzazione*.

[87] Dopo un primo articolo dedicato alle definizioni utili, sono previsti: "accesso illeciti a sistemi di informazione", "interferenza illecita per quanto riguarda i sistemi" e "interferenza illecita per quanto riguarda i dati"; *Artt. 2, 3, 4 Decisione Quadro 2002/222/GAI*

di disposizioni generiche relative a suddetti delitti, contenenti profili di diritto penale sostanziale e processuale[88].

Con l'entrata in vigore del Trattato di Lisbona la situazione dell'Unione Europea relativa al riparto delle competenze muta considerevolmente[89]. Prendendo a riferimento il diritto penale, esso non rientra tra le materie di competenza − esclusiva o concorrente − dell'Unione; la regola generale prevede che il diritto penale resti, infatti, nella sfera di sovranità nazionale degli Stati.

Tuttavia l'ordinamento dell'UE ha previsto ipotesi derogatorie alla regola appena affermata, individuando, quindi, circostanze in cui, a determinate condizioni e con specifiche limitazioni[90], attraverso la procedura ordinaria, «Il Parlamento europeo e il Consiglio [...] possono stabilire norme minime relative alla definizione dei reati e delle sanzioni»[91]. Viene così attribuito all'Unione il potere, mediante direttiva, di dettare disposizioni generali minime per sfere di criminalità particolarmente gravi e che, per loro natura, presentano dimensioni transnazionali. Il comma 1 dell'art 83 TFUE, oltre che affermare quanto appena detto, provvede anche alla tassativa elencazione delle suddette sfere di criminalità, tra le quali si inserisce, per quanto interessa al fine di questa trattazione, la criminalità informatica.

È proprio in ragione di questa competenza penale c.d. "accessoria"[92] che il Parlamento europeo e il Consiglio dell'Unione Europea, nell'agosto del 2013 adottano la direttiva 2013/40/UE, che sostituisce la decisione quadro 2002/222/GAI, relativa agli attacchi contro i sistemi di informazione. È corretto segnalare in via preliminare che gli obblighi di incriminazione enunciati dal testo del provvedimento in esame ricalcano i reati introdotti dal legislatore italiano nel 1993 e nel 2008[93].

---

[88] Sono norme relative a circostanze aggravanti, sanzioni, responsabilità delle persone giuridiche e competenza; *Decisione Quadro 2002/222/GAI*.
[89] Per esaustiva trattazione si veda DANIELE, *Diritto dell'Unione Europea* op. cit., 421 ss.
[90] Per approfondimento della questione si rimanda a DE MATTEIS, *L'articolo 83 TFUE e la competenza dell'Unione in materia di diritto penale sostanziale*, in *Diritto Penale sostanziale e processuale dell'Unione Europea*, volume 1, 2011, Padova.
[91] *Art. 83, co. 1, Trattato sul Funzionamento dell'Unione Europea.*
[92] Sul punto si veda BERNARDI, *La competenza penale accessoria dell'Unione Europea: problemi e prospettive*, in *Diritto Penale Contemporaneo*, 2012.
[93] Vedi *infra* par 3.3.

Come si evince in maniera esplicita nella proposta di direttiva del Parlamento europeo e del Consiglio dell'Unione, il presupposto imprescindibile che venne assunto per la costruzione di questo provvedimento faceva leva sulla natura ultrastatuale del fenomeno dei *cyber-crimes*, avvertendo la conseguente necessità di armonizzare le discipline penalistiche sostanziali e processuali nazionali, e la creazione di un sistema di «effettiva cooperazione e scambio sicuro di informazioni tra gli Stati membri sugli incidenti e i rischi a carico della SRI»[94].

In questo caso il legislatore comunitario ha voluto delineare un sistema di prevenzione e gestione del rischio di commissione dei reati informatici, richiedendo il contributo degli "operatori del mercato" e delle pubbliche amministrazioni. La proposta di direttiva punta a creare un sistema gerarchico piramidale per lo scambio di informazioni sensibili tra le autorità competenti, costituendo il fulcro del sistema di prevenzione del *cybercrime* a livello dell'Unione[95].

Al vertice del sistema si pone la Commissione, punto di raccordo tra le varie Autorità nazionali competenti in materia di *cyber*-sicurezza; ad essa è attribuito il potere di delineare periodicamente, attraverso specifici atti di esecuzione, un piano di collaborazione dell'Unione Europea in materia di sicurezza delle reti e dell'informazione (anche solamente SRI), e viene investita della facoltà di concludere accordi internazionali con Stati terzi o altre organizzazioni, per permettere il coordinamento o la partecipazione ad attività di collaborazione per la sicurezza della rete − come previsto dall'art. 13 della proposta di direttiva.

Gli interlocutori della Commissione sono le Autorità nazionali, competenti in materia di sicurezza informatica e delle reti, che − a norma dell'art. 14 della proposta di direttiva − vengono investiti di poteri-doveri di controllo sull'adozione di «misure tecniche e organizzative adeguate alla gestione dei rischi che corre la sicurezza delle reti, e dei sistemi informativi di cui hanno il controllo e che usano

[94] Relazione introduttiva alla proposta di direttiva COM (2013) 48 final - 2013/27 (COD), sulla sicurezza delle reti e delle informazioni.

[95] Sul punto si rimanda a BIGOTTI, *La sicurezza informatica come bene comune. Implicazioni penalistiche e di politica criminale*, in FLOR, FALCINELLI, MARCOLINI (a cura di), *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di* Internet, in *Lab. Per. Dir. Pen*., 2014, 109.

nelle loro operazioni»[96], da parte degli "operatori di mercato", cioè le pubbliche amministrazioni e le imprese che si occupano di fornire i servizi dell'informazione[97].

La già citata dottrina descrive la struttura delineata dalla presente direttiva come basata su un modello preventivo fondato su «una sorta di autoregolamentazione regolata», in cui la Legge impone agli stessi attori che agiscono sul mercato virtuale di dotarsi di regole da osservare[98]. In questo quadro la Commissione avrà il compito di uniformare e coordinare il panorama Comunitario delle prescrizioni a contenuto cautelare; le Autorità nazionali svolgeranno, invece, tra le altre cose, il compito di assicurarsi il corretto adempimento delle prescrizioni indirizzate agli operatori.

Il grande contributo della direttiva 2013/40/UE consiste proprio nella creazione dell'appena descritta rete di collaborazione, oltre alla riformulazione degli obblighi di incriminazione già contenuti, e qui sostituiti, dalla Decisione Quadro 2005/222/GAI, rispetto ai quali si è poc'anzi avuto modo di sottolineare l'effettiva e precedente introduzione nel nostro ordinamento penale.

Per concludere la breve analisi del panorama di tutele e cautele in materia di *Cybersecurity* dell'Unione Europea, resta da segnalare la creazione, sempre nel 2013, dell'*European Cybercrime Center* (EC3), all'interno dell'EUROPL. Si tratta di un'unità specializzata, fondata per rafforzare la risposta delle forze dell'ordine al *cybercrime*. Si occupa di coordinare le attività transfrontaliere delle forze dell'ordine contro il crimine informatico, e contestualmente svolge il compito di centro di competenza tecnica in materia[99].

---

[96] Art. 14, par. 1, proposta di direttiva COM (2013) 48 final - 2013/27 (COD).

[97] L'Allegato II della proposta di direttiva si occupa di specificare quali siano i soggetti qualificati "operatori di mercato", attraverso un'analitica elencazione per individuarne l'ambito di operatività.

[98] V. BIGOTTI, *La sicurezza informatica come bene comune* op. cit., 110.

[99] Nel corso degli anni ha subito sensibili modifiche volte ad adattarsi alla specificità dei crimini informatici, creando nuove e più dettagliate funzioni. Oggi l'EC3 si concentra principalmente in 3 aree: "reati informatici commessi da gruppi della criminalità organizzata", "crimini informatici che causano gravi danni alle loro vittime" e "crimini informatici che colpiscono infrastrutture critiche e sistemi informativi dell'Unione". Per approfondimento si veda STEFANI, *European Cybercrime Center: come lavora e di cosa si occupa il centro europeo per il cybercrime*, in *Cybersecurity360*, 2021, *https://www.cybersecurity360.it/cybersecurity-nazionale/european-cybercrime-centre-come-lavora-e-di-cosa-si-occupa-il-centro-europeo-per-il-cyber-crime/*.

3.3. Disciplina nazionale: dalla prassi giurisprudenziale all'attuale normativa: Legge 3 dicembre 1993 n. 547 e Legge 18 marzo 2008 n. 48

Come si è avuto modo di segnalare in apertura del presente paragrafo, l'*iter* di introduzione ed evoluzione della disciplina nazionale in materia di reati informatici ha risentito, nelle sue tappe, degli impulsi sovranazionali, derivanti da diversi provvedimenti, con differente forza vincolante, che nelle pagine precedenti si è sinteticamente analizzato.

Le principali fonti legislative che hanno introdotto prima, e sensibilmente modificato poi, il panorama normativo relativo ai reati informatici sono due: la Legge 3 dicembre 1993 n. 547, di modificazione e integrazione alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, e la Legge 18 marzo 2008 n. 48, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

In entrambi i casi il legislatore italiano ha recepito le disposizioni contenute in specifici provvedimenti derivanti dalle organizzazioni internazionali che, nel corso del tempo, si sono sensibilizzate alla questione dei *cyber-crimes*, offrendo una, quanto più possibile, immediata risposta alle esigenze di tutela rispetto ai beni giuridici, e agli obblighi di criminalizzazione esplicitamente contenuti nelle fonti sovranazionali di riferimento[100].

Prima di procedere all'analisi del contenuto delle suddette norme nazionali, parrebbe opportuno effettuare brevi cenni sulla situazione dell'ordinamento giuridico penale nel periodo immediatamente precedente ad esse, quando cioè non vigeva alcuna disciplina generale relativa ai reati informatici − salvo alcuni interventi legislativi settoriali[101].

Ancor prima della "presa di coscienza" dei legislatori nazionali e sovranazionali, il fenomeno della criminalità informatica aveva assunto dimensioni «preoccupanti»[102]. Pur in mancanza di una normativa generale sui

---

[100] Tra i principali provvedimenti emanati dalle organizzazioni internazionali che sono stati oggetto di analisi nei paragrafi precedenti, è possibile individuare i 2 che sono stati fonte diretta per le norme interne citate: la Raccomandazione R(89)-9 del 1989 da cui discende la Legge 547/1993, e la Convenzione di Budapest, che la Legge 48/2008 ha ratificato ed eseguito. V. *supra* par. 3.1.

[101] Cfr. nota n. 55.

[102] Così lo descriveva già nel 1990 CASO, *sentenza 23 ottobre 1989*, in *Il Foro Italiano: giurisprudenza penale*, vol. 113, II, 1990, 463.

computer crimes, la Corti penali si sono trovate, quindi, a doversi interfacciare con una fenomenologia criminosa avverso la quale non erano stati disposti adeguati strumenti di diritto sostanziale e processuale.

L'approccio adottato della giurisprudenza penale di allora prevedeva l'inquadramento delle condotte *cyber* in fattispecie "tradizionali", attraverso operazioni di interpretazione estensiva delle disposizioni contenute nelle norme già presenti nel codice Rocco.

A titolo esemplificativo, circoscrivendo l'ambito di analisi al delitto di danneggiamento − *ex* art. 635 c.p. − tema centrale del presente elaborato, pare doveroso citare la sentenza del 23 ottobre 1989 pronunciata dalla Pretura di Torino[103].

Oltre ad essere una delle più note sentenze (precedenti all'emanazione di una disciplina generale) che portò alla ribalta un caso di *computer crimes*, il provvedimento giurisprudenziale in parola dimostra efficacemente come gli operatori del diritto, posti di fronte alla necessità di relazionarsi con condotte riconducibili alla sfera informatica, non potevano fare altro che "appoggiarsi" sulle categorie dogmatiche convenzionali, manifestando, tra l'altro, un'evidente difficoltà nel qualificare gli elementi c.d. "*cyber*".

Nel dettaglio, la pretura di Torino, al termine dell'istruttoria, condannò i due imputati del procedimento, rinvenendo gli estremi per la configurazione del delitto di danneggiamento *ex* art. 635 c.p., all'esito di un *iter* logico che, per la dottrina e la giurisprudenza successiva, risulterà sicuramente suscettibile di rilievi critici. Infatti, ciò che ha permesso all'organo giudicante di ritenere sussunto il reato di danneggiamento è l'aver rigettato la tesi, sostenuta dalla difesa, che riscontrava una necessaria scissione tra la componente *hardware* e quella *software*, considerando quest'ultima come elemento riconducibile alla sfera materiale del *computer*[104].

---

[103] Pretura di Torino 23.10.1989, in *Il Foro Italiano: giurisprudenza penale*, vol. 113, II. 1990, 462 ss.

[104] La pretura di Torino, pur cogliendo la suggestione della tesi della difesa che mira a ricondurre il *software* all'immaterialità, appoggiandosi su una precedente dottrina secondo cui per "sistema informativo" si doveva intendere «un connubio indivisibile tra le apparecchiature fisiche (*hardware*) ed i programmi che le utilizzano e specializzano», accogliendo poi la posizione del perito che «non esita a definire il *software* come materiale, pur non manipolabile con gli usuali strumenti», afferma che «le modifiche di un programma possono esser considerate sia come

Difatti la pretura conclude con l'identificazione di una "violenza sulle cose" in un caso di mera cancellazione dei c.d. "codici sorgente" e l'apposizione di una "protezione a tempo" su alcuni *software*. A tale conclusione questa giurisprudenza arriva muovendo dall'assunto che ogni alterazione di programmi o dati informatici causa un'invalidazione strutturale o funzionale alla componente *hardware* di un *computer*[105].

L'interpretazione dell'art. 635 c.p., come eseguita dalla giurisprudenza nel caso in esame, pur ritenendola ancora accettabile nel caso di un'alterazione logica di dati e programmi, contenuti in un supporto magnetico fisico, che cagioni il danneggiamento o la manomissione del supporto stesso, incontra degli evidenti limiti nei casi di danneggiamento di dati in trasmissione, vale a dire non "incorporati", neanche momentaneamente, in un *device* fisico. La difficoltà che emerge in maniera chiara è quella di non poter, in questo caso, ricondurre i dati informatici nella nozione materiale di "cose"[106].

Si intuiscono quindi, in modo chiaro, le ragioni che hanno alimentato in Italia, ma anche in molti altri ordinamenti nazionali e sovranazionali, la richiesta di adottare una adeguata disciplina generale in materia di *cyber-crimes*. La prima risposta alla suddetta richiesta arrivò dal Comitato dei Ministri degli stati membri del Consiglio d'Europa che, nel 1989, approvò la Raccomandazione n. R (89)-9, provvedimento che si è già avuto modo di analizzare[107].

A seguito delle raccomandazioni contenute nel documento del Consiglio d'Europa, viene emanata la Legge 3 dicembre 1993 n. 547, di modificazione e integrazione alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, inserendo, per la prima volta nel nostro ordinamento giuridico, una normativa specifica avente a riguardo i *computer crimes*.

Il legislatore con la legge 547/93 ha introdotto nuove fattispecie criminose, inserendole all'interno del codice penale, effettuando la preliminare scelta di non

---

alterazioni materiali che come cambiamenti strutturali alla prestazione di un sistema»; cfr. CASO, *Sentenza 23 ottobre 1989* cit.

[105] Sul punto si veda anche SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici, un bilancio poco esaltante*, in *Riv. it. dir. proc. pen.*, 2012, 204 ss.

[106] Per approfondimento si richiama SALVADORI, *Il "microsistema" normativo* op. cit., 206.

[107] Vedi *supra* par. 3.1.

considerare i reati informatici come aggressivi di nuovi beni giuridici, ma legandoli a quelli tutelati dalle norme preesistenti[108].

A livello contenutistico, è possibile individuare cinque categorie distinte di reati, rispetto alle quali vengono modificate o aggiunte norme nel codice penale e nel codice di procedura penale, in perfetta adesione con la "lista minima" di fattispecie contenuta nella Raccomandazione R(89)-9. Le categorie in questione sono: aggressioni alla riservatezza dei dati e delle comunicazioni informatiche, aggressioni alle integrità dei dati e dei sistemi informatici, condotte in tema di falso, estese anche ai documenti informatici e le frodi informatiche[109].

Lo *step* successivo della legislazione nazionale concernente la disciplina generale dei reati informatici avviene con l'approvazione della Legge 18 marzo 2008 n. 48, di ratifica ed esecuzione della convenzione del Consiglio d'Europa sulla criminalità informatica. Anche in questo caso, l'intervento del legislatore nazionale arriva in adempimento di obblighi scaturenti da fonti sovranazionali, nella fattispecie la Convenzione di Budapest, della quale si è già avuto modo di parlare[110].

Come si è detto *supra*, il lavoro preparatorio della Convenzione era stato improntato alla realizzazione di un'armonizzazione delle normative in materia di *cybercrime*, ma anche e soprattutto alla creazione di un sistema di cooperazione

---

[108] Sul punto si veda OBIZZI, *I reati commessi su Internet: computer crimes e cybercrimes*, in *https://www.fog.it/corsoinformatica/reati.htm*, 2009; VERDE, *I reati informatici*, in *Diritto.it*, 2020, *https://www.diritto.it/i-reati-informatici/*.

[109] Nel dettaglio la legge 547/93: modifica l'art. 392 c.p., aggiungendovi un comma, estendendo la punibilità per "l'esercizio arbitrario delle proprie ragioni con violenza su cose" anche nel caso di modifica, alterazione o cancellazione di un programma informatico; sostituisce integralmente l'art, 420 c.p., rubricato "attentato a impianti di pubblica utilità", estendendo la punibilità anche a chi commette un fatto diretto a danneggiare sistemi informatici o telematici di pubblica utilità; sostituisce il quarto comma dell'art. 616 c.p. includendovi la corrispondenza mediante strumenti informatici; aggiunge un comma all'art. 621 c.p., estendendo la nozione di documento anche a quelli aventi natura informatica; inserisce *ex novo* i seguenti articoli: art. 491 *bis* c.p. "documenti informatici", art. 615 *ter* c.p. "Accesso abusivo a un sistema informatico o telematico", art. 615 *quater* c.p. "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici", art. 615 *quinquies* c.p. "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico", art. 617 *quater* c.p. "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche", art. 617 *quinquies* c.p. "Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche", art. 617 *sexies* c.p. "Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche", art. 635 *bis* c.p. "Danneggiamento di sistemi informatici e telematici", art. 640 *ter* c.p. "Frode informatica". In riferimento al codice di procedura penale, vengono modificati gli artt. 266 e 268 c.p.p. Per tali modifiche si vedano gli *Artt. 1-13 L. 547/93*.

[110] Vedi *supra* par. 3.1.

internazionale; per questo motivo la Legge 48/08 interviene in maniera più consistente sugli aspetti processualpenalistici e sulle procedure di cooperazione tra gli Stati e le organizzazioni internazionali, apportando solo poche, seppur significative, modifiche all'assetto normativo sostanziale costituito dalla precedente legge 547/93[111].

Volgendo l'attenzione sul sistema dei delitti di danneggiamento informatico è sicuramente utile sottolineare che la disciplina ad oggi in vigore, che sarà oggetto di approfondita analisi nei capitoli successivi[112], è quella che emerge dalla legge 48/08, che all'art. 5, capo II, apporta modifiche al Titolo XII Libro II del codice penale[113].

Meritevole di autonoma segnalazione è l'art. 7, capo II, della medesima legge, il quale dispone modifiche al d.lgs. 231/2001, inserendo l'art. 24 *bis*, che integra l'elenco dei reati presupposto per la disciplina della responsabilità amministrativa dell'ente dipendente da reato, mediante l'inserimento dei reati informatici, indicati esplicitamente dal comma I dello stesso articolo[114].

Il capo III della legge 48/08 è, invece, integralmente dedicato alle numerose modifiche apportate al codice di procedura penale, nel perseguire l'obbiettivo di creare un sistema di collaborazione internazionale e di scambio di informazioni, tra gli Stati firmatari della Convenzione di Budapest, incidendo, inoltre, sulla c.d. "*digital forencis*"[115]. Le tre *macro* aree di attività delle suddette modifiche possono essere così categorizzate: i mezzi di ricerca delle prove, acquisizione, conservazione e trasmissione dei dati informatici, e la competenza distrettuale[116].

---

[111] Analisi condivisa da OBIZZI, *I reati commessi su Internet* op. cit.
[112] Vedi *infra* cap. 2 e cap. 3.
[113] L'intero capo II della legge 48/08 è dedicato alle modifiche apportate al codice penale. Le norme modificate, oltre i delitti di danneggiamento informatico, sono: l'art. 492 *bis* c.p., che subisce sensibili modifiche, gli artt. 495 *bis* e 640 *quinquies* c.p., aggiunti *ex novo* e l'art. 420 c.p., a cui vengono abrogati il secondo ed il terzo comma. Cfr. *artt. 3-6, cap. II legge 48/08*
[114] Cfr. nota n. 14; si rimanda anche a *infra* cap. 4, par 2.
[115] Per una completa ed approfondita analisi delle modifiche all'impianto processualepenalistico operate dalla legge 48/08 si veda MAIOLI, SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, in *Altalex*, 2012, *https://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008*.
[116] Così si esprime sul tema CALICE, *Le principali modifiche introdotte con la Legge 18.3.2008 n. 48 di ratifica ed esecuzione della Convenzione europea sulla criminalità informatica*, in *http://www.distretto.torino.giustizia.it/documentazione/D_1967.pdf*, 2008, 9 ss.

Per concludere la presente ricostruzione dell'evoluzione normativa nazionale in materia di reati informatici si effettuano brevi cenni ai cambiamenti derivanti dal d.lgs. 22 gennaio 2016 n. 7, riguardante disposizioni in materia di abrogazione di reati e introduzione di illeciti con sanzioni pecuniarie civili.

Il decreto in parola, tra le numerose modifiche che apporta all'ordinamento penale, aggiunge alcune disposizioni al c.d. "microsistema" normativo dei delitti di danneggiamento informatico. Viene aggiunto a ciascuno degli artt. 635 *bis* - 635 *quinquies* c.p. l'aggravante per il fatto commesso «con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema»[117].

In conclusione, si può affermare che l'attività del legislatore di costruire un adeguato sistema generale di tutela e repressione dei *cyber-crimes*, in adempimento degli impulsi sovranazionali, è in continuo e progressivo sviluppo. Le legislazioni devono costantemente adeguarsi ad un sistema criminoso basato sulla incessante ed inarrestabile innovazione delle tecnologie informatiche e virtuali, che mai quanto oggi hanno pervaso la vita della società, a tutti i livelli possibili − tanto per gli enti pubblici o privati, nella loro attività, di qualsiasi dimensione, quanto per i singoli utenti privati. I bilanci che periodicamente vengono realizzati a livello nazionale e internazionale dimostrano che il numero di reati informatici commessi sia in continuo aumento[118]. In questo senso, si deve riconoscere lo sforzo del legislatore di fornirvi una, quanto più possibile, efficace risposta normativa.

[117] Artt. 635 *bis* e 635 *quater*, comma 2, c.p., artt. 635 *ter* e 635 *quinquies*, comma 3, c.p., come modificati dal d.lgs. 22 gennaio 2016 n. 7.

[118] Secondo un'indagine del *Sole24ore*, solo nei primi 6 mesi del 2021 sono stati commessi 136 mila ca. reati informatici, contro le 113 mila ca. del 2020. Cfr. FABBRI, *L'indagine "indice di criminalità 2021"*, in *CybersecurityItalia*, *https://www.cybersecitalia.it/cyber-crimine-800-reati-informatici-al-giorno-in-italia-nel-2021-soprattutto-nelle-citta-del-nord/14871/*.

CAPITOLO II

DANNEGGIAMENTO DI DATI E SISTEMI INFORMATICI PRIVATI

1. Le nuove disposizioni dei delitti contro l'integrità di dati e sistemi informatici "privati": gli artt. 635-*bis* e 635-*quater* c.p.

Per il tramite della legge 48/2008 l'ordinamento italiano ha recepito, ratificato ed eseguito le disposizioni contenute nella Convenzione del Consiglio d'Europa sulla criminalità informatica, adeguando le norme interne agli *standard* identificati dagli obblighi pattizi assunti in sede internazionale[1]. Nelle pagine precedenti si è ricostruito l'*iter* evolutivo della normativa dei *cybercimes* che ha avuto come punto di arrivo la creazione di una disciplina di diritto penale, sostanziale e processuale, in materia di reati informatici. Nel prosieguo del presente elaborato si circoscriverà l'analisi ad un gruppo di fattispecie penali che vengono comunemente etichettate e definite dalla dottrina penalistica come il "sistema dei delitti di danneggiamento informatico"[2].

Si tratta di un gruppo composto da quattro norme, contenute nel codice penale − artt. 635 *bis*, *ter*, *quater* e *quinquies* c.p. − costruite a partire dalla fattispecie "tradizionale" codificata dall'art. 635 c.p. − reato di danneggiamento − ed evolutesi nel corso del sopracitato *iter* normativo di impulso sovranazionale. Difatti l'art. 635 *bis* c.p., rubricato, al tempo, come "danneggiamento di sistemi informatici e telematici"[3], venne inserito nel primo grande intervento di riforma, relativamente ai *cybercrimes*, del codice penale che, come disciplinato della legge 547/1993[4], ha introdotto nell'ordinamento la categoria dei reati informatici; invece, la definitiva introduzione del c.d. "microsistema" composto dalle quattro norme oggetto di esame, avvenne solamente con la ratifica della Convenzione di Budapest, in occasione dell'emanazione della legge 48/2008.

Il legislatore del tempo dovette colmare un vuoto di tutela manifestatosi nel corso degli anni precedenti, rispetto al susseguirsi di episodi, sempre più frequenti, di danneggiamento informatico, giacché l'ordinamento era del tutto

[1] V. *supra* Cap. I, par 3.1, par 3.3.
[2] Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit.
[3] Così indicato dall'art. 9 legge 1993/547 che introduce l'art. 635 *bis* c.p.
[4] V. *supra* Cap I, par. 3.3.

sprovvisto di norme penali *ad hoc*; la conseguente unica opzione possibile era quella di applicare, attraverso l'interpretazione estensiva, le norme dei delitti comuni − segnatamente il danneggiamento *ex* art. 635 c.p. − al fine di inquadrare tali fenomeni in fattispecie positivizzate nell'ordinamento[5].

La norma introdotta dalla legge 547/1993 delineava una fattispecie chiaramente modellata sulla struttura del tradizionale delitto di danneggiamento *ex* art. 635 c.p.[6], colmando così, seppur parzialmente, il vuoto normativo e concedendo la possibilità di inquadrare le diverse condotte di danneggiamento informatico in una fattispecie specificamente dedicata ad esse[7].

Con la ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, avvenuta, si ricorda, con la legge 48/2008, l'art. 635 *bis* c.p. è stato oggetto di riordino; ne è conseguito l'ampliamento del numero e della complessità e completezza delle norme dedicate ai reati contro l'integrità dei dati, programmi e sistemi informatici e telematici e, quindi, la creazione del già citato "microsistema dei delitti di danneggiamento informatico".

---

[5] Tale analisi è condivisa da diversi autori e riscontrabili in numerosi contributi, su tutti: SALVADORI, *"microsistema" normativo concernente i danneggiamenti informatici* cit., 205; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, Milano, 2019, pp 762 ss.

[6] L'art. 635 *bis* precedente la riforma che ha dato seguito alla Convenzione di Budapest, infatti, prevedeva sia le modalità di esecuzione della condotta sostanzialmente identici alla fattispecie "tradizionale", sia il trattamento sanzionatorio che, seppur più grave, ricalcava quello delle ipotesi di danneggiamento aggravato, con la sola sensibile differenza di individuare un oggetto materiale c.d. "speciale", cioè sistemi, programmi o dati informatici, che comunque, in via interpretativa, venivano fatti ricadere nel 635 c.p. Si può segnalare come il legislatore abbia comunque voluto risolvere i dubbi allora esistenti circa la possibilità di sussumere i dati e i programmi nell'ambito delle *res materiales* per scongiurare l'eventuale inapplicabilità del 635 c.p. ai casi di danneggiamento di beni immateriali. Per approfondimento si veda a LEONE, *Il nuovo danneggiamento informatico*, in *Cyberspazio e Diritto*, Vol. 11, n. 1, 2010, 213.

[7] La sostanziale trasposizione del "danneggiamento semplice" *ex* art. 635 c.p. nella nuova fattispecie di "danneggiamento informatico" ha determinato il sorgere di una questione circa il rapporto tra le due norme, anche e soprattutto in considerazione del fatto che la giurisprudenza antecedente la riforma del 1993 aveva già esteso in via ermeneutica l'oggetto materiale anche ai dati ed ai programmi per l'elaboratore, si veda Pretura di Torino, sentenza 23 ottobre 1983. La relazione allo schema del disegno di legge della riforma del 1993 ha espresso che la norma introdotta e codificata all'art. 635 *bis* c.p. si dovesse porre «in rapporto di specialità con la comune fattispecie di danneggiamento, salva la sussistenza di un più grave reato» cfr. MINISTERO DI GRAZIA E GIUSTIZIA, *Schema di disegno di legge contenente modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*: *relazione*, atto Camera 2773, 1993; a riguardo si sono pronunciate le Sezioni Unite, affermando che tra le due norme sussistesse un rapporto di successione di leggi penali nel tempo, disciplinato dall'art. 2 c.p., in ragione della già affermata posizione giurisprudenziale che, prima della riforma del 1993, aveva esteso l'operatività del 635 c.p. alle condotte strettamente informatiche, v. Cass. pen., Sez. Un., 9.10.1996, n. 1282; per approfondimento sul tema si rimanda a LEONE, *Il nuovo danneggiamento informatico* cit., 212 s.

Le ragioni che hanno spinto il legislatore ad individuare più fattispecie risiedono, da una parte nel necessario adeguamento della normativa interna agli obblighi assunti in sede internazionale, dall'altra nella volontà, condivisa dalla dottrina e raccolta dal legislatore nazionale, di fornire una quanto più possibile ampia tutela avverso le numerose e diverse forme di attacchi informatici[8]; la strategia normativa adottata ha determinato la diversificazione delle singole fattispecie sulla base di elementi specializzanti che caratterizzano, di volta in volta, il fatto tipico.

La prima distinzione, operata dal legislatore del 2008, pervenne direttamente dalle disposizioni contenute nella Convenzione di Budapest[9]: rispetto a quanto precedentemente previsto dalla raccomandazione R(89) 9 (la quale ha determinato l'adozione del primo "pacchetto di norme" relativo ai *cybercrimes* nell'ordinamento giuridico nazionale[10]) la Convenzione del 2001 ha diversificato la tutela richiesta dai paesi firmatari rispetto agli attentati rivolti contro − non più solamente − l'integrità dei sistemi, ma anche l'integrità dei dati e programmi informatici[11].

Il legislatore nazionale, tuttavia, non si è limitato a recepire la suddetta istanza, ma ha apportato un'ulteriore distinzione nel comparto di norme penali riguardante i delitti di danneggiamento informatico, distinguendo tra i delitti avverso dati o sistemi informatici c.d. "privati"[12], e quelli avverso dati o sistemi informatici di pubblica utilità[13].

---

[8] V. *supra* Cap. I par 2.

[9] Si vedano gli artt. 4 e 5, *Convenzione del Consiglio d'Europa sulla criminalità informatica*, 2001, Budapest.

[10] V. *supra* Cap I, par. 3.1.

[11] Si vuole segnalare, in breve, la scelta del legislatore di non ratificare l'art. 1 della Convenzione nella legge 48/2008, il quale contiene l'insieme di definizioni tecniche funzionali all'applicazione della Convenzione stessa. Con riguardo ai delitti di danneggiamento informatico, l'art. 1 trascura il "sistema telematico", includendo invece, e concentrandosi, sul "sistema informatico"; la ragione di questa scelta della Convenzione può riconoscersi nella definizione di "sistema informatico" che viene fornita, cioè «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati», perfettamente in grado di includere il "sistema telematico", per tale intendendosi un gruppo di apparecchiature interconnesse tra loro. La scelta, invece, del legislatore italiano di non vincolarsi alle definizioni offerte dall'art. 1 della Convenzione, in particolare per la definizione positiva offerta in riferimento al "sistema informatico", può giustificarsi per il non volere incorrere nel ristretto limite del principio di tassatività. A riguardo si veda a LEONE, *Il nuovo danneggiamento informatico* cit., 218.

[12] Artt. 635 *bis*, *quater* c.p.

[13] Artt. 635 *ter*, *quinquies* c.p.

La trattazione delle norme in parola non può non tenere conto delle suddette distinzioni e categorizzazioni. Per economia descrittiva e per ragioni di chiarezza sistematica, anziché analizzare singolarmente ed in successione le norme che compongono il c.d. "sistema" dei delitti di danneggiamento informatico, di cui agli artt. 635 *bis* c.p. e seguenti, è diffuso in dottrina − e il presente elaborato vi si uniforma − il metodo di trattazione che vede divise le norme in due coppie, accomunate non dalla differenza dell'oggetto materiale, quanto, piuttosto, divise dalla titolarità privatistica o qualifica pubblicistica dello stesso, che, come vedremo, sembrerebbero avere più incisività sulla struttura generale delle fattispecie[14].

Per questo motivo le pagine che seguiranno prenderanno ad oggetto l'art. 635 *bis* c.p., rubricato danneggiamento di informazioni dati e programmi informatici, e l'art. 635 *quater* c.p., rubricato danneggiamento di sistemi informatici o telematici, cioè i delitti contro l'integrità di dati e sistemi informatici c.d. "privati"[15].

2. Soggetto attivo e bene giuridico tutelato: tesi tradizionale e tesi moderna

Procedendo ora nell'analisi dettagliata delle fattispecie, la prima questione che deve necessariamente essere affrontata riguarda il bene giuridico oggetto di tutela. A riguardo si segnala, preventivamente, la contrapposizione tra due tesi distinte.

La prima , c.d. tradizionale, diffusasi in dottrina sin dall'introduzione dell'art. 635 *bis* c.p., a seguito della legge 547/1993, si basa sulla collocazione sistematica all'interno del codice penale delle fattispecie − inserite, per l'appunto, nel libro XIII del codice, relativo ai reati contro il patrimonio. I sostenitori[16] ritengono che la norma tuteli il valore patrimoniale di particolari beni informatici

[14] Per approfondimento si veda Cappellini, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 777.
[15] Per l'analisi dei delitti di danneggiamento di dati o sistemi informatici di pubblica utilità si veda *infra* Cap III.
[16] A sostegno della tesi patrimonialista: PICA, *Diritto penale delle tecnologie informatiche*, Milano, 1999, 86 s. secondo l'Autore «l'inquadramento sistematico appare corretto, anche perché non vi è dubbio che la norma vuole offrire tutela al bene informatico sotto il profilo patrimoniale»; più recentemente SCOPINARO, *Internet e reati contro il patrimonio*, Torino, 2007, 206; FIANDACA, MUSCO, *Diritto penale. Parte speciale* cit., 145; ANTOLISEI, *Diritto penale, Parte speciale I*, ed. XVII, Milano, 2022, 604 s.

− dati, informazioni, programmi informatici, sistemi informatici o telematici − individuando, quindi, il bene giuridico nel patrimonio, da intendersi in senso funzionalistico rispetto all'utilità che esso comporta per la persona umana[17].

Autorevole dottrina, a favore della tesi opposta, sostiene che in questo modo si sia sopravvalutata la posizione sistematica delle norme nel codice, ignorando che, per determinare il bene giuridico tutelato da una norma, nel rapporto tra il "titolo", "sezione" o "capo" e il testo normativo, bisogna far prevalere sempre quest'ultimo, per la vincolatività e la maggiore ricchezza descrittiva[18]. L'«intitolato non è che uno dei criteri a disposizione dell'interprete per confermare, ma non per fondare, quanto si è ricavato dall'interpretazione del testo normativo»[19]. Il vincolo per l'interprete risiede nel fatto tipico e non nella locazione sistematica all'interno del codice.

In questo modo, sembrerebbe opportuno orientarsi verso la tesi c.d. moderna, che, concentrandosi sul testo normativo, in particolar modo valorizzando «l'irriducibile specificità»[20] dell'oggetto passivo delle condotte e delle modalità aggressive di queste fattispecie, rispetto a quelle "tradizionali", individua come bene giuridico tutelato dagli artt. 635 *bis* e *quater* c.p. l'integrità dei dati, programmi e sistemi informatici[21].

---

[17] Sul punto si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 777.

[18] Per approfondimento sul tema cfr. SALVADORI, *"microsistema" normativo concernente i danneggiamenti informatici* cit., 238.

[19] Così ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, 13.

[20] Cosi si esprime CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 777.

[21] A sostegno si segnalano: PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di internet*, Milano, 2004, 70 s; l'Autore, pur inserendosi in un periodo che ancora non aveva visto la definitiva evoluzione della normativa in materia di reati informatici, già colse l'emersione di beni giuridici che definisce «nuovi», identificandone due: la riservatezza informatica e l'integrità e sicurezza informatica; quanto "all'integrità dei dati", aggiunge, poi, l'autore che questa consisterebbe nella «pronta e corretta utilizzabilità dei nuovi mezzi informatici [...] prima ancora ed, anzi, indipendentemente dal fatto che si abbia poi la lesione di altri più tradizionali beni giuridici, che restano sullo sfondo». Anche SALVADORI, *"microsistema" normativo concernente i danneggiamenti informatici* cit., 238. In questo caso l'Autore richiama le disquisizioni da lui effettuate circa i fatti tipici dei delitti di danneggiamento informatico e, in particolare, l'intangibilità dell'elaboratore, per escludere la rilevanza del patrimonio come bene giuridico tutelato − il quale indirizzerebbe la tutela delle norme esclusivamente verso il diretto proprietario degli oggetti materiali o immateriali su cui agisce il soggetto attivo − sostenendo invece la rilevanza dell'integrità e la disponibilità dei dati e dei sistemi informatici, che fanno capo a una cerchia più ampia di interessati.

Una parte della dottrina sostiene, infatti, che i delitti di danneggiamento informatico, pur non rappresentando la disciplina nella sua interezza, possono considerarsi come «l'asse portante» dei reati contro l'integrità dei dati, programmi e sistemi informatici, nonché della certamente più ampia categoria dei *computer crimes*, o anche, reati informatici c.d. "propri", ovvero quelli in cui l'elaboratore risulta essere l'oggetto dell'illecito, in mancanza del quale il fatto non si potrebbe considerare penalmente rilevante ai sensi degli artt. 635 *bis* o *quater* c.p.[22].

Per quanto riguarda, invece, il soggetto attivo, le norme si qualificano entrambe come reati comuni, potendo, quindi, essere commessi da "chiunque".

3. Gli oggetti materiali: dati, informazioni e programmi informatici

Volgendo ora l'attenzione della presente analisi normativa verso l'oggetto materiale del reato, vale a dire l'entità su cui ricade materialmente la condotta criminosa del soggetto agente, è necessario effettuare una premessa: quello dell'oggetto materiale è il profilo su cui si impernia la distinzione tra le due fattispecie in analisi, richiedendosi, quindi, necessariamente, di proseguire la trattazione su due binari separati.

Prima ancora, però, di addentrarsi nel tema in questione, si può segnalare un ulteriore profilo introduttivo, generico e condiviso da tutti i reati che compongono il "microsistema" dei delitti di danneggiamento informatico. A differenza dei danneggiamenti "ordinari", gli oggetti materiali delle c.d. "varianti informatiche" possono essere non soltanto le componenti *hardware*, cioè gli elementi strettamente fisici o materiali, come elaboratori, periferiche o memorie informatiche, ma anche le componenti "immateriali", i *software*, per l'appunto dati o programmi[23].

Proseguendo nella trattazione, si evidenzia come nell'originaria formulazione dell'art. 635 *bis* c.p. la ripartizione tra dati, programmi, informazioni e sistemi informatici o telematici era già presente, sebbene effettuata all'interno

[22] Così CADOPPI, CANESTRARI, MANNA, PAPA, *Diritto Penale*, tomo III, Milano, 2022, 7160.
[23] Per approfondimento CADOPPI, CANESTRARI, MANNA, PAPA, *Diritto Penale* cit. 7162.

del testo della norma[24]; il legislatore del 2008, recependo le istanze della Convenzione di Budapest, ha riformulato e diversificato le fattispecie.

Per quanto attiene all'art. 635 *bis* c.p., la norma identifica, alternativamente "informazioni", "dati" e "programmi" informatici. La distinzione parrebbe da subito complessa, giacché da una preliminare osservazione i concetti sembrerebbero, in parte, sovrapporsi. Si aggiunge poi che tale partizione non perviene dalla necessità di ottemperare agli obblighi internazionali: la Convenzione sul *cybercrime*, infatti, fornisce una sola definizione, unitaria e onnicomprensiva, quella di «dati informatici», rilevante per la fattispecie in esame[25]. Il legislatore, nel riformulare l'articolo in parola, ha preferito, tuttavia, mantenere la tripartizione già presente nella previgente disciplina.

Volendo fornire una definizione per ciascuno dei tre concetti espressi dalla norma, parrebbe conveniente partire da quella di "programma", di più agevole individuazione. Seguendo le definizioni provenienti da ambiti strettamente tecnici, è un "programma" la serie di istruzioni espresse in un linguaggio comprensibile dall'elaboratore, progettate al fine di ottenere o eseguire specifiche prestazioni[26]. Tale nozione risulta, tra l'altro, in linea con la concezione "funzionalistica" di programma − pur formalmente ricondotta alla definizione di «dati informatici» − desumibile dalla Convenzione sul *cybercrime*[27].

Maggiori difficoltà, invece, suscitano le nozioni di "dati" e "informazioni", specialmente rispetto alla loro distinzione, dal momento che, sulla base della definizione della Convenzione, ma anche secondo il linguaggio comune, parrebbero totalmente sovrapponibili. La dottrina maggioritaria, per attribuire un

[24] Nella sua prima introduzione, avvenuta con la legge 547/1993, l'art. 635 *bis* c.p. recitava «Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni».

[25] L' art. 1 lett. b) della Convenzione del Consiglio d'Europa sulla criminalità informatica definisce i «dati informatici» come «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione».

[26] Sul punto cfr. PICA, *Diritto penale delle tecnologie informatiche* cit., 26; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit, 778.

[27] Altra autorevole dottrina non esita, tuttavia, a definire pleonastica la definizione in parola «essendo questi [i programmi] costituiti da un insieme di coordinate di dati, attraverso i quali l'elaboratore è in grado di operare»; l'Autore impernia la riflessione sulla funzionalizzazione del concetto di "programma" rispetto alla prestazione dell'elaboratore informatico di «coordinate di dati», e quindi già assorbita nel concetto "base" di dati. Sul punto cfr. MANTOVANI, *Diritto penale. Parte speciale II*, ed. VIII, Milano, 2022, 150.

significato autonomo a ciascuno di questi concetti, individua nel "dato" «l'unità definitoria base, intendendolo come una qualunque rappresentazione di un fatto, espressa in linguaggio comprensibile all'elaboratore, priva di interpretazioni»[28], in altre parole un'unità informativa grezza. Nell'"informazione", invece, si ravvisa una rete di dati organizzati secondo una logica che permette all'utente del sistema informatico di attribuire loro un determinato significato[29].

Secondo tale impostazione i concetti riportati dall'art. 635 *bis* c.p. sarebbero posti in una progressione di complessità, che muove dal concetto base di "dati", che si aggregano e si combinano funzionalisticamente rispetto all'utente nell'"informazione" e rispetto all'elaboratore nel "programma". Il suddetto indirizzo avrebbe il pregio di rispettare il *dictum* legislativo, conformandosi comunque alla *ratio* della norma, che ricerca l'onnicomprensività della tutela rispetto a possibili lacune «tipiche in queste branche moderne di norme incriminatrici»[30].

Un'opzione interpretativa difforme rispetto a quanto fin qui espresso è riscontrabile in autorevole dottrina che, oltre a considerare la menzione dei "programmi" un pleonasmo, seppur «opportuna per eliminare dubbi e incertezze», riconduce il concetto di "informazione" a ciò che è incorporato in un supporto fisico-materiale, che presenti un legame funzionale con un sistema informatico, tale per cui il suo danneggiamento ne pregiudichi il funzionamento[31].

Tale orientamento è stato oggetto di numerose critiche per la sua tendenza ad un'eccessiva dilatazione delle possibilità di incriminazione, fino al punto di ricomprendere qualsiasi "scritto" destinato ad un trattamento di tipo informatico, con il conseguente e possibile «travolgimento del bene giuridico e della ratio della norma»[32].

---

[28] Definizione recuperata da CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 779. Si veda anche MANTOVANI, *Diritto penale. Parte speciale II* cit., 150.
[29] Si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 779; PICA, *Diritto penale delle tecnologie informatiche* cit., 26.
[30] V. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 779.
[31] Così cfr. MANTOVANI, *Diritto penale. Parte speciale II* cit. 150. L'autore specifica, a titolo esemplificativo, di intendere per "informazioni" «tutto il materiale informativo destinato ad essere elaborato dal computer».
[32] Così CORRIAS LUCENTE, *Commento all'art. 5*, in CORASANITI, CORRIAS LUCENTE (a cura di), *Cybercrime, responsabilità degli enti e prova digitale: commento alla Legge 18 marzo 2008, n.*

Analizzando l'oggetto materiale del reato *ex* art. 635 *bis* c.p., si può affermare che, in mancanza di un'esplicita previsione normativa, si dovrebbe ritenere che "dati", "informazioni" e "programmi" non debbano necessariamente essere presenti nella memoria interna di un *device*, attribuendo rilievo anche al loro danneggiamento ove memorizzati in un supporto esterno, finanche nel caso di dati c.d. "in transito", cioè durante la trasmissione da un elaboratore all'altro.

3.1. ... (segue) I sistemi informatici e telematici

Prendendo ora in considerazione l'oggetto materiale previsto dall'art. 635 *quater* c.p. si può osservare sin da subito che esso si riconduce al concetto unitario di "sistemi", declinato poi nel binomio qualificante "informatici" o "telematici".

Il legislatore italiano, in questo caso, si uniforma in maniera coerente con le previsioni della Convenzione del Consiglio d'Europa in materia di reati informatici[33]; l'art. 1, lett. a), prevede proprio la definizione di «sistema informatico», articolandola come «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati»[34].

La dottrina sembrerebbe non dubitare del fatto che il termine "sistema" debba riferirsi alle componenti *hardware*[35], cioè ai dispositivi materiali i quali elaborano dati e informazioni in base alle istruzioni ricevute da un programma

48, Padova, 2009, 140; similmente SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit. 208.

[33] Invero, parrebbe più corretto affermare che è la Convenzione ad essersi uniformata alle previsioni della precedente Raccomandazione del Consiglio d'Europa R(89) 9, la quale già nelle fattispecie della c.d. "lista minima" di reati aveva incluso la nozione di "sistema informatico", difatti già prevista, nel sistema penale italiano, dall'art. 635 *bis* c.p., prima della riforma dettata dalla legge 48/2008. V. *supra* Cap I, par. 3.1.

[34] Traduzione non ufficiale a cura del consigliere dr. Ilarda e del dr. Pasqua del testo ufficiale della Convenzione del Consiglio d'Europa sulla criminalità informatica.

[35] Sul punto si rimanda a PICA, *Diritto penale delle tecnologie informatiche* cit., 24, l'Autore affronta l'interessante problema della distinzione tra un autonomo sistema informatico e una parte di un sistema più grande, quando ad esempio due o più elaboratori si trovino ad interagire via *web* in via integrata, risolvendola nel senso che la qualifica di "sistema" viene assunta dall'*hardware* singolo, in grado di svolgere funzioni di elaborazione autonomamente, indipendentemente dalla connessione con altri sistemi; PECORELLA, *Diritto penale dell'informatica*, Milano, 2006, 188; più recentemente anche CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 780; MANTOVANI, *Diritto penale. Parte speciale II* cit., 156.

informatico[36], rilegando, evidentemente, le componenti immateriali, c.d. *software*, alla disposizione contenuta nell'art. 635 *bis* c.p. − dati, informazioni e programmi informatici. La concezione "fisica" degli oggetti materiali attinenti al fatto tipico del delitto in esame non determina certamente il confine delle aggressioni possibili ai soli casi di danneggiamento materiale, estendendosi anche alle ipotesi di danneggiamento c.d. "logico"[37].

Quanto, poi, alle qualifiche di "informatico" e "telematico": la prima appare una nozione ampia, riferendosi alla capacità del sistema di elaborazione di dati − includendo quindi sia elementi *hardware* che *software* − sostanzialmente connaturata e inscindibile dalla definizione di "sistema", sopra riportata, della Convenzione di Budapest; la seconda viene, in sintesi, intesa come la combinazione della funzione strettamente informatica − di elaborazione dati − con quella telecomunicativa − di trasmissione di informazioni verso l'esterno dell'apparecchio[38].

Invero, parte della dottrina ritiene che la conservazione della dizione "telematico" «piuttosto che frutto di una specifica scelta politico-criminale [...] risulta il relitto del binomio locuzionale "informatico e telematico"»[39], riconoscendovi ormai scarsa autonomia concettuale; questa posizione parte dall'assunto che il contesto tecnologico in cui si operava al momento della prima introduzione della nozione di "sistema telematico", avvenuto con la riforma della legge 547/1993, realizzava *devices* che operavano sostanzialmente "isolati", utilizzando sistemi telematici per comunicare tra loro. La modernità ha portato a una costante connessione della quasi totalità dei sistemi informatici, a *internet* o reti locali, «svolgendo già dunque autonomamente le necessarie funzioni "telematiche"».

[36] Si escludono dal rango di "sistema" comuni apparecchiature o elettrodomestici, quando siano in grado di elaborare ed organizzare dati, rimanendo alla stregua di semplici apparati elettronici. Così CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici* cit., 6.
[37] Sul punto CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 780.
[38] Cosi MANTOVANI, *Diritto penale. Parte speciale II* cit., 156.
[39] In questo modo si esprime CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 781.

3.2. ... (segue) Il nuovo concetto di "altruità"

Rimanendo, ancora, nell'ambito dell'oggetto materiale del fatto tipico, resta da analizzare un elemento comune ad entrambe le fattispecie di reato *ex* artt. 635 *bis* e *quater* c.p., il quale ha generato non pochi problemi interpretativi: la necessaria titolarità dell'oggetto materiale del reato, qualificata da entrambe le norme come «altrui».

Suddetto concetto, tipico delle fattispecie di reato offensive del patrimonio, venne inserito nel corpo della vecchia disposizione dedicata al danneggiamento informatico, introdotta mediante la legge 547/1993, e venne riconfermata nella riformulazione delle due norme di danneggiamento informatico c.d. "private"[40], in questa sede esaminate[41].

Un indirizzo giurisprudenziale[42], sviluppatosi agli albori delle manifestazioni criminose informatiche, escludendo la configurabilità del danneggiamento commesso dal proprietario ai danni del titolare di un diritto di godimento, pareva orientarsi per una pretesa uniformità del concetto di "cosa altrui" in sede civile e penale. Parte della dottrina ha criticato aspramente suddetta impostazione, segnalando come, non solo non cogliesse le peculiarità proprie del settore dell'informatica, ma anche come comportasse un'eccessiva limitazione dell'ambito di applicazione del delitto di danneggiamento informatico; tale dottrina afferma, in aggiunta, che così si arriverebbe «all'erronea conclusione di lasciar privo di tutela penale il meritevole interesse del titolare di un diritto di godimento o di chiunque sia comunque legato da un'effettiva relazione o vincolo

[40] V. *supra* par. 1

[41] Già prima della riforma del 2008, autorevole dottrina segnalava come lo stesso Consiglio d'Europa, nel sollecitare gli Stati ad adottare, tra l'altro, una norma sul danneggiamento di dati, suggeriva di sostituire il riferimento "all'altruità", costituendo tradizionalmente oggetto di proprietà solamente i beni materiali, con l'espressione "senza diritto", in modo da ricomprendere nella norma tutte le azioni di danneggiamento, e non solo quelle perpetrate a danno del diretto proprietario. Cfr. PECORELLA, *Diritto penale dell'informatica* cit., 185.

[42] Cort. App. Pen. 29.11.1990 Vincenti e altro, in *Foroplus*, *https://www.foroplus.it/home.php*. Pur pronunciandosi in un momento in cui non vigeva alcuna norma relativa a fattispecie di reato informatiche, la pronuncia va ricondotta a quella parentesi storica, di cui già si è detto, in cui le prime manifestazioni criminose di danneggiamento informativo venivano ricondotte, mediante interpretazione estensiva, alla fattispecie di danneggiamento *ex* art. 635 c.p. V. *supra* par. 1.

di interesse ai nuovi "oggetti" informatici, rispetto ai danneggiamenti posti in essere dal proprietario»[43].

Le difficoltà interpretative sorgono, poi, in ragione del fatto che, per i delitti di danneggiamento informatico, si passa al riferimento di una *res* immateriale − dati, informazioni etc.− rispetto alla *res* fisica, a cui tipicamente ci si riferisce nelle fattispecie "tradizionali" offensive del patrimonio. I nuovi oggetti "informatici" − immateriali − mancando di fisicità, non possono, quindi, essere oggetto di possesso al pari delle "cose".

Estendendo la questione a tutte le fattispecie di reato c.d. "unilaterale", che prevedono "l'altruità" come attributo dell'oggetto materiale del fatto tipico, autorevole dottrina perviene alla conclusione che, nel procedimento ermeneutico, l'unica funzione che può con certezza essere attribuita a tale concetto è di identificare in negativo le caratteristiche minime della cosa cui si riferisce: essa, infatti, non deve essere di totale ed esclusiva proprietà del soggetto agente né, tantomeno, *nullius* − di nessuno[44].

L'immaterialità dei "nuovi" oggetti informatici e l'impossibilità di rendersi beni di possesso, tuttavia, fa venir meno anche la possibilità di desumere in negativo il concetto di "cosa altrui". In altre parole «si perde il riferimento alla immediata "realità" del concetto di altruità». Ne consegue che il perimetro dei soggetti passivi del reato, aventi diritto alla tutela dell'integrità dei dati, programmi o sistemi informatici, e quindi titolari del diritto di querela *ex* art. 635 *bis*, co. 1, c.p., dovrà essere determinato da una «pluralità di interessi giuridicamente rilevanti»[45].

È evidente come il concetto di "altruità", nell'ambito del diritto penale dell'informatica, vada inteso in senso estensivo, alla stregua di un interesse all'integrità dei dati, programmi, etc., meritevole di tutela penale, riferito a un soggetto diverso dall'agente[46].

---

[43] Così sul punto SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 217. Viene richiamata anche la posizione offerta da PECORELLA, *Diritto penale dell'informatica* cit., 205.

[44] Per approfondimento cfr. MANTOVANI, *Diritto penale. Parte speciale II* cit., 29.

[45] Cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 781.

[46] Cfr. PECORELLA, *Diritto penale dell'informatica* cit., 208. In realtà già rispetto alle "cose" in senso fisico la maggior parte della dottrina intende la nozione di "altruità" in senso estensivo,

Per determinare e delimitare, poi, la sfera dei soggetti "interessati" si può effettuare un richiamo al c.d. codice della *privacy*[47], che definisce con precisione i soggetti «interessati» − art. 4, co. 1, lett. i) − vale a dire coloro ai quali i dati si riferiscono, ma anche i «titolari» − art. 4, co. 1, lett. f) − i «responsabili» − art. 4, co. 1, lett. g) − e gli «incaricati» − art. 4, co. 1, lett. i) − del trattamento dei dati personali, oltre che le più ampie categorie degli «abbonati» − art. 4, co. 2, lett. f) − e degli «utenti» − art. 1, co. 2, lett. g) − cioè soggetti che stipulano un contratto con fornitori di servizi di comunicazione elettronica nonché soggetti che utilizzano suddetti servizi[48]

Ad ogni modo, la conclusione della maggior parte della dottrina, viste le evidenti difficoltà interpretativa che comunque permangono, pur assumendo l'impostazione estensiva della nozione, è quella di sollecitare il legislatore alla sostituzione del termine in parola in favore di una clausola di illiceità espressa − l'agire "senza il diritto" − come, tra l'altro, indicato dalle fonti sovranazionali[49] e recepito dalla maggioranza dei legislatori europei.

4. Le condotte incriminate: definizioni e contenuto

Si volge ora l'attenzione ad un altro elemento proprio del fatto tipico dei reati *ex* artt. 635 *bis* e *quater* c.p., vale a dire le condotte incriminate. Si può affermare in via preliminare che le condotte, rilevanti ai sensi dei citati articoli, risultino in larga parte sovrapponibili, in quanto quelle previste dal delitto di danneggiamento di dati vengono espressamente richiamate nel secondo illecito penale, il quale si "limita" ad aggiungere un numero esiguo di modalità alternative di realizzazione del fatto.

Partendo dall'art. 635 *bis* c.p., l'originario testo introdotto dalla l. 547/1993, come già affermato, fu modellato sulla figura del tradizionale reato di danneggiamento *ex* art. 635 c.p., richiamando le condotte *ivi* previste del

creando una "rete" di situazioni giuridiche protette che, muovendosi in ambito informatico, e quindi, immateriale, è destinata ad ampliarsi. Così MANTOVANI, *Diritto penale. Parte speciale II* cit., 33 s.

[47] D.lgs. n. 196 del 2003, comunemente noto come "codice in materia di protezione dei dati personali" o anche "codice della "*privacy*".

[48] Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 217 s.

[49] Artt. 4 e 5 Convenzione del Consiglio d'Europa sul *cybercrime* e artt. 3 e 4 decisione quadro 2005/222/GAI. Si veda anche nota n. 41.

«distruggere» e «deteriorare», nonché il «rendere [...] inservibili» dati o sistemi informatici; il legislatore del 2008 optò per la conservazione delle suddette condotte − salvo "l'inservibilità", che venne inserita nel testo dell'art. 635 *quater* c.p.[50] − prevedendone tre aggiuntive − la «cancellazione», la «soppressione» e l'«alterazione» − espressamente menzionate dalla Convenzione di Budapest[51].

Si segnalano a riguardo posizioni critiche in dottrina rispetto all'esecuzione di questa scelta di politica-criminale da parte del legislatore, segnatamente in riferimento alla non totale adesione alle previsioni della Convenzione, la quale indica, oltre alle condotte correttamente aggiunte all'alveo di quelle rilevanti al fine della configurazione dei delitti di danneggiamento informatico, un'ulteriore forma, quella del «damaging»[52] − letteralmente «danneggiamento» − non prevista dall'ordinamento interno. Secondo tali orientamenti sarebbe sembrato più opportuno inserire quella che è la formula di sintesi dei delitti di danneggiamento, usata nelle rubriche degli articoli e comprensiva delle diverse condotte alternative[53].

Passando al riempire di significato i termini utilizzati dalla disposizione, l'orientamento più seguito distingue tra aggressioni materiali tradizionali − «distruzione» e determinati casi di «deterioramento» − traendo tali concetti dalla tradizione interpretativa consolidatasi attorno all'art. 635 c.p., e condotte di danneggiamento informatico in senso stretto − «cancellazione», «alterazione» «soppressione» e gli altri casi di «deterioramento»[54].

---

[50] V. *infra* par. 4.1.

[51] In ragione dell'ampio numero di condotte ad oggi incluse, parte della dottrina riconosce da parte del legislatore uno "spiccato *horror vacui*" rispetto a possibili lacune di tutela, che si esprime in una «pletora ridondante di modalità d'azione alternative atte ad integrare la fattispecie». Cfr CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 783.

[52] Art. 4 Convenzione del Consiglio d'Europa sulla criminalità informatica.

[53] Così si esprimono SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 209; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 783; l'Autore prova a giustificare tale scelta del legislatore in ragione della sostituzione del «*damaging*» con la «distruzione», forma già presente nell' originaria formulazione dell'art. 635 *bis* c.p.; MANTOVANI, *Diritto penale. Parte speciale II* cit., 150.

[54] Si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 784. L'Autore specifica che tale divisione si giustifica in ragione del fatto che le aggressioni c.d. "logiche" agirebbero direttamente sui dati o informazioni, mentre gli attacchi materiali pregiudicherebbero i *software* in via mediata, agendo cioè fisicamente e direttamente sulle componenti *hardware* in cui sono incorporati. Le diverse letture secondo le quali tutte e cinque le condotte *ex* art. 635 *bis* c.p. debbano essere interpretate come "aggressioni logiche" incappano nel probabile errore di «confondere l'immaterialità degli oggetti materiali [...] con la supposta necessità di immaterialità delle aggressioni, confinando il danneggiamento informatico di tipo

In altre parole si vuole affermare che, fin quando le ipotesi di danneggiamento, seppur inquadrate negli artt. 635 *bis* o *quater* c.p., e quindi classificabili come "informatiche", hanno ad oggetto beni informatici materiali, le condotte andranno interpretate secondo l'elaborazione derivante dall'art. 635 c.p.; viceversa, laddove l'oggetto del reato risulti essere immateriale, l'interpretazione dovrebbe essere adeguata alle nuove modalità di aggressione[55].

Ad ogni modo, si intende per «distruzione» l'eliminazione di dati, definitiva ed irreversibile, totale o parziale, attraverso l'annientamento del supporto fisico in cui sono incorporati[56].

Ci si riferisce, invece, al «deteriorare» intendendo la diminuzione, sensibile ed apprezzabile, della funzione strumentale dell'oggetto materiale, con conseguente decremento del valore o dell'utilizzabilità, operata attraverso interventi pregiudizievoli sui supporti materiali − in tal caso si parlerà di deterioramento materiale − oppure sui dati o programmi − riferendosi al deterioramento logico[57].

In dottrina si intende, invece, per «alterazione» una qualsiasi modificazione dell'essenza strutturale del dato, programma o informazione, ottenuta mediante la manipolazione, totale o parziale, delle istruzioni che vi sono contenute, con perdita, totale o parziale, della sua funzionalità originaria[58].

Parrebbe riscontrarsi una potenziale sovrapposizione tra le condotte di "deterioramento logico" con quelle di "alterazione" o, quantomeno, una attiguità delle prime rispetto alle seconde, in quanto la limitazione dell'accessibilità o

---

fisico-tradizionale al solo sabotaggio di sistemi [*ex.* Art. 635 *quater* c.p.], aventi natura di *hardware*». Al contrario è ben possibile, secondo l'autore, individuare danneggiamenti informatici materiali, inquadrabili nella norma espressa dall' art. 635 *bis* c.p., ogni qual volta che il *software*, cioè l'oggetto materiale del reato, sia inserito in un supporto esterno ad un sistema.

[55] Sul punto si rimanda a MANTOVANI, *Diritto penale. Parte speciale II* cit., 150.

[56] Si segue a linea interpretativa tracciata da CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 784; MANTOVANI, *Diritto penale. Parte speciale II* cit., 151.

[57] Per approfondimento cfr. CORRIAS LUCENTE, *Commento all'art. 5* cit., 135; MANTOVANI, *Diritto penale. Parte speciale II* cit., 151.

[58] Si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 786; MANTOVANI, *Diritto penale. Parte speciale II* cit., 151. L'Autore afferma che è possibile includere nelle condotte di alterazione anche la "modificazione" dei dati o programmi, non prevista dall'art. 635 *bis* c.p. ma inclusa nell'art. 392, co. 3, c.p. − rubricato «Esercizio arbitrario delle proprie ragioni con violenza sulle cose», il quale prevede al terzo comma l'ipotesi di violenza su un programma informatico − e dalla Convenzione di Budapest, art. 4, assunta nel significato ivi attribuito di rendere il dato o il programma diverso, in tutto o in parte, senza però modificare la sua originale funzione.

fruibilità dei dati è tendenzialmente conseguente alla manipolazione degli stessi − ipotesi che viene solitamente ricondotta, nella sua interezza, ad operazioni di «alterazione», «privilegiando la nota modale piuttosto che la perdita di utilità»[59].

Di conseguenza i fatti rilevanti come "deterioramento logico" sembrerebbero limitarsi alle sole ipotesi di diminuzione di accessibilità o funzionalità dei dati, senza che ne sia intaccata l'integrità effettiva. Secondo la dottrina che ha rilevato la questione in esame, il deterioramento logico potrebbe essere considerato − fuori dai casi riassorbiti nell'«alterazione» − come ipotesi sostitutiva della vecchia espressione di chiusura, del rendere «in tutto o in parte inservibili», del vecchio art. 635 *bis* c.p.[60].

La «cancellazione», ipotesi più frequente, consiste nella distruzione, totale o parziale, dei dati o programmi, attraverso la smagnetizzazione del supporto fisico, la sostituzione di dati originari con dati nuovi o diversi, l'imposizione all'elaboratore di un comando, o anche mediante l'inserimento di un *virus*, in grado di determinare la cancellazione dei dati stessi[61].

Per quanto riguarda l'ultima ipotesi di condotta contenuta nel testo dell'art. 635 *bis* c.p., la «soppressione», non pare agevole individuarne un'autonoma portata applicativa, giacché sembra condividere con la «cancellazione» il comune significato di aggressione logica volta all'eliminazione definitiva di dati o programmi[62].

Sono riscontrabili in dottrina diversi tentativi di tracciare un confine tra le due condotte. Una prima posizione ricondurrebbe alla «soppressione» condotte di eliminazione definitiva di dati, ovvero anche la procurata inaccessibilità, seppur temporanea, agli stessi, mentre la «cancellazione» consisterebbe nel rendere completamente e definitivamente irriconoscibile il contenuto degli stessi mediante

---

[59] Così cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 785.

[60] Si rimanda per approfondimento a CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 785.

[61] Cfr, MANTOVANI, *Diritto penale. Parte speciale II* cit., 151. L'Autore aggiunge che, nell'originaria formulazione dell'art. 635 *bis* c.p., non essendo prevista la "cancellazione", pur rimanendo la più frequente delle modalità aggressive, veniva ricondotta nelle ipotesi di «distruzione»; essendo poi stata integrata nel nuovo dettato del 635 *bis* c.p., si è determinata la diminuzione della portata applicativa della «distruzione», residuando ormai solo per le ipotesi di annientamento materiale dei supporti fisici.

[62] Sul punto v. MANTOVANI, *Diritto penale. Parte speciale II* cit., 151.

aggressione del supporto fisico in cui sono contenuti, oppure per mezzo di operazioni logiche, quali formattazione o sovrascrizione[63].

Altra dottrina riconduce, invece, la condotta di «cancellazione» all'aggressione informatica delle sole informazioni, quella di «distruzione» alle aggressioni logiche a dati e programmi, mentre la «soppressione» indicherebbe la rimozione permanente di dati, informazioni o programmi, agendo sui relativi supporti fisici[64].

Merita senz'altro di essere segnalato uno dei rarissimi interventi della giurisprudenza di merito in materia, proprio riguardo all'interpretazione della nozione di «cancellazione»; la V sezione penale della Suprema Corte specifica che, nel «gergo informatico», l'operazione di cancellazione consiste in una rimozione provvisoria dei dati, da un certo ambiente all'apposito "cestino", oppure in una rimozione definitiva dei dati attraverso lo svuotamento dello stesso. Appare quindi del tutto irrilevante, al fine della configurazione del reato *ex* art. 635 *bis* c.p. per cancellazione, la circostanza che i *files* possano essere recuperati in un secondo momento, mediante specifiche tecniche informatiche[65].

Prendendo ora a riferimento le condotte previste dall'art. 635 *quater* c.p., come si è segnalato in precedenza, esse, in parte, richiamano espressamente quelle disposte dall'art. 635 *bis* c.p., appena esaminate. A queste se ne aggiungono due ulteriori, consistenti nella «introduzione» o «trasmissione di dati, informazioni, o programmi».

Si segnala che le previsioni appena espresse sono state inserite dal legislatore nazionale per adempiere agli obblighi internazionali scaturenti dalla Convenzione di Budapest, segnatamente dall'art. 5, ribaditi successivamente dall'Unione Europea, precisamente dall'art. 3 della decisone quadro 2005/222/GAI[66].

Tali condotte sono previste per colpire ipotesi di danneggiamento logico-informatico, realizzati a distanza, mediante programmi *virus* o altri dati c.d.

---

[63] Posizione espressa da SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 210.
[64] Per approfondimento v. ATERNO, *Le fattispecie di danneggiamento informatico*, in LUPARIA (a cura di) *Sistema penale e criminalità informatica*, Milano, 2009, 49 s.
[65] Cass. pen., sez. V, 18.11.2012, n. 8555, in *Foroplus, https://www.foroplus.it/home.php*.
[66] V. *supra* Cap I, par. 3.2.

"maligni"; ipotesi, queste, già riconducibili all'originario testo dell'art. 635 *bis* c.p., alle condotte di «distruzione» per cancellazione di dati, o anche dell'«inservibilità» del sistema[67].

4.1. Gli eventi dell'art. 635-*quater* c.p.

Prima di affrontare le delicate questioni ermeneutiche relative alla struttura e qualifica delle due fattispecie, nonché sul rapporto tra le condotte, appena descritte, e gli oggetti materiali dei reati[68], ci si soffermerà su un ulteriore elemento proprio del fatto tipico: gli eventi indicati dall'art. 635 *quater* c.p.

In dettaglio, l'articolo in parola prevede esplicitamente quattro eventi: la «distruzione» e il «danneggiamento» di un sistema informatico o telematico, ovvero anche il «renderlo, in tutto o in parte, inservibile», nonché l'«ostacolarne gravemente il funzionamento».

La «distruzione», come anche il «danneggiamento», seguono la tradizione interpretativa consolidatasi attorno all'art. 635 c.p. Nel dettaglio, entrambe le nozioni sembra corrispondano ad un danno cagionato, di tipo fisico-materiale, attraverso modalità che siano anch'esse materiali, cioè perpetrate nei confronti delle componenti *hardware*[69]. Volendo essere ancora più specifici, per «distruzione» si intende un completo e definitivo pregiudizio del sistema informatico o telematico dal punto di vista materiale; per «danneggiamento» si intende, invece, un danno materiale che «menomi ma non annulli del tutto la funzionalità strumentale dello stesso»[70].

L'altra coppia di eventi, invece, sembrerebbe essere riconducibile ad aggressioni logiche-immateriali, che cagionano un danno alle componenti *software*, di tale entità da pregiudicare l'integrità del sistema informatico o telematico.

L'«inservibilità totale o parziale», già prevista nell'originaria formulazione dell'art. 635 *bis* c.p., precedente alla riforma della l. 48/2008, dovrebbe intendersi

---

[67] Così MANTOVANI, *Diritto penale. Parte speciale II* cit., 156 s.
[68] V. *infra* par. 4.2.
[69] Per approfondimento v. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 791.
[70] In questo modo si esprime CAPPELLINI, *ivi*, 791, che richiama la posizione di PECORELLA, *Diritto penale dell'informatica* cit. 193.

come l'inidoneità allo svolgimento della funzione strumentale propria del sistema, cagionata dal soggetto attivo[71]. Si tratta della più tipica ipotesi del delitto in parola, configurandosi nel caso di cancellazione o alterazione dei c.d. "dati di sistema"[72], ovvero anche attraverso la trasmissione di *malware*[73], in grado di bloccare del tutto il funzionamento del sistema.

Da ultimo, «l'ostacolo grave al funzionamento del sistema» costituisce l'ipotesi conclusiva che estende la punibilità del danneggiamento informatico anche ai casi in cui l'aggressione logica cagioni un pregiudizio solo parziale o temporaneo alla funzionalità del sistema[74].

La dottrina che si è espressa sulla questione oggetto della presente analisi, ha accolto favorevolmente la scelta del legislatore di includere quest'ultima ipotesi di evento nell'alveo dell'art. 635 *quater* c.p. − riconducibile all'art. 5 della Convenzione del Consiglio d'Europa in materia di criminalità informatica del 2001 − evidenziando come abbia colmato un vuoto di tutela presente nella precedente normativa. Infatti, è possibile ricondurvi le manifestazioni aggressive informatiche di tipo "funzionale", che rallentino o blocchino, anche solo per un determinato intervallo di tempo, un sistema informatico o telematico[75].

Il riferimento alla «gravità» dell'ostacolo, contenuto anch'esso nelle fonti sovranazionali sopra citate, è frutto della scelta politico-criminale, condivisa dal legislatore nazionale. L'obbiettivo era quello di impedire l'inclusione di condotte dall'offensività limitata rispetto al bene giuridico tutelato, nel campo applicativo di una fattispecie, evidentemente, considerata «di una certa gravità»[76].

---

[71] Per approfondimento cfr. MANTOVANI, *Diritto penale. Parte speciale II* cit., 158.

[72] Noti anche come *File system*, definiti come «sistema di gestione dei file che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di un volume di archiviazione. [...] gestisce [...] tutta l'informazione necessaria per la localizzazione e l'accesso da parte di utenti locali o remoti», in *Enciclopedia Treccani online*, *https://www.treccani.it/enciclopedia/file-system_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/*

[73] V. *supra* Cap I, par. 2.

[74] Così CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 792; MANTOVANI, *Diritto penale. Parte speciale II* cit., 157.

[75] È il caso degli attacchi *Denial of Service*, ovvero *Distributed Denial of Service*, per i quali si rimanda a *supra* Cap I, par. 2. Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 213. Di opinione diversa è invece PECORELLA, *Diritto penale dell'informatica* cit., 219, secondo cui le ipotesi di danneggiamento "funzionale" debbono essere ricondotte alla «inservibilità totale o parziale».

[76] Sul punto si è espresso CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 793.

4.2. Qualificazione delle fattispecie e questioni interpretative

Rispetto al fatto tipico delle norme oggetto di trattazione del presente capitolo, rimangono da affrontare delle questioni relative alla qualifica delle fattispecie.

Avendo riguardo alla norma *ex* art. 635 *bis* c.p., come in più occasioni affermato, la struttura del reato è mutuata da quella del tradizionale delitto di danneggiamento comune − *ex* art. 635 c.p.; di conseguenza, anche rispetto al danneggiamento di dati, informazioni e programmi di privata utilità, è dominante la linea interpretativa secondo cui le descritte condotte incriminate, di realizzazione del fatto, non inquadrano una specifica e vincolante modalità di commissione, quanto piuttosto il risultato naturalistico che ne consegue[77].

In altre parole, la posizione dottrinale dominante afferma che le condotte alternative del «distruggere», «deteriorare», «cancellare», «alterare» e «sopprimere» debbono intendersi come «il cagionare» la distruzione, il deterioramento, la cancellazione, l'alterazione e la soppressione di dati, programmi o informazioni, costituendo in questo modo non le condotte, quanto piuttosto gli eventi del reato[78].

Ne consegue che il delitto *ex* art. 635 *bis* c.p. debba necessariamente essere qualificato come reato di evento, a condotta sostanzialmente libera, causalmente orientata, cioè connessa mediante nesso di causalità, alla realizzazione di un ventaglio di cinque eventi alternativi. Poiché "a forma libera", non si richiede che l'azione del reato si articoli attraverso predeterminate forme o mezzi tipici, ma si caratterizza esclusivamente per la sua causalità diretta dell'evento.

La qualificazione del delitto appena esposta, permette che il reato possa essere posto in essere non solo mediante "un'azione", ma anche mediante "un'omissione", da parte di un soggetto destinatario di un obbligo giuridico di

[77] Rispetto alla dottrina consolidata in riferimento alla qualifica dell'art. 635 c.p. cfr. MANTOVANI, *Danneggiamento e deturpamento di cose altrui*, in *Digesto penale*, III, Torino, 1989, 307; ID, *Diritto penale. Parte speciale II* cit., 137; FIANDACA, MUSCO, *Diritto penale. Parte speciale* cit., 140.

[78] Per tutti si rimanda a SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 209; FIANDACA, MUSCO, *Diritto penale. Parte speciale* cit., 146; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 788; MANTOVANI, *Diritto penale. Parte speciale II* cit., 152.

garanzia. Difatti, l'essere un reato d'evento, causalmente orientato, permette l'equiparazione del «non impedire» l'evento al «cagionarlo», in ragione dell'applicazione dell'art. 40, co. 2, c.p. Come rilevato da parte della dottrina di settore, sarà quindi possibile che il reato in esame si manifesti in forma omissiva c.d. "impropria"[79].

Posto che la qualifica dell'art. 635 *bis* c.p. risulti tutto sommato pacifica e priva di rilevanti complicazioni ermeneutiche, lo stesso non può dirsi in riferimento all'art. 635 *quater* c.p.

La costruzione della disposizione relativa al danneggiamento di sistemi informatici o telematici di privato utilizzo, emerge, da una prima lettura, come fattispecie d'evento, a forma vincolata − potendo commettere l'evento, necessariamente attraverso le condotte previste dal testo della disposizione e già esaminate in precedenza[80].

Ciò che complica le operazioni ermeneutiche è l'apparente sovrapponibilità delle condotte richiamate dell'art. 635 *bis* c.p. con gli eventi specificamente descritti nel prosieguo della disposizione *ex* art. 635 *quater* c.p., con il conseguente «assurdo logico» che si avrebbe l'integrazione del delitto da parte di chi, attraverso le condotte di «distruzione», «deterioramento», ecc., «distrugge, danneggia, rende in tutto o in parte inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento»[81].

Volendo intendere suddetta ripetizione linguistica, determinata dal richiamo all'art. 635 *bis* c.p., come una svista tecnica del legislatore, e proseguendo su tale linea interpretativa, si dovrebbe riconoscere per il delitto di "sabotaggio informatico"[82] la sussistenza di quattro eventi, tra loro alternativi, realizzabili mediante una delle cinque condotte richiamate dal danneggiamento di dati o informazioni, ovvero attraverso le due condotte integrate dal testo dell'art. 635 *quater* c.p., di «introduzione o trasmissione di dati informazioni o programmi».

---

[79] Per approfondire il tema dei reati omissivi "impropri" si rimanda a MANTOVANI, *Diritto penale. Parte generale*, ed. XI, Milano, 2020, 152 ss. FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 631 ss; MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 290 ss.
[80] V. *supra* par. 4.
[81] Così si esprime CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 789.
[82] La dottrina appella in questo modo il reato *ex* art. 635 *quater* c.p.

L'esposta posizione ermeneutica è stata criticata in più sedi dalla dottrina maggioritaria, segnalando come, in questo modo, si finirebbe con il porre tutte le condotte sul medesimo piano, non riuscendo a cogliere la funzione estensiva della punibilità esercitata dalle due espressamente previste dall'art. 635 *quater* c.p. In particolare, l'«introduzione o trasmissione di dati informazioni o programmi» sarebbero facilmente integrabili nella più generica condotta di «alterazione» − *ex* art. 635 *bis* c.p. − laddove si riferisca a sistemi informatici o telematici[83].

Inoltre, l'interpretazione delle condotte (*rectius* eventi) poc'anzi fornita, identificate dal delitto di danneggiamento dei dati, deve necessariamente applicarsi anche al reato di sabotaggio informatico, che ne fa espresso richiamo. In tal modo il quadro ermeneutico della fattispecie si complica considerevolmente. Verrebbe, difatti, dipinta una situazione tale per cui le ipotesi sanzionabili ai sensi dell'art. 635 *quater* c.p. possono alternativamente essere eseguite mediante condotte «inutilmente»[84] vincolate − l'«introduzione o trasmissione di dati informazioni o programmi» − ovvero per il tramite di condotte sostanzialmente libere − come già indicato per il danneggiamento di dati o informazioni − causalmente orientate verso un ampio ventaglio di eventi, da individuare nell'incrocio tra quelli enumerati per il delitto di danneggiamento dei sistemi, e quelli disciplinati dall'art. 635 *bis* c.p.

La soluzione a questa realtà normativa perverrebbe, secondo la dottrina maggioritaria, dal riconoscere che le cinque condotte *ex* art. 635 *bis* c.p. conservano l'oggetto materiale della loro sede originaria, anche nel richiamo effettuato dall'art. 635 *quater* c.p., vale a dire i «dati, le informazioni e i programmi» e non i «sistemi informatici o telematici».

In questo modo, la struttura del delitto di sabotaggio informatico risulterebbe una norma a più fattispecie, e si articolerebbe, principalmente, su uno schema a doppio evento consequenziale − distaccandosi dalla tradizione ermeneutica riguardante il danneggiamento comune − ovvero, in alternativa, come reato d'evento a forma vincolata[85].

---

[83] Per approfondimento cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 790.
[84] Così CAPPELLINI, op. cit., 790.
[85] Opinione condivisa da diversi autori, tra i quali si segnalano SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 210 s.; CAPPELLINI, *I delitti contro*

Nel primo caso, l'evento "intermedio" consiste nella commissione di uno degli eventi tipici descritti dall'art. 635 *bis* c.p., agendo sugli oggetti materiali indicati dalla stessa norma; vi segue un evento c.d. "finale", consistente nel «distruggere», «danneggiare», «rendere in tutto o in parte inservibili» ovvero «ostacolare gravemente il funzionamento» di sistemi informatici o telematici[86].

Nel secondo caso, la fattispecie si integra realizzando uno dei quattro eventi *ex* art. 635 *quater* c.p. mediante una delle due condotte espressamente previste dal dettato della norma di sabotaggio informatico, cioè l'«introduzione o trasmissione di dati informazioni o programmi», le quali hanno come oggetto immediato i sistemi informatici o telematici.

Adottando la linea interpretativa appena esposta si riuscirebbe, non solo, ad individuare una specifica autonomia funzionale delle condotte integrate dall'art. 635 *quater* c.p., ma anche ad inquadrare le due norme di danneggiamento di dati o sistemi "privati", in uno schema di progressione criminosa: laddove, infatti l'offesa che integra il reato *ex* art. 635 *bis* c.p. sia di portata tale da estendere gli effetti lesivi, dal dato o programma singolo, all'intero sistema informatico, cagionando l'ulteriore danno, integrerà anche il delitto *ex* art. 635 *quater* c.p.[87].

4.3. Il *locus commissi delicti*

Un'ulteriore questione che deve, a questo punto, necessariamente essere affrontata attiene alla determinazione del *locus commissi delicti* delle fattispecie di *cyber crime*, segnatamente di danneggiamento informatico.

Essere in grado di attribuire coordinate spaziali ad una determinata ipotesi di reato non è, ovviamente, un'operazione fine a se stessa. Il principio di territorialità è, infatti, posto alla base del sistema di norme che disciplinano l'applicazione della legge penale nello spazio[88] − e quindi la determinazione della

---

l'integrità dei dati, dei programmi e dei sistemi informatici cit., 790; CADOPPI, CANESTRARI, MANNA, PAPA, *Diritto Penale* cit., 7169 s.

[86] Per approfondire maggiormente si rimanda a MANTOVANI, *Diritto penale. Parte speciale II* cit., 157. L'autore distingue anche i due eventi come "evento inferiore" *ex* art. 635 *bis* c.p., e "evento maggiore" *ex* art. 635 *quater* c.p.

[87] Per i discorsi circa il rapporto tra i reati si veda *infra* par. 8.

[88] L'art. 6, co. 1, c.p. afferma il principio secondo cui il reato commesso nel territorio italiano è punito secondo la legge italiana; al co. 2 si prevede 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. Per esaustiva trattazione si rimanda a FIANDACA, MUSCO,

giurisdizione in materia di diritto penale − nonché concorre alla disciplina del sistema di ripartizione della competenza degli organi giurisdizionali[89]. Ebbene, tanto per la giurisdizione, quanto per la competenza, risulta centrale il problema della precisa identificazione del *locus commissi delicti*.

Le ragioni che fanno emergere la necessità di affrontare il tema in questione sono molteplici, e attingono tutte alle peculiarità della materia − la *cyber security* − ovvero delle singole fattispecie che vi appartengono − i *cyber crimes*.

Il primo motivo risiede nella caratteristica mancanza di territorialità, tipica del *cyber*-spazio, di cui si è già avuto modo di parlare[90], rispetto alla quale un'autorevole dottrina si è espressa proprio in commento ad una sentenza della Suprema Corte di Cassazione, chiamata a dirimere una questione circa il *locus commissi delicti* dei reati informatici[91]. L'Autore in questione, oltre a sottolineare la mancanza di limiti territoriali, rileva il superamento della concezione meramente "tecnica" del *cyberspace* e di *internet*, «per abbracciare una dimensione sociologica, basata sulla loro forza riconfigurativa della società e delle esperienze personali degli utenti».

Difatti il *cyberspace* costituisce un ambiente virtuale in rapida e continua espansione, specialmente con l'avvento della nuova dimensione del *cloud* e della struttura del *web*, determinando «delocalizzazione» e «detemporalizzazione» delle attività che possono essere eseguite, programmate se non anche automatizzate.

Il punto di partenza, sicuramente pacifico, della presente riflessione, consiste nel riconoscere ed affermare che *internet*, ed il *cyber-space*, ignorano i confini territoriali.

Posto che il problema, in linea generale, attiene alla disciplina dei *cybercrimes*, è tuttavia possibile escludere determinate categorie di reati informatici che, per loro proprie peculiarità, non recano difficoltà all'interprete nel

---

Diritto penale. Parte generale cit., 139 ss.; MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 169 ss.

[89] L'art. 8 co. 1 c.p.p. recita, infatti, che «la competenza per territorio è determinata dal luogo in cui il reato è stato consumato»; per esaustiva trattazione cfr. TONINI, CONTI, *Manuale di procedura penale*, ed. XXII, Milano, 2021, 75 ss.

[90] V. *supra* Cap I, par. 1.

[91] FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. Proc. Pen*, 2015, 10, 1296 ss., in commento a Cass. Pen., Sez. Un. 24.04.2015, n. 17325.

determinare il *locus commissi delicti*, attraverso la generale disciplina di diritto penale sostanziale[92].

Suddette categorie sono: i reati di evento c.d. naturalistico − così chiamati per distinguerli dai reati di evento c.d. informatico, per i quali, invece si pone il problema oggetto del presente paragrafo − rispetto ai quali la consumazione è legata alla realizzazione del risultato fenomenico ed empirico della condotta; i reati informatici commessi *offline*; i reati omissivi propri, in ragione della connotazione strettamente personale del dovere di ottemperare all'obbligo imposto dalla legge penale. Per tutte le altre categorie di reati informatici, *ivi* inclusi i delitti di danneggiamento di dati o sistemi informatici, è emerso il problema della determinazione del *locus commissi delicti*.

La già citata dottrina riassume le posizioni della giurisprudenza di legittimità, precedenti alle Sezioni Unite n. 17325, che hanno posto un punto alla problematica, offrendo una possibile soluzione interpretativa[93].

Suddette posizioni sono sintetizzabili in due tesi: una prima identifica il *locus commissi delicti* nel luogo dove si ubica la banca dati, cioè ove sono contenuti i dati oggetto della condotta criminosa; ne deriva che l'ubicazione si deve determinare rispetto a dove viene materialmente conservato l'elaboratore su cui sono inserite le informazioni digitali[94]. La seconda tesi, invece, pone rilievo sul luogo ove si trova la postazione remota, o il *server*, da cui il soggetto attivo esegue materialmente la condotta criminosa[95].

Le citate Sezioni Unite, tra le due, segnalano positivamente la seconda tesi per essere stata in grado di superare la concezione classica, strettamente fisica e materiale, del *locus* − nozione, questa, posta alla base della prima teoria − valorizzando le modalità di funzionamento dei sistemi informatici o telematici, tipicamente delocalizzate.

Difatti la Corte rileva come non sia possibile esaurire la complessità dei sistemi informatici nel luogo ove essi sono archiviati, così come non è altrettanto possibile ritenere che i dati informatici si ubichino esclusivamente nel *server*,

[92] Per le principali e maggiormente diffuse classificazioni dei reati informatici si rimanda a *supra* Cap. I, par 2.
[93] Cass. Pen., Sez. Un. 24.04.2015, n. 17325, in *Foroplus*, *https://www.foroplus.it/home.php*.
[94] Cass. Pen., Sez. I, 27.05.2013, n. 40303, *ivi.*
[95] Cass. Pen., Sez. I, ord. 28.10.2014, n. 52575, *ivi.*

poiché «l'intera banca dati sarebbe "ubiquitaria", "circolare" o "diffusa" sul territorio, nonché contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso»[96]. A dimostrazione di ciò viene sottolineato, anche, come le "tracce" delle operazioni compiute nella rete siano rinvenibili, in tutto o in parte, sia sul *server* che presso il *client*.

In conclusione, le Sezioni Unite del 2015 adottano come criterio per l'identificazione del *locus commissi delicti* − e quindi per l'identificazione della giurisdizione penale nazionale, nonché, in quanto compatibile, del giudice naturale competente − il luogo in cui si trova il soggetto che perpetra la condotta delittuosa, affermando, infatti, che il delitto «si determina nel luogo ove viene effettivamente superata la protezione informatica e [...] quindi, dove è materialmente situato il server violato»[97].

La dottrina che riporta la sentenza in commento, non esita ad effettuare rilievi critici alle conclusioni teoriche a cui la Suprema Corte è giunta. Innanzitutto segnala come l'individuazione dell'ubicazione del *client*, cioè del luogo dell'accesso al *server* da cui viene eseguita la condotta, è spesso di particolare difficoltà, se non anche impossibile, per l'uso di *devices* mobili. In secondo luogo, il soggetto attivo potrebbe facilmente sfruttare a suo vantaggio tale principio di diritto per scegliere il Paese da cui far partire l'attacco − c.d. *forum shopping*[98]. Da ultimo, l'Autore riconosce come la soluzione adottata dalla Suprema Corte altro non è che una *fictio* giuridica, considerando che il "protocollo comunicativo" tra *client* e *server* si basa su un'infrastruttura centralizzata, e non unitaria o decentralizzata, come, invece, rileva la Cassazione[99].

---

[96] Così cfr. FLOR, *I limiti del principio di territorialità nel cyberspace* cit., 1299.

[97] Cass. Pen., Sez. Un. 24.04.2015, n. 17325, in *Foroplus*, *https://www.foroplus.it/home.php.* Si segnala che il fatto in questione aveva ad oggetto un'ipotesi di accesso abusivo ad un sistema informatico o telematico *ex* art. 615 *ter* c.p.

[98] Voce FORUM SHOPPING, in *Enciclopedia Treccani online*, «*Fenomeno per cui le parti di una controversia possono di fatto scegliere di incardinare il relativo giudizio di fronte a una delle diverse corti astrattamente competenti a conoscere la materia*», in questo contesto la nozione viene intesa in senso di "abuso" del soggetto attivo, potendo, in astratto, scegliere di perpetrare la condotta da un territorio in cui vige un ordinamento di diritto penale a lui più favorevole, o comunque, preferibile.

[99] Cfr. FLOR, *I limiti del principio di territorialità nel cyberspace* cit., 1302 s.

La soluzione, in alternativa, proposta dalla medesima dottrina, recupera una pronuncia della Corte di Giustizia dell'Unione Europea[100], la quale, in materia di competenza del giudice civile, afferma che «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 amministrazione della giustizia».

La volontà di parte della dottrina penalistica, sarebbe di esportare il principio qui esposto anche nell'ambito del diritto penale, con l'obbiettivo di distaccarsi dalla nozione tradizionale di "ambito territoriale", in favore di un approccio più flessibile, adeguato al *cyberspace*, per l'identificazione del *locus commissi delicti*.[101].

La teoria così elaborata prevede che, al fine di individuare il *locus*, non dovrebbe assumere rilevanza la collocazione fisica del server, ovvero delle infrastrutture logiche o fisiche, bensì il legame tra la persona offesa, l'ambiente informatico ed il bene giuridico protetto, su cui ricadono gli effetti dell'azione; il luogo, quindi, dovrebbe essere identificato dove è avvenuta l'azione − o almeno una parte di essa[102] − vale a dire nell'ubicazione «in cui "si trova" l'area informatica violata[103] che, se non è territorialmente definibile, deve essere individuata tramite il legame con il suo titolare».

Di conseguenza, la competenza dovrebbe essere riconosciuta in capo al giudice del luogo dove la persona offesa detiene il suo centro di interessi[104].

Viene fornito, in questo modo, un criterio ermeneutico che, pur essendo "costruito" sul principio di territorialità, opera in maniera flessibile e modulare,

---

[100] Corte di Giustizia EU, 25.10.2011, (C-509/09, C-161-10), in *eur.lex*, *https://eur-lex.europa.eu/homepage.html.*

[101] Idea centrale nelle riflessioni esposte in FLOR, *I limiti del principio di territorialità nel cyberspace* cit., 1305.

[102] Espressione che richiama apertamente l'art. 9, co. 1, c.p.p., in cui l'autore propone di individuare la fonte normativa *de jure condito* per la soluzione adottata.

[103] Il discorso da cui è colta la citazione della dottrina ruota intorno alla fattispecie di accesso abusivo ad un sistema informatico o telematico *ex* art. 615 *ter* c.p.

[104] Per approfondimento v. FLOR, *I limiti del principio di territorialità nel cyberspace* cit., 1307. L'Autore definisce la sua come "soluzione ermeneutica evolutiva".

valorizzando il sopracitato legame tra persona offesa, ambiente informatico e bene giuridico protetto[105].

5. L'elemento soggettivo, il momento consumativo e il tentativo

Per quanto attiene all'elemento soggettivo dei due delitti in esame, gli artt. 635 *bis* e *quater* c.p. prevedono fattispecie di reato punite a titolo di dolo generico; esso consisterà, nel primo caso, nella coscienza e nella volontà di cagionare la «distruzione», il «deterioramento», la «cancellazione», l'«alterazione» o la «soppressione» di dati, informazioni o programmi informatici; nel secondo caso, di sabotaggio informatico, consisterà nella coscienza e volontà di provocare la «distruzione», il «danneggiamento», l'«inservibilità» ovvero l'«ostacolo grave al funzionamento» di sistemi informatici o telematici[106].

Relativamente alla consumazione, invece, avendo qualificato entrambe le norme come reati d'evento[107], essi si perfezionano nel momento di realizzazione dell'evento stesso. Merita di essere specificato che, nel caso del reato *ex* art. 635 *quater* c.p., data la struttura a doppio evento, si considera realizzata la fattispecie al realizzarsi di quello dannoso per il sistema informatico o telematico[108].

Per entrambe le norme è configurabile il tentativo.

6. Le circostanze aggravanti speciali

Volgendo l'attenzione verso le circostanze aggravanti dei reati in discussione, sembrerebbe opportuno valutarne l'evoluzione, avvenuta parallelamente agli interventi di riforma normativa che hanno influito sul dettato delle disposizioni in questione.

---

[105] Tale principio ermeneutico pare essere, tra l'altro, in linea con le disposizioni contenute nelle fonti sovranazionali, segnatamente l'art. 12, co. 2, direttiva 2013/40/EU che ha sostituito la decisione quadro 205/222/GAI, nella parte in cui prevede assegna competenza giurisdizionale ad uno Stato membro anche nel caso in cui «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»; v. *supra* Cap I, par. 3.2.

[106] Sul punto si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 793; MANTOVANI, *Diritto penale. Parte speciale III* cit., 158.

[107] V. *supra* par. 4.2.

[108] Per utilizzare la terminologia adottata da parte della dottrina, alla realizzazione dell'evento "maggiore"; cfr. MANTOVANI, *Diritto penale. Parte speciale II* cit., 157.

La formulazione dell'unico articolo − anteriormente alla riforma posta in essere dalla l. 48/2008 − dedicato al danneggiamento di dati o sistemi informatici, vale a dire l'art. 635 *bis* c.p., effettuava un indiscriminato richiamo a tutte le circostanze aggravanti speciali previste dalla fattispecie di reato dalla quale era stata mutuata, l'art. 635 c.p. A questo si aggiungeva la previsione di una circostanza espressamente dedicata al danneggiamento informatico, cioè l'ipotesi di commissione del fatto «con abuso della qualità di operatore di sistema».

La dottrina del tempo criticò aspramente il cieco rinvio alla totalità delle aggravanti contenute nel testo del reato di danneggiamento comune, per due ordini di ragioni. Le circostanze richiamate dall'art. 635 c.p., infatti, risultavano sostanzialmente estranee ai fatti descritti dal delitto informatico, riguardando queste beni immobili − «edifici pubblici o destinato ad uso pubblico o di culto» − beni naturali − «piante, viti, boschi, selve, foreste, etc.» − oppure beni la cui rilevanza appariva del tutto marginale[109].

Il rimando, in aggiunta, includeva, inevitabilmente, la circostanza descritta dall'art. 625, n. 7, c.p. − articolo che disciplina le circostanze aggravati alle ipotesi di furto *ex* art. 624 c.p. − a cui faceva espresso ed ulteriore rinvio l'art. 635 c.p.[110]. Per la suddetta circostanza − avente ad oggetto «beni esistenti in uffici o stabilimenti pubblici [...] o destinati al pubblico servizio o pubblica fede» − pur rilevando maggiore pertinenza con la fattispecie di danneggiamento informatico, il verificarsi della situazione assunta ad elemento aggravante avrebbe determinato la riconduzione del fatto nell'ambito di un'altra più grave ipotesi di reato, vale a dire l'art. 420 c.p., dedicato all'«attentato a impianti di pubblica utilità».

Il legislatore del 2008, nel ratificare la Convenzione del Consiglio d'Europa, riformulando ed ampliando, come si è visto, la tutela normativa, offerta dall'ordinamento, alle ipotesi criminali di danneggiamento avverso beni informatici, ha "messo mano" anche al panorama delle circostanze aggravanti, «rimediando»[111] alla situazione che era stata delineata dalla riforma *ex* l.

[109] Così si esprimeva PECORELLA, *Diritto penale dell'informatica* cit., 228.
[110] V. ANTOLISEI, *Diritto penale, Parte speciale I*, ed. XII, Milano, 1999, 426, il quale segnalava l'improprietà del semplice rinvio; appariva critico rispetto alla scelta del legislatore anche PICA, *Diritto penale delle tecnologie informatiche* cit., 94 ss.; più recentemente PECORELLA, *Diritto penale dell'informatica* cit., 228.
[111] Cfr. MANTOVANI, *Diritto penale. Parte speciale II* cit., 153.

547/1993. La soluzione adottata prevedeva, per ciascuna delle quattro norme proprie del "microsistema" dei delitti di danneggiamento informatico, un singolo rinvio ad una circostanza prevista dall'originario art. 635, co. 2, n. 1 c.p., quella relativa alle ipotesi di commissione del fatto «con violenza o minaccia alla persona».

L'attuale situazione normativa perviene dall'ultimo intervento di riforma − seppur lieve − delle fattispecie in esame. Il quadro degli interventi normativi succedutisi in relazione alle norme considerate, qui brevemente ricostruito[112], si conclude con le modifiche introdotte dal d.lgs. n. 7 del 2016 in tema di depenalizzazioni.

Per ciò che attiene alle norme qui analizzate, il decreto in parola ha declassato la fattispecie classica di "danneggiamento comune", prevista dal vecchio testo dell'art. 635 c.p., ad illecito civile, riformulando l'articolo in modo tale che mantenesse rilievo penale, sulla base delle ipotesi che, precedentemente, erano qualificate di "danneggiamento aggravato".

Tale operazione ha determinato la necessità di intervenire anche sul testo delle norme di danneggiamento informatico, le quali, come segnalato, rinviavano, per una delle due circostanze aggravanti previste, proprio al vecchio testo dell'art. 635 c.p. Tuttavia, l'intervento sui quattro delitti sembrerebbe solo apparente, essendosi limitato, il legislatore, a trasfondere testualmente l'aggravante citata direttamente nel testo delle fattispecie, al posto del rinvio, lasciando intatto ed immutato il sostanziale contenuto delle norme in parola[113].

Si passerà, ora, all'analisi delle due circostanze aggravanti speciali previste dagli artt. 635 *bis* e *quater* c.p. − ma anche dagli artt. 635 *ter* e *quinquies* c.p.; la prima prevede un trattamento sanzionatorio più grave nel caso in cui il fatto venga commesso «con violenza alla persona o con minaccia». Le nozioni di violenza personale e minaccia si fondano sulla tradizionale elaborazione penalistica, a cui si rimanda[114].

---

[112] Per approfondita ricostruzione si rimanda a *supra* Cap I, par 3.3.
[113] Per approfondimento si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 776.
[114] Per tutti cfr. FIANDACA, MUSCO, *Diritto penale. Parte speciale, Volume II, Tomo I* cit., 208 ss.; MANTOVANI, *Diritto penale. Parte speciale I* cit., 271 ss.

In questa sede occorre, però, segnalare che il rapporto che deve intercorrere tra la violenza o minaccia e il danneggiamento informatico deve essere strettamente strumentale, vale a dire che le prime dovranno essere funzionali alla realizzazione della condotta di cui al secondo. In tal senso si può configurare la circostanza aggravante sia per le aggressioni materiali sia in riferimento a quelle logiche[115].

La seconda aggravante, prevista sin dalla prima introduzione dell'art. 635 *bis* c.p. e sostanzialmente immutata, consiste nell'aver commesso il fatto «con abuso della qualità di operatore del sistema». La *ratio* della previsione in parola consiste nel riconoscere una posizione di evidente vantaggio del soggetto attivo, determinata dalla qualifica di «operatore del sistema», la quale rileva una condizione "privilegiata" in capo agli "operatori" per maggiori e più concrete possibilità di commissione del danneggiamento. Vista da un'altra prospettiva, si rinviene una maggiore vulnerabilità dei dati, programmi o sistemi informatici, rispetto a tali tipologie di aggressioni[116].

Si è aperto un dibattito ermeneutico in dottrina circa il significato da attribuire alla "qualifica di operatore"; una parte privilegia una lettura sostanzialmente restrittiva, secondo la quale la presente aggravante deve intendersi applicabile soltanto ai c.d. *system administrator* − coloro che, all'interno di un'azienda, detengono il controllo delle diverse fasi del processo di elaborazione dei dati[117] − con il potere, potenzialmente, di accedere a qualsiasi sistema informatico ed operare qualsiasi modifica[118].

---

[115] È da segnalare un'opinione in dottrina, largamente condivisa, che rileva la marginalità dell'aggravante per «violenza o minaccia»; si sostiene che il legislatore non deve aver tenuto conto che la maggioranza degli attacchi all'integrità dei dati o sistemi sia perpetrata a distanza, vale a dire da remoto, per mezzo di reti telematiche, specialmente attraverso *internet*. Così SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 236 s.

[116] Per approfondimento v. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 794.

[117] Cfr. MANTOVANI, *Diritto penale. Parte speciale II* cit., 153.

[118] A sostegno si segnala PECORELLA, *Diritto penale dell'informatica* cit., 122. L'autore afferma, infatti, che «questa circostanza appare particolarmente grave già per la violazione del dovere di fedeltà nei confronti del titolare (o comunque dell'utente) del sistema informatico, sia delle persone i cui interessi economici sono gestiti da quel sistema [...] in questa prospettiva [...] è evidente che non potrà definirsi "operatore di sistema" chiunque» ma solo la particolare figura di tecnico informatico che «all'interno dell'azienda ha l controllo delle diverse fasi del processo di elaborazione dei dati».

Altra posizione, c.d. "intermedia", meno condivisa in dottrina, non richiede che l'operatore sia esclusivamente l'*administrator*, ma ritiene comunque necessaria una qualche specifica tecnica in capo al soggetto attivo[119].

La posizione maggiormente seguita, però, privilegia una lettura particolarmente ampia, secondo cui sarebbe qualificabile come "operatore di sistema" chiunque risulti legittimato a compiere azioni su di esso, anche solo l'addetto all'immissione dei dati[120].

Si segnala, in conclusione, che la giurisprudenza, in occasioni relative comunque ad altre ipotesi di reato informatico, le quali, tuttavia, prevedono la medesima circostanza aggravante, si è dimostrata orientata verso quest'ultima soluzione ermeneutica. Infatti la Seconda Sezione penale della Corte di Cassazione, in una sentenza del 2009, afferma che «operatore del sistema deve intendersi, nella ratio della norma chiunque, nell'ambito del sistema informatico, svolge una funzione dal cui abuso può derivare un'agevolazione nella perpetrazione del reato»[121].

7. Il trattamento sanzionatorio e la procedibilità

Il delitto *ex* art. 635 *bis* c.p. è punito con la reclusione da sei mesi a tre anni, nella forma semplice, e con la reclusione da uno a quattro anni nella forma aggravata, indipendentemente dal fatto che si tratti di danneggiamento operato su beni − informatici − materiali o immateriali; tale cornice sanzionatoria ricalca in maniera precisa quella prevista nell'originaria forma dispositiva dell'art. 635 *bis*, co. 1, c.p.

Per il reato di sabotaggio informatico, invece, *ex* art. 635 *quater* c.p., è prevista la pena base della reclusione da uno a cinque anni, mentre in presenza delle circostanze aggravanti speciali «la pena è aumentata».

Evidentemente, il legislatore del 2008, ha adottato un trattamento sanzionatorio più grave per le ipotesi di danneggiamento di sistemi informatici o

[119] Segnalata ma non condivisa da CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 794; allo stesso modo MANTOVANI, *Diritto penale. Parte speciale II* cit., 153.
[120] A sostegno, su tutti, POMANTE, *Internet e criminalità* cit., 11; SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 236.
[121] Cass. Pen. Se. II, 11.11.2009, n. 44720, in *Foroplus*, *https://www.foroplus.it/home.php*.

telematici, rispetto a quello rivolto verso dati o informazioni, discostandosi dalla previsione del legislatore del 1993; quest'ultimo, infatti, formulando solo l'art. 635 *bis* c.p., valido sia per il danneggiamento di dati che per quello dei sistemi, ne aveva equiparato il regime sanzionatorio.

La distinzione operata con la l. 48/2008 deriva dall'adempimento delle indicazioni contenute nella Convenzione del Consiglio d'Europa in materia di criminalità informatica[122].

Merita, però, di essere segnalata una situazione, circa il quadro sanzionatorio, che non ha lasciato indifferente la dottrina di settore: vale a dire lo scompenso punitivo, a livello sistematico, tra i delitti di danneggiamento informatico ed il sistema di danneggiamento *tout court* considerato[123].

Già in passato era stata segnalata la sproporzione sanzionatoria tra il danneggiamento comune e quelli informatici.[124], sia ritenendo eccessiva la pena per questi ultimi, sia trovando privo di giustificazione l'ampio scarto sanzionatorio, soprattutto considerando che le fattispecie informatiche erano plasmate sul modello dell'art. 635 c.p.

Tale situazione si aggrava maggiormente, alla luce delle più recenti modifiche alla normativa, vale a dire il d.lgs. 7/2016, con cui la fattispecie di danneggiamento semplice viene declassata ad illecito civile e, di conseguenza, assoggetta a sanzioni civili pecuniarie, aumentando ancora di più lo "scompenso" sanzionatorio.

Sotto il profilo strettamente processuale, invece, il delitto di cui all'art. 635 *quater* c.p. è procedibile d'ufficio, mentre l'illecito penale *ex* art. 635 *bis* c.p., a seguito della riforma del 2008, prevede la procedibilità a querela della persona offesa.

In origine, il legislatore del 1993 aveva previsto la sola procedibilità d'ufficio, per agevolare la persecuzione di tali tipologie delittuose, nonché per rimarcare la gravita del fatto di reato realizzato sugli "oggetti materiali"

---

[122] Artt. 4 e 5 *Convenzione del Consiglio d'Europa in materia di criminalità informatica*.
[123] Per approfondimento v. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 776.
[124] CORRIAS LUCENTE, *I reati di danneggiamento informatico*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Trattato di diritto penale. Parte speciale*, X, Torino, 2011, 450.

informatici, «per la loro capacità di contenere e trattare grandi quantità di informazioni, anche di elevatissimo valore»[125].

Di contro, il legislatore del 2008 ha preferito allineare le previsioni dell'art. 635 *bis* c.p., in merito al regime di procedibilità, a quelle dell'ipotesi base di danneggiamento semplice, vale a dire la procedibilità a querela di parte. A seguito, però, delle modifiche *ex* d.lgs. 7/2016, suddetto allineamento è venuto meno, in considerazione del fatto che le ipotesi di danneggiamento aggravato − ormai le sole perseguibili *ex* art. 635 c.p. − prevedono la procedibilità d'ufficio.

In ultima battuta, è rilevabile che, il regime di perseguibilità a querela della persona offesa, incastrandosi con il requisito dell'oggetto materiale "dell'altruità"[126], genera un duplice effetto. Da una parte, infatti, ne incrementa le difficoltà di ricostruzione concettuale, «giacché solo la persona offesa "titolare" del software "altrui" godrà del diritto di querela»; dall'altra può risultare funzionale nell'individuare in concreto le condotte dotate di reale offensività rispetto al bene giuridico tutelato, rimettendo l'attivazione della tutela alla persona offesa[127].

8. Il rapporto tra reati

Il discorso che ruota attorno al rapporto tra reati delle fattispecie di danneggiamento informatico si sviluppa su due punti.

Il primo parte dal segnalare che le fattispecie *ex* artt.635 *bis* e *quater* − ma anche l'art. 635 *ter* c.p. − contengono, in apertura, una clausola di sussidiarietà espressa, che recita «salvo che il fatto costituisca più grave reato».

In dottrina si sostiene che la portata di tale clausola non attenga tanto alla gestione dei rapporti tra queste fattispecie ed altri reati, quanto, piuttosto, alla funzione regolativa "interna" del sistema dei delitti di danneggiamento

[125] Cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 798.
[126] V. *supra* par. 3.2.
[127] In questo modo si esprime CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 798.

informatico[128], evidenziato, tra l'altro, dalla mancanza della suddetta clausola dal dispositivo dell'art. 635 *quinquies* c.p., fattispecie, teoricamente, più grave.

In questo modo è possibile scongiurare il rischio che, con la «quadruplicazione del vecchio art. 635 *bis* c.p.», come taluno ipotizzava, si possa ricondurre un medesimo fatto sotto più delitti del "microsistema" di danneggiamento informatico, tra loro in concorso[129].

Quello che emerge è un quadro che pone i delitti di danneggiamento informatico in progressione criminosa tra loro; così, ad esempio, come si è già accennato in precedenza[130], se uno degli eventi previsti dal sabotaggio informatico fosse commesso attraverso la «trasmissione di dati o programmi» − *ex* art. 635 *quater* c.p. − e si accompagnasse alla «distruzione» o «alterazione» di dati o programmi informatici contenuti nel sistema offeso, ricorrerà solo la più grave fattispecie del danneggiamento di sistemi informatici o telematici.

Lo stesso discorso si estende alle fattispecie di danneggiamento di dati o sistemi di "pubblico utilizzo", di cui si parlerà nel capitolo successivo.

Volgendo l'attenzione al rapporto con fattispecie di reato esterne al "microsistema", una prima, pacifica, questione attiene al danneggiamento comune *ex* art. 635 c.p., rispetto al quale è sufficiente osservare che tutti i danneggiamenti informatici si pongono, rispetto ad esso, in rapporto di specialità. Per questo motivo, nelle ipotesi di concorso, ricorreranno sempre le fattispecie informatiche, a discapito di quella comune[131].

Più complesso è, invece, il rapporto con il delitto di "accesso abusivo a sistema informatico", *ex* art. 615 *ter* c.p., con particolare riferimento all'aggravante speciale, di cui al co. 2, n. 2, ovvero all'evento aggravatore, di cui al co. 2 n. 3, i quali sanzionano, rispettivamente, l'uso strumentale di violenza informatica sulle cose ed il verificarsi di un evento di danneggiamento di dati o sistemi informatici o telematici in conseguenza dell'accesso abusivo.

---

[128] Per approfondimento cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 795.
[129] Cfr. DE MATTEIS, *sub artt. 635 bis, ter, quater, quinquies*, in LATTANZI, LUPO (diretto da) *Codice penale*, XII, Milano, 2010, 275.
[130] V. *supra* par. 4.2.
[131] CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 796.

Una prima tesi ermeneutica, considerando le ipotesi previste dal secondo comma dell'art. 615 *ter* c.p. come "speciali" rispetto ai danneggiamenti informatici, ritiene che questi ultimi vengano sempre e comunque assorbiti dalle prime.

Sembrerebbe più corretta, però, una diversa impostazione, la quale prevede che, in caso di condotte criminose, di accesso ad un sistema informatico con conseguente danneggiamento, laddove fossero commesse con dolo, si avrebbe l'applicazione di uno tra gli artt. 635 *bis* e seguenti c.p., in concorso con l'ipotesi base di accesso abusivo; di contro, l'aggravante e l'evento aggravatore *ex* art 615 *ter*, co. 2, n. 2 e 3, c.p., sarebbero applicabili rispetto alle medesime condotte qualora queste fossero "non volute", cioè non rilevanti *ex* artt. 635 *bis* e seguenti c.p. in ragione della mancanza dell'elemento soggettivo doloso, ma comunque imputabili al soggetto attivo in veste di circostanza aggravante, piuttosto che di evento aggravatore, i quali non richiedono «copertura soggettiva necessariamente dolosa»[132].

In conclusione si segnala che questa soluzione teorica non trova ostacoli all'applicazione rispetto all'evento aggravatore, previsto al comma 2 numero 3, giacché contiene una definizione autonoma di «evento di violenza reale informatica», la quale è sostanzialmente coincidente con quella emergente dalle fattispecie di danneggiamento informatico.

Viceversa, invece, la proposta ermeneutica in commento non si pone con la medesima unitarietà rispetto alla circostanza aggravante, prevista al comma 2 numero 2 dell'art. 615 *ter* c.p., segnatamente con la definizione di «violenza informatica sulle cose» ad essa attribuita, essendo mutuata dall'art. 392, co. 3, c.p., e concettualmente più ristretta di quella desumibile *ex* artt. 635 *bis* e seg[133].

---

[132] Per approfondimento si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 797.

[133] In estrema sintesi, la norma *ex* art. 392 c.p., al coma 3, introdotto con la l. 547/1993, effettua una sostanziale equiparazione tra la "violenza sulle cose" e la " violenza informatica". Nell'analizzare quest'ultima nozione, si segnala che l'ambito applicativo è residuale rispetto alle altre fattispecie autonome di reato che tipizzano la violenza su "oggetti materiali" informatici, e ciò accade essenzialmente con i delitti di danneggiamento informatico. A livello contenutistico, l'autonoma definizione fornita prevede che venga integrata la violenza informatica, *ex* art 392, co. 3, c.p., quando «un programma informatico viene alterato, modificato o cancellato in tutto o in parte», ovvero quando «viene impedito o turbato il funzionamento di un sistema informatico o telematico». Si può quindi notare facilmente come la nozione in parola appaia sensibilmente più

Nelle ipotesi di reato che da suddetta nozione rimangono escluse, la possibilità di configurare un fatto di acceso abusivo aggravato dalla strumentale «violenza informatica sulle cose» viene, a sua volta, esclusa a priori[134].

In ogni caso questa precisazione teorica potrebbe rimanere priva di risvolti pratici, tenendo conto delle difficoltà, tipiche del settore dei *cyber crimes*, di accertare in concreto se si tratti di violenza informatica "strumentale" all'accesso, ovvero "derivante" dall'accesso abusivo al sistema, rispettivamente rientranti nelle ipotesi di cui al comma 2, numero 2 − circostanza aggravante della "strumentalità" della violenza informatica sulle cose − e al numero 3 − evento "aggravatore" della violenza informatica derivante dall'accesso − *ex* art. 615 *ter* c.p. In questi casi la più ampia previsione *ex* comma 2 numero 3 ben potrà ricomprendere le carenze definitorie di quella del comma 2, numero 2, *ex* art. 615 *ter* c.p.

restrittiva rispetto a quella di cui agli artt. 635 *bis* e seg c.p. Cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 822.

[134] Per approfondimento CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 797.

CAPITOLO III

DANNEGGIAMENTO DI DATI E SISTEMI INFORMATICI PUBBLICI E DI PUBBLICA UTILITÀ

1. Le nuove disposizioni dei delitti contro l'integrità di dati e sistemi informatici pubblici e di pubblica utilità gli artt. 635-*ter* e 635-*quinquies* c.p.

L'evoluzione normativa, disciplinata dalla l. 48/2008, che ha, tra le altre cose, avuto ad oggetto la riformulazione dell'allora singolo delitto di danneggiamento informatico − art. 635 *bis* c.p. − è derivata dal formale recepimento delle disposizioni contenute nella Convenzione del Consiglio d'Europa del 2001 in materia di *cyber crimes*[1].

Tuttavia, le numerose modifiche apportate all'ordinamento giuridico, segnatamente al codice penale, non derivano esclusivamente dalla citata fonte sovranazionale; con specifico riferimento al "microsistema" dei delitti di danneggiamento informatico, elaborato proprio dalla riforma di cui si sta parlando, il legislatore non si è limitato ad operare la bipartizione tra il danneggiamento di dati o programmi e il danneggiamento di sistemi informatici o telematici, oggetto di analisi nel capitolo precedente − in adempimento degli artt. 4 e 5 della Convenzione − ma si è spinto oltre: sono, infatti, state inserite nell'ordinamento due ulteriori fattispecie di reato − agli artt. 635 *ter* e *quinquies* c.p. − le quali si aggiungono ed esauriscono il c.d. "microsistema" normativo di danneggiamento informatico[2].

I due reati, i quali sanzionano, rispettivamente, il «danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità» − *ex* art. 635 *ter* c.p. − ed il «danneggiamento di sistemi informatici o telematici di pubblica utilità» − *ex* art. 635 *quinquies* c.p. − saranno oggetto di approfondita disamina nelle pagine che seguiranno.

[1] V. *supra* Cap. I, par. 3.1 e par. 3.3.
[2] Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 220.

In via introduttiva è possibile segnalare come le suddette scelte del legislatore, nonché le modalità di esecuzione, sono state ampiamente criticate da illustri esponenti della dottrina penalistica informatica. Viene contestato, innanzitutto, il fatto che, secondo tali opinioni, ci si trovi dinanzi a un'ipotesi di *abrogatio legis sine abolitio criminis*[3], vale a dire una successione c.d. impropria di leggi penali. Infatti, contemporaneamente all'introduzione dei suddetti reati vi è stata l'abrogazione dei commi 2 e 3 dell'art. 420 c.p. − rubricato «attentato a impianti di pubblica utilità» − per opera dell'art. 6 della stessa l. 48/2008. Per le norme dei delitti di danneggiamento di dati o sistemi "di pubblica utilità" sono, infatti, stati presi come modello i commi abrogati di cui sopra, facendo sì che se ne conservasse il nucleo essenziale, senza soluzione di continuità, non effettuandosi, quindi, una vera e propria nuova formulazione delle fattispecie[4].

Entrando più nel dettaglio, si rileva come, tanto il trattamento sanzionatorio[5] − identico a quello previsto dall'abrogato comma 2 *ex* art. 420 c.p. − quanto la tecnica di formulazione della fattispecie "base", ed anche dell'ipotesi aggravata dall'evento[6] − ripresa rispettivamente dal comma 2 e dal comma 3 *ex* art. 420 c.p. − sono perfettamente identici a quelli che, a seguito della riforma del 2008, avrebbero dovuto sostituire.

In commento alla scelta sostenuta dal legislatore che, come vedremo in seguito, ha determinato diversi risvolti dal punto di vista ermeneutico, la critica della dottrina sostiene che si sarebbe dovuto preferire come modello di incriminazione la struttura adottata per gli altri due delitti di danneggiamento

[3] Si esprime in questo modo PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa - profili di diritto penale sostanziale*, in *Dir. Proc. Pen*, 2008, 6, 714.

[4] Senza addentrarsi eccessivamente nella questione, l'Autore che riporta tali osservazioni prende in considerazione che, non essendo di fronte ad una ipotesi di abrogazione di reato con contestuali nuove incriminazioni, non si applicheranno le disposizioni di cui all'art. 2, co. 1 e 2, c.p., relativi al fenomeno della "nuova incriminazione", quanto piuttosto il quarto comma *ex* art. 2 c.p., relativo alla retroattività della norma più favorevole al reo. Cfr. PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 714. Sulla generale disciplina della successione delle leggi penali nel tempo si rimanda a FIANDACA, MUSCO (a cura di), *Diritto penale. Parte generale* cit., 96 ss; MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 135 ss.; per una trattazione approfondita della questione si rimanda a GAMBARDELLA, *L'abrogazione della norma incriminatrice*, Napoli, 2008.

[5] V. *infra* par. 7.

[6] Si anticipa che le "ipotesi base", relative al comma 1 degli artt. 635 *ter* e *quinqies* c.p. si caratterizzano per la peculiare struttura dei delitti di attentato, mentre le ipotesi previste al comma 2 dei medesimi delitti risultano strutturati come fattispecie aggravate dall'evento. V. *infra* par. 4.

informatico − artt. 625 *bis* e *quater* c.p. − mantenendo, in questo modo, una più precisa e completa unitarietà sistematica[7].

Ulteriore elemento, verso il quale sono stati rivolti commenti sfavorevoli da diversi autori, consiste nella scelta, considerata del tutto priva di giustificazioni di natura politico-criminale, di ricorrere ad espressioni diverse per definire oggetti passivi aventi identica rilevanza pubblica. Al posto della «complessa e controversa locuzione» di «utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità» per indicare gli oggetti materiali su cui ricadono le condotte punite ai seni dell'art. 635 *ter* c.p., il legislatore avrebbe fatto meglio ad utilizzare la più chiara e sintetica espressione di «pubblica utilità»[8].

Si segnala, comunque, che la medesima dottrina, pur rilevando le problematicità ermeneutiche derivanti dall'adozione a modello dei commi abrogati dell'art. 420 c.p., e quindi del fenomeno della *abrogatio legis sine abolitio criminis*, non esita dall'individuare anche profili di allontanamento e differenziazione, a partire dalla ben diversa collocazione sistematica. Difatti gli artt. 635 *ter* e *quinquies* c.p. hanno determinato che fossero inseriti nella parte del codice dedicata ai delitti contro il patrimonio le disposizioni che precedentemente erano rilegate nel titolo V, libro II, dedicato, invece, ai delitti contro l'ordine pubblico[9].

A ciò si aggiunge che le nuove norme, in conformità con le disposizioni della Convenzione di Budapest, hanno effettuato la scorporazione basata sui diversi oggetti materiali del fatto tipico, rispettivamente «dati, informazioni e

---

[7] A riguardo si veda SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 221.

[8] Posizione sostenuta da SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 220. La posizione dell'Autore si basa su quanto, in precedenza, affermato da PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715. L'Autore sviluppa il discorso circa l'ingiustificabilità della scelta del legislatore per le locuzioni adottate per identificare gli oggetti materiali *ex* art. 635 *ter* c.p.; prima di tutto non si comprende come mai il legislatore abbia adottato l'infelice locuzione dei beni «utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità» solo per una, e non entrambe le fattispecie di danneggiamento informatico di beni "pubblici". Un secondo problema sorgerebbe per'uso del pronome «ad essi», il quale sembra riferirsi necessariamente ai termini «Stato» ed «ente pubblico», peraltro già complemento d'agente del verbo «utilizzati». La locuzione appare così superflua, o forse un residuo dell'originaria formulazione del comma 2 dell'art. 420, dalla quale è tratta. In ogni caso è opinione dell'Autore che la locuzione «di pubblica utilità» sarebbe stata preferibile. Afferma poi che «non è chiaro quale potrebbe essere, al di fuori delle due ipotesi dell'utilizzazione e della pubblica utilità, il rapporto di "pertinenza" con lo Stato od un ente pubblico».

[9] Cfr. PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 714.

programmi informatici» e «sistemi informatici e telematici», non prevista dalle disposizioni contenute nei commi 2 e 3 *ex* art. 420 c.p.

Anche le previsioni delle condotte penalmente rilevanti ai sensi degli articoli in esame sono state, parzialmente, riformulate, allineandosi, in questo senso, agli artt. 635 *bis* e *quater* c.p. Emergerebbe, però, in questo senso, che la prescelta struttura del delitto di attentato renderebbe le condotte «eccessivamente evanescenti» rispetto ad eventi in relazione ai quali dovrebbero essere soltanto "diretti".

In conclusione, la sopracitata dottrina, pur apprezzando la scelta del legislatore di garantire ai dati e ai sistemi di "pubblica utilità" una protezione più forte avverso le condotte di danneggiamento, non ne giustifica il metodo; infatti, non si riteneva necessaria un'ulteriore differenziazione in due distinti delitti, certamente non prescritta dalle fonti sovranazionali, potendosi, secondo tale opinione, ottenere il medesimo risultato con una circostanza aggravante speciale, analogamente a quelle già previste dagli artt. 635 *bis* e *quater* c.p., ovvero anche con una fattispecie autonoma − per evitare il giudizio di bilanciamento tra circostanze aggravanti *ex* art. 69 c.p. − ma senza l'adozione della struttura dei delitti di attentato, la quale «trovava un pur controverso fondamento solo nella prospettiva di tutela di un bene collettivo come l'ordine pubblico»[10].

2. Soggetto attivo e bene giuridico tutelato: tre possibili orientamenti

Per iniziare l'analisi delle due fattispecie di reato previste dagli artt. 635 *ter* e *quinquies* c.p. si indirizzerà il discorso al dibattito dottrinale che ha coinvolto l'identificazione del bene giuridico tutelato.

Rispetto a quanto si è avuto modo di analizzare in riferimento agli artt. 635 *bis* e *quater* c.p.[11], la situazione appare più complessa. Difatti, dalle numerose disquisizioni riscontrate in dottrina riguardo l'individuazione del bene giuridico tutelato dai delitti in parola, è possibile identificare tre diverse teorie che si orientano su altrettante oggettività giuridiche.

[10] In argomento PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715. Il giudizio *ivi* espresso si chiude con il commento dell'Autore che recita «non è chiaro lo scopo di politica criminale perseguito con la fragile e complessa costruzione sistematica in esame».

[11] Si rimanda a *supra* Cap. 2, par. 2.

Un primo orientamento, che ragiona sull'attuale collocazione sistematica dei reati sottoposti ad analisi, stabilita dalla riforma operata per mezzo della legge di ratifica della Convenzione di Budapest l. 48/2008, arriverebbe alla conclusione che, anch'essi, al pari dei delitti di danneggiamento di dati, informazioni o programmi informatici "privati", orienterebbero la tutela verso il patrimonio. Il fatto che, poi, il patrimonio informatico abbia una maggiore rilevanza per la collettività, o, per meglio dire, sia qualificato «di pubblica utilità», giustificherebbe il diverso, e più grave, trattamento sanzionatorio, rispetto alle ipotesi di danneggiamento informatico c.d. "comune"[12].

Il secondo orientamento, invece, valorizza il fatto che le fattispecie, pur essendo state riformulate e reinserite in un diverso contesto del codice penale, mantengano la struttura del delitto di attentato *ex* art. 420 c.p., individuando, quindi, un'oggettività giuridica marcatamente pubblicistica (l'ordine pubblico), come emergeva già dalle norme abrogate e sostituite per mezzo della l. 48/2008. In altre parole, le disposizioni *ex* artt. 635 *ter* e *quater* c.p. rimangono del tutto indifferenti alla nuova collocazione sistematica, ponendosi comunque a presidio del bene giuridico, già oggetto di tutela dagli abrogati commi 2 e 3 *ex* art. 420 c.p.[13].

La posizione appena espressa è stata ampiamente criticata da altra dottrina, la quale ha rilevato che, innanzitutto, se il legislatore avesse effettivamente voluto tutelare con le nuove fattispecie qui esaminate l'ordine pubblico, non si spiegherebbe la collocazione nel titolo dedicato ai «delitti contro il patrimonio»; in secondo luogo, a prescindere dalla considerazione appena effettuata, neppure il

[12] Sul punto di veda BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza*, in MARINUCCI, DOLCINI (a cura di), *Trattato di diritto penale, Parte speciale*, VIII, Padova, 2010, 1144. L'Autore, evidentemente, si inserisce nella schiera dei sostenitori della tesi patrimonialista anche in riferimento ai delitti di cui agli artt. 635 *bis* e *quater* c.p.; afferma infatti che «il bene giuridico tutelato sia da considerarsi [...] quello comune a tutti i reati di danneggiamento informatico e, cioè, l'integrità del patrimonio informatico». Allo stesso modo sembrerebbe orientasi LEONE, *Il nuovo danneggiamento informatico* cit., il quale, critico rispetto alla scelta del legislatore di inserire suddetti reati nell'ambito del titolo XIII dei «delitti contro il patrimonio», avrebbe trovato di maggior pertinenza l'inserimento degli stessi nella *species* degli illeciti di cui al titolo VIII, libro II, dei «*delitti* contro l'economica pubblica, l'industria e il commercio», ovvero anche nel titolo V, dedicato ai delitti «*contro l'ordine pubblico*»; stante l'attuale ubicazione all'interno del codice dei reati in esame, l'Autore afferma che si tratterebbe di «delitti che offendono in via esclusiva o principale interessi di natura economico-patrimoniale in una dimensione superindividuale».

[13] Così pare orientato ATERNO, *Le fattispecie di danneggiamento informatico* cit., 55.

richiamo ad un bene giuridico di natura strettamente pubblicistica, e, quindi, di interesse collettivo, riuscirebbe a giustificare la «sproporzionata» anticipazione della soglia di punibilità rispetto alla gravità dell'offesa[14].

Peraltro, la collocazione sistematica dell'art. 420 c.p., nella sua più recente riformulazione, derivante dalle modifiche apportate dalla l. 191/1978 − che ha convertito il d.l. 59/1978 − sicuramente precedente alle abrogazioni dettate dalla l. 48/2008, si giustificava per ragioni di ordine storico, evidentemente non più attuali; il legislatore del tempo, infatti, si trovò a dover fronteggiare una realtà sociale fatta, anche, di atti di delinquenza politica, per lo più terroristici, avverso beni di pubblica utilità, in quanto messo in pericolo era anche il senso di sicurezza generale dei cittadini. In questo contesto si è rilevato come la dimensione collettiva dei beni di sicurezza e dell'ordine pubblico abbiano avuto preminenza su qualsiasi altro, seppur più concreto, profilo lesivo nelle scelte di criminalizzazione delle fattispecie di reato[15].

La terza opzione, che tra le altre è quella che riscontra maggior sostegno in dottrina, avendo come obbiettivo quello di ritrovare unicità nel "microsistema" dei delitti di danneggiamento informatico, interamente considerato, estende anche alle fattispecie aventi ad oggetto dati, informazioni o sistemi di pubblica utilità il medesimo bene giuridico tutelato dai delitti avverso gli oggetti materiali informatici c.d. "privati", vale a dire l'integrità e disponibilità dei dati e sistemi informatici e telematici[16].

Oltre alle ragioni di ordine sistematico di omogeneità offensiva, la tesi che estende l'integrità e la disponibilità dei dati e sistemi informatici, quali beni

---

[14] Così SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 239. Il discorso effettuato dall'Autore verrà ripreso ed approfondito nel paragrafo dedicato all'analisi della struttura dei delitti di attentato. V. *infra* par. 4.

[15] Per approfondimento si veda BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza* cit., 1144; riflessioni effettuate dagli Autori riprendendo una più vecchia dottrina cfr. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati* cit., 57. L'autore segnalava che una delle prime fattispecie introdotte per combattere i *cyber crimes* consisteva nell'art. 420 c.p., riguardante l'incriminazione di attentati «ad impianti di elaborazione date» se "di pubblica utilità", venne inserita dal legislatore del 1978 per far fronte alla diffusa preoccupazione nei paesi in cui lo sviluppo tecnologico aveva portato a fatti di sabotaggio se non anche di terrorismo.

[16] A sostegno di tale tesi si richiamano SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 238; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 799. Con riferimento al vecchio art. 420, co. 2 e 3, c.p. cfr. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati* cit., 57 s.

giuridici tutelati, anche ai delitti di cui agli artt. 635 *ter* e *quinquies* c.p., trova ulteriore riscontro nella considerazione che la minaccia alla pronta utilizzabilità di beni informatici, diversamente da «un più macchinoso richiamo al patrimonio», permetterebbe di giustificare il profilo di offesa ad una vasta ed indeterminata gamma di utenti, radicato, per l'appunto, nella pubblica utilità degli oggetti materiali[17].

Con riguardo al soggetto attivo, così come gli artt. 635 *bis* e *quater* c.p., anche i delitti *ex* artt. 635 *ter* e *quinquies* c.p. si qualificano come reati comuni, potendo, di conseguenza, essere commessi da chiunque.

3. Gli oggetti materiali e la peculiare "qualificabilità" pubblica

Con riguardo agli oggetti materiali delle condotte, intese in senso stretto, vale a dire a prescindere dalla qualificabilità "pubblica" o "privata", il legislatore ha allineato i due delitti in esame agli artt. 635 *bis* e *quater* c.p., sia per quanto riguarda la bipartizione tra dati, programmi e informazioni − verso cui si rivolge l'art. 635 *ter* c.p. − e i sistemi informatici o telematici − ai quali è dedicato l'art. 635 *quinquies* c.p. − sia in riferimento alle definizioni attribuite agli stessi. Per la trattazione di tali concetti, quindi, si rimanda integralmente al paragrafo dedicato, nel capitolo precedente[18].

L'elemento che, però, differenzia le norme in commento dalla coppia descritta in precedenza, posto a fondamento della rilevante diversità di disciplina, è la qualificabilità "pubblica" degli oggetti passivi, rispetto alla natura essenzialmente "privata" − fondata sul concetto di "altruità" della cosa − di quelli di cui al capitolo precedente. Sulla suddetta peculiarità degli artt. 635 *ter* e *quinquies* c.p. è opportuno soffermarsi.

Si segnala preventivamente che il legislatore del 2008 non ha formulato gli articoli sottoposti al presente esame in maniera omogenea. Infatti, se pure entrambe le disposizioni prevedono che l'oggetto materiale debba essere «di pubblica utilità», solo per la norma dell'art. 635 *ter* c.p. − e non anche l'art. 635 *quinquies* c.p. − viene prevista l'alternativa che attribuisce rilievo al

[17] In questo modo CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 799.
[18] V. *supra* Cap. II, par. 3.

danneggiamento di dati, informazioni e programmi «utilizzati dallo Stato, o da altro ente pubblico o ad essi pertinenti». A tale diversa previsione del legislatore nel dato testuale delle due norme in parola si è già brevemente accennato, nelle pagine precedenti[19], sopratutto in riferimento alle aspre critiche rivoltegli dalla dottrina maggioritaria[20].

Proseguendo con l'attribuire un significato alle espressioni adottate dal legislatore in riferimento alla qualificabilità degli oggetti materiali, si può cominciare dalla nozione che condividono entrambi gli articoli. Secondo l'opinione dominante per «pubblica utilità» deve intendersi la destinazione al servizio di una collettività indifferenziata e indeterminata di persone[21]. Viene espresso così un concetto indipendente da una formale pubblica titolarità del bene materiale; la maggior tutela fornita dalla norma si giustifica per il fatto che, in ragione della destinazione alla fruizione da parte di una vasta platea di soggetti o utenti, una lesione del bene materiale tutelato è destinata a concretizzarsi in un nocumento diffuso[22].

Tale nozione, definita in questo modo, rispetto all'alternativa qualifica "formalmente pubblicistica" − basata, cioè, sulla titolarità pubblica del bene − risulta, secondo dottrina, «certamente più vicina al disvalore effettivo specifico di tali incriminazioni», basata su un danno rivolto ad una indeterminata collettività di soggetti[23].

Si deve, però, notare anche che una nozione così intesa, per quanto concettualmente più concreta rispetto all'astratta titolarità dell'ente pubblico, risulta inevitabilmente fluida e dai contorni sfumati, giacché la destinazione al pubblico servizio di dati o programmi informatici potrebbe, in taluni casi, risultare opinabile. Secondo la medesima dottrina, quindi, sembrerebbe innegabile un «appannamento della determinatezza della fattispecie», che assume maggior

[19] V. *supra* par. 1.
[20] Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 220.
[21] Sul punto si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 800, che riprende la definizione fornita da BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza* cit., 1145 s.
[22] V. MANTOVANI, *Diritto penale. Parte speciale II* cit., 154. L'autore sinteticamente afferma la necessità di intendere l'espressione in parola in senso ampio, slegandolo dalla formale titolarità pubblica.
[23] Così CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 801.

rilievo se si considera la formulazione delle incriminazioni quali delitti di attentato.

In merito, invece, all'ulteriore previsione dell'art. 635 *ter* c.p., riguardante beni «utilizzati dallo Stato, o da altro ente pubblico o ad essi pertinenti», per quanto un'interpretazione letterale della norma sembrerebbe porre quest'ultimo come requisito primario rispetto a quello sopra descritto della «pubblica utilità», si dovrebbe preferire un approccio ermeneutico di tipo sistematico che, al contrario, suggerirebbe un rapporto tre le qualifiche dei beni materiali invertito.

Tenendo conto che la nozione in parola, come già affermato, appartiene esclusivamente alla fattispecie di danneggiamento di dati o programmi informatici, si deve considerare necessariamente residuale rispetto all'alternativa, condivisa da entrambi i delitti, a cui si attribuisce portata generale, in grado, tra l'altro, di abbracciare tutte le ipotesi e situazioni riconducibili all'espressione menzionata esclusivamente dall'art. 635 *ter* c.p.[24].

Nell'attribuire significato alla suddetta espressione adottata dal legislatore, si incappa nella difficoltà di individuarne uno autonomo ed ulteriore rispetto alla nozione di «*pubblica utilità*», che ampli l'area del penalmente rilevante della norma.

Procedendo in questa direzione, per individuare il perimetro concettuale "dell'utilizzazione" potrebbe farsi riferimento ad un rapporto di concreta disponibilità di dati, informazioni e programmi in capo al soggetto pubblico, indipendentemente dalla titolarità effettiva del bene o dal titolo che ne legittima l'uso[25].

Riguardo alla "pertinenza" ad un ente pubblico la migliore dottrina non sembra essere stata in grado di individuarne un autonomo significato, affermando in diverse occasioni, che la locuzione in parola appare del tutto superflua, costituendo, infatti, un residuo dell'abrogato art. 420, co. 2, c.p., dove, però, deteneva un preciso significato, diversamente dall'attuale situazione[26].

---

[24] Considerazioni effettuate in PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715.

[25] Così pare esprimersi ATERNO, *Le fattispecie di danneggiamento informatico* cit., 5o; allo stesso modo BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza* cit., 1146.

[26] Sul punto si è pronunciato MANTOVANI, *Diritto penale. Parte speciale II* cit., 154. L'autore ha sottolineato che nel vecchio, ed ormai abrogato, testo dell'art. 420 co. 2 c.p. la"pertinenza" si

In sintesi, dunque, la previsione aggiuntiva dell'art. 635 *ter* c.p. amplierebbe la punibilità anche alle ipotesi di danneggiamento di dati, programmi o informazioni, seppur non destinati ad una vasta platea di soggetti − cioè non di «pubblica utilità» − ma comunque nella "legittima disponibilità" − ovvero anche nella "utilizzazione o "pertinenza" − di un soggetto pubblico[27].

Peraltro, volendo soffermarsi brevemente sul concetto di "legittima disponibilità", con cui la maggior parte degli autori riassumono i termini di "utilizzazione o pertinenza"[28], si può cogliere come essa, pur non perfettamente coincidente, si avvicini moltissimo ad una nozione di «pubblica titolarità del bene informatico»; estendendo a questo discorso le riflessioni effettuate in riferimento al concetto di «altruità» rispetto agli artt. 635 *bis* e *quater* c.p.[29], il bene informatico non può essere oggetto, al pari delle *res* fisiche, di proprietà o possesso, determinando, quindi, un riferimento a una «quanto mai ampia ed evanescente rete di interessi funzionalistici all'integrità dello stesso»[30].

Proseguendo su questa linea di pensiero, condivisa da autorevole dottrina, si potrebbe affermare che i concetti di "utilizzazione e pertinenza" ad un soggetto pubblico di dati o programmi informatici vadano sostanzialmente a coincidere con i criteri di identificazione di soggetti passivi "pubblici" ai sensi dell'art. 635 *bis* c.p., quando, cioè, il *software* "altrui" sia di titolarità pubblica; in questo caso ricorrerà sempre il più grave delitto di cui all'art. 635 *ter* c.p.

D'altra parte, poi, l'assenza dell'espressione «altrui» riferita ai dati o sistemi "pubblici" lascerebbe intendere che i reati in parola possano sussistere anche se i suddetti beni informatici danneggiati, «di pubblica utilità» − non

---

riferiva ai dati, informazioni o programmi "pertinenti", per l'appunto, ai sistemi informatici o telematici; con la riformulazione e la bipartizione dei delitti di danneggiamento c.d. "pubblico" − *ex* l. 48/2008 − si è deciso di conservare la locuzione «ad essi pertinenti» modificandone, però, il significato poiché riferibile, come sembra, allo Stato o ad enti pubblici. Siffatta pertinenza appare certamente assorbita dalla generale "utilizzazione", nel significato inteso dalla dottrina maggioritaria e sopra riportato, determinandone l'assoluta superfluità. Alla medesima conclusione è pervenuto PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715.

[27] Per approfondimento cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 802.

[28] Così si orientano PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 802; MANTOVANI, *Diritto penale. Parte speciale II* cit., 154.

[29] V. *supra* Cap. II, par. 3.2.

[30] Sul punto CAPPELLINI, *ibidem.*

necessariamente di formale titolarità pubblica − siano «propri» dell'autore del danneggiamento[31].

Riferendosi, invece, esclusivamente all'art. 635 *quinquies* c.p., prevedendo solamente la «pubblica utilità» del bene materiale, non avrà alcun rilievo la concreta titolarità, pubblica o privata, del sistema informatico o telematico, ma esclusivamente la sua destinazione alla fruizione di una platea indeterminata di utenti

4. Le condotte incriminate e struttura dei delitti

Il più evidente riflesso della scelta da parte del legislatore del 2008 di mutuare la formulazione dei delitti *ex* artt. 635 *ter* e *quinquies* c.p. dai commi 2 e 3 *ex* art. 420 c.p. attiene alla struttura delle fattispecie.

Difatti, i delitti di danneggiamento di dati o sistemi informatici "pubblici" si caratterizzano per essere delitti a consumazione anticipata, ovvero, più sinteticamente, di attentato. Ne consegue che la perfezione del reato avviene ogni qual volta siano commessi «fatti diretti a» cagionare uno degli eventi di danno rilevanti.

In via preliminare si può segnalare un'ulteriore differenza di previsione tra i due articoli in commento: se, infatti, l'art. 635 *ter*, co. 1, c.p. punisce «fatti diretti a» cagionare un danneggiamento avverso i beni materiali identificati − qualificando sostanzialmente il reato "a forma libera" − per l'art. 625 *quinquies*, co. 1, c.p., anziché punire simmetricamente rispetto al menzionato delitto anche gli atti diretti a danneggiare un sistema informatico o telematico, il legislatore ha caratterizzato la fattispecie per la sua condotta "a forma vincolata"; ciò deriva dalla previsione, posta all'*incipit* dell'art. 635 *quinquies* c.p., «se il fatto di cui all'art. 635 *quater* è diretto a». Per dare un senso al rimando al fatto tipico del delitto di danneggiamento di sistemi "privati", si dovrebbe ritenere che il legislatore abbia voluto criminalizzare soltanto le condotte commesse con le modalità espressamente previste dall'art. 635 *quater* c.p., diretta a cagionare uno

[31] Così sul punto si veda MANTOVANI, *Diritto penale. Parte speciale II* cit., 154.

dei danni inclusi nella disposizione *ex* art. 635 *quinquies* c.p., e quindi qualificare la fattispecie in parola come reato a forma vincolata[32].

La struttura dei delitti di attentato ha determinato un'anticipazione della soglia di punibilità, che viene fatta coincidere il momento che integra l'ipotesi del tentativo dei rispettivi delitti comuni[33]; questa costituisce una scelta del legislatore di particolare peso, a partire dalla considerazione del fatto che viene riservato al delitto, sostanzialmente, tentato, la stessa, se non anche più grave, cornice punitiva di quello consumato. Tale previsione dovrebbe essere adottata per la tutela di beni giuridici di particolare importanza[34].

Per questa ragione, come anche già anticipato, suddetta scelta del legislatore del 2008 ha suscitato aspre critiche in dottrina, per diversi profili; innanzitutto la collocazione all'interno del codice nel campo dei delitti contro il patrimonio, e quindi rispetto a beni giuridici lontani «dal rilievo costituzionale di primo piano che sarebbe opportuno»[35]. Sul punto si è già detto che, però, le norme in parola rimangono del tutto indifferenti rispetto alla collocazione sistematica, sia per quanto attiene al bene giuridico tutelato[36], sia in riferimento alla compatibilità con la struttura delle fattispecie di delitti di attentato.

Altro aspetto problematico deriva dall'«eccessiva estensione» dell'ambito di applicazione delle fattispecie; delimitando la tipicità a tutte le condotte potenzialmente dirette a danneggiare i dati o sistemi informatici «utilizzati dallo Stato, o da altro ente pubblico o ad essi pertinenti» o comunque «di pubblica utilità», comporta la potenziale inclusione anche di atti la cui possibilità di sfociare in una seria e concreta minaccia al bene giuridico tutelato risulti troppo esigua. Oltretutto la tipicità dei delitti di attentato *ex* artt. 635 *ter* e *quinquies* c.p.

---

[32] Per approfondimento si rimanda a SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 220.

[33] La dottrina maggioritaria riscontra nel tentativo il massimo arretramento possibile della soglia di tutela tollerabile senza entrare eccessivamente in contrasto con il principio costituzionale di offensività *ex* art. 49 c.p.; per questo motivo per individuare i contorni oggettivi dei reati di attentato, ad configurazione anticipata si fa riferimento ai criteri e nozioni relative alla disciplina generale di diritto penale sostanziale. Si veda a riguardo su tutti FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 502 ss.; MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 571 ss.

[34] Così CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 803.

[35] Cfr. CAPPELLINI, *ibidem.*

[36] V. *supra* par. 2.

risulta talmente ampia da poter portare "all'assurdità" di punire con una pena detentiva sproporzionata qualsiasi condotta diretta a danneggiare anche un "singolo" dato o sistema informatico «utilizzato» dallo Stato o ente pubblico[37].

Va poi precisato che, per la configurazione del reato, è richiesta la "non" distruzione, deterioramento, ecc., ma solamente la concreta idoneità a cagionare il danno, in ragione del fatto che tali eventi siano previsti come "aggravatori" dai commi 2 degli artt. 635 *ter* e *quinquies* c.p. (per la trattazione del tema si rimanda al paragrafo dedicato)[38].

Fornendo ulteriori indicazioni circa la struttura dell'offesa dei delitti in parola è corretto affermare che, per via delle considerazioni appena effettuate, gli stessi debbano considerarsi non come reati d'evento ma fattispecie di pericolo.

In riferimento, invece, agli eventi di danno verso cui devono essere proiettate le condotte sanzionate, è possibile riconoscere un parallelismo rispetto alle due fattispecie di danneggiamento informatico "privato" *ex* artt. 635 *bis* e *quater* c.p., ipotesi in cui, invece, l'evento deve necessariamente realizzarsi.

Così l'art. 635 *ter* c.p. richiede che le condotte siano dirette a cagionare uno dei cinque eventi propri della norma di cui all'art. 635 *bis* c.p., vale a dire la «distruzione», il «deterioramento», l'«alterazione», la «cancellazione» e la «soppressione» di dati, informazioni o programmi informatici «di pubblica utilità».

Più complessa appare l'operazione ermeneutica necessaria rispetto l'art. 635 *quinquies* c.p., in ragione del richiamo espresso al "fatto" previsto dall'art. 635 *quater* c.p., a cui si faceva riferimento in apertura del presente paragrafo. Non potendosi interpretare in maniera letterale il termine «fatto», per risolvere il «bisticcio testuale» del legislatore esso deve legarsi alle condotte tipiche del delitto di danneggiamento di sistemi "privati". In questo modo è possibile ritrovare unitarietà sistematica e completare il parallelismo tra eventi − verso cui

[37] Sul punto per approfondimento si rimanda a SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 239.
[38] Così MANTOVANI, *Diritto penale. Parte speciale II* cit., 154; nel presente elaborato si veda *infra* par. 6.

devono orientarsi le condotte − *ex* artt. 635 *ter* e *quinquies* c.p., e quelli − che devono concretizzarsi − *ex* artt. 635 *bis* e *quater* c.p.[39].

Sciolto questo nodo interpretativo è possibile affermare che le condotte rilevanti ai fini del delitto di danneggiamento di sistemi informatici o telematici «di pubblica utilità» devono essere idonee a cagionare uno dei quattro eventi individuati dal rispettivo delitto di sabotaggio informatico avverso beni materiali "privati", vale a dire la «distruzione» e il «danneggiamento» di un sistema informatico o telematico, ovvero anche il «renderlo, in tutto o in parte, inservibile», nonché il fine di «ostacolarne gravemente il funzionamento».

4.1. I delitti a consumazione anticipata e il principio di offensività. Brevi cenni

In questa sede si vuole fornire una breve analisi della tecnica normativa dei delitti a consumazione anticipata, categoria estremamente dibattuta in dottrina perché propone una – apparente - deroga al modello di reato come offesa a beni giuridici, in potenziale contrasto con il fondamentale principio di offensività, cardine della materia di diritto penale sostanziale[40].

Il requisito, previsto espressamente della generale categoria dei delitti di attentato, consiste nella direzione degli atti a cagionare il risultato dannoso designato; accanto a questo, la dottrina maggioritaria e la giurisprudenza richiedono, in via interpretativa, che gli atti siano altresì idonei alla realizzazione degli eventi verso cui sono diretti, e questo per evitare l'eventuale contrasto con il principio di offensività − secondo cui non può esserci reato senza un'offesa a un bene giuridico − da cui potrebbero scaturire dubbi di legittimità costituzionale[41].

---

[39] Per approfondimento si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 804.

[40] Sul punto offre diversi spunti SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 222 ss.

[41] Indipendentemente dal contenuto del principio di offensività, una questione che merita brevi cenni attiene alle fonti normative che lo prevedono; in effetti nessuna norma di rango costituzionale o ordinario prevede espressamente il principio in parola, sebbene sia realistico credere che dal senso complessivo delle norme costituzionali fonti del diritto penale «si possa ricavare una direttrice di politica criminale». In particolare l'esistenza del principio di offensività si ricaverebbe, in via interpretativa, dall'art. 13 della Costituzione, nella parte in cui prevede la possibilità di derogare all'inviolabilità della libertà personale in ragione di uno specifico interesse comunque perseguito dall'Autorità pubblica, ma anche dagli artt. 25, co. 2 e 3 e 27, co. Della Costituzione. Per quanto la posizione di chi riconosca nelle suddette disposizioni il fondamento del principio di offensività sia suscettibile di contestazione, non sono mancate pronunce della Corte

L'obbiettivo della dottrina maggioritaria, ritenendo che i delitti di attentato debbano avere una struttura oggettiva come minimo affine a quella del tentativo, sarebbe quello di trovare fondamento teorico al requisito − implicito − dell'idoneità[42].

I sostenitori della c.d. concezione realistica del reato, i quali individuano il principio della necessaria offensività della condotta dei reati, desumendolo dall'art. 49, co. 2, c.p., fondano su questo la necessità di richiedere il suddetto requisito di idoneità per tutti i delitti di attentato[43]. Tale posizione, per quanto condivisa dalla maggior parte degli autori, non è stata unanimemente condivisa e, proprio in ragione delle critiche rivolte alla concezione realistica, hanno spinto la dottrina a trovare altre basi teoriche e argomentative su cui fondare la necessità dell'idoneità degli atti diretti ad un determinato evento.

Anche chi non si allinea alla teoria realistica del reato, non riconoscendo nella violazione del principio di offensività un rischio di illegittimità costituzionale, non può non riconoscere che senza il requisito dell'idoneità i delitti di attentato, «che si caratterizzano per la descrizione a forma "aperta" e quindi indeterminata», andrebbero in contro al contrasto con il principio − costituzionale − di tassatività e sufficiente determinatezza, corollario del generale principio di legalità *ex* art. 25 della Costituzione[44].

Volgendo lo sguardo alla prassi applicativa, non è riscontrabile un consenso unanime circa il grado ed il giudizio di idoneità. Un primo orientamento giurisprudenziale ha sostenuto che, per i delitti di attentato, essa avrebbe dovuto

---

Costituzionale che hanno riconosciuto valenza costituzionale al principio in parola, su tutte Cort. Cost 21.11.2000, n. 519, in *Foroplus*, *https://www.foroplus.it/home.php*. I sostenitori del principio rinvengono anche nel codice penale una possibile fonte normativa, nell'art. 49 c.p., nella parte che prevede che «la punibilità è esclusa quando è impossibile l'evento dannoso o pericoloso». Si fa riferimento alla c.d. concezione realistica del reato, che attribuisce rilevanza solo alle condotte concretamente ed effettivamente offensive dei beni giuridici. Sul punto si è pronunciata in diverse occasioni anche la Corte di Cassazione; su tutte si cita Cass. Pen., Sez. V, 28.06.2011, n. 25674, in *Foroplus*, *https://www.foroplus.it/home.php*. La Corte riconosce che «secondo la più attenta dottrina e giurisprudenza, la mera aderenza del fatto alla norma di per sé non integra il reato, essendo necessario anche che la condotta sia effettivamente lesiva del bene giuridico protetto dalla norma : non solo quindi "*nullum crimen sine lege*" ma anche "*nullum crimen sine iniuria"*».

[42] Sul punto cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 223.

[43] Sul punto si rimanda a MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 571 ss.

[44] Valutazione offerta da SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 223. Sul generale principio di sufficiente determinatezza si rimanda a FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 85 ss.

avere un perimetro concettuale autonomo rispetto ai delitti tentati, considerandola in dettaglio come «mera possibilità» del verificarsi dell'evento, da valutarsi solo in riferimento alla condotta del soggetto agente, e non anche sulle eventuali circostanze[45].

Un successivo e diverso orientamento, invece, riteneva l'idoneità come la «non impossibilità» del verificarsi dell'evento lesivo, criticato apertamente dalla dottrina per non aver ristretto a sufficienza la portata dei delitti di attentato, potendo, però, in questo caso, il giudice, tener conto anche «del concorso di altri fattori imprevisti ed eventuali, ma possibili»[46].

Secondo la dottrina contemporanea, entrambe le suddette interpretazioni non sono convincenti, in considerazione dell'effetto estensivo dei delitti a consumazione anticipata anche a meri atti preparatori, che però non costituiscono un pericolo concreto per il bene giuridico tutelato. La citata dottrina sostiene che la modulazione del requisito dell'idoneità dovrà avvenire secondo la concezione propria del medesimo criterio richiesto per il tentativo; rileveranno, quindi, solo le condotte che determinano una situazione di concreto pericolo per il bene tutelato; che abbiano, cioè, una rilevante possibilità o probabilità di tramutarsi in danno. L'idoneità si dovrebbe quindi valutare sulla base di un giudizio avente «carattere di prognosi postuma», ovvero posto in essere *ex ante*[47].

Una diversa elaborazione dottrinale in merito alla nozione in esame, ha fortemente criticato la pretesa funzione tipizzante dell'implicito requisito dell'idoneità. Questa viene, invece, posta al fianco del concetto di causalità materiale nel reato, che, al suo pari, non ha alcuna portata determinativa della tipicità delle condotte. Si tratterebbe, piuttosto, di un «concetto di relazione», che consente di mettere in rapporto il risultato intenzionale − l'evento − e la condotta volta a provocarlo – "l'atto diretto a"[48]. Ne conseguirebbe che l'ambito delle condotte tipiche possa essere circoscritto dal criterio dell'idoneità solo quando

[45] Cass. Pen., Sez. Un., 19.05.1957, Toffanin e altri, in *Il Foro italiano*, Vol. 81, II, 1958.
[46] Cass. Pen., Sez. Un., 14.03.1970, p. m. c. Kofler ed altri, in *Il Foro italiano*, Vol. 94, III, 1971.
[47] Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 224. Sulla idoneità del tentativo si veda FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 484 ss.; MANTOVANI, *Diritto penale. Parte generale* cit., 439 ss.
[48] Posizione elaborata da PADOVANI, *La tipicità inafferrabile. Problemi di struttura obiettiva delle fattispecie di attentato contro la personalità dello Stato*, in Aa. Vv., *Il delitto politico dalla fine dell'ottocento ai giorni nostri*, Roma, 1984, 170 ss.

anche il secondo termine di relazione, cioè l'evento-risultato, sia sufficientemente determinato.

Anche nel caso di delitto di attentato che preveda un evento descritto in maniera dettagliata, non sarà sufficiente ricorrere al requisito dell'idoneità, così intesa, per selezionare i fatti − astrattamente − conformi a quelli autonomamente lesivi del bene giuridico. Sarà, invece, necessario che le condotte a forma libera, rapportate all'evento, siano caratterizzate dalla necessaria offensività[49]. L'autore afferma infatti che «soltanto in questa ipotesi si potrà ricorrere al menzionato criterio dell'idoneità, per ricomprendere nella sfera di tipicità quelle condotte che [...] risultino offensive dell'interesse tutelato».

È possibile essere ancora più specifici, riconoscendo la possibilità di differenziare l'apparentemente unitaria categoria dei delitti di attentato in tre sottogruppi, in base alla formulazione degli eventi tipici.

Un primo gruppo ricomprende ipotesi di attentato che riferiscono a risultati privi di un connotato intrinsecamente offensivo, come ad esempio il delitto di «attentato contro organi costituzionali e contro le assemblee regionali» *ex* art. 289 c.p. Un secondo gruppo, invece, include ipotesi di delitti di attentato che riferiscono di eventi c.d. "iperlesivi", *ivi* inclusi, a titolo esemplificativo, i delitti di «insurrezione armata contro i poteri dello Stato» − *ex* art. 284 c.p.− ovvero di «guerra civile» − *ex* art. 286 c.p. Il terzo, ed ultimo, gruppo abbraccia i delitti di attentato che anticipano e specializzano la tutela offerta da delitti comuni a determinati beni giuridici, la cui struttura viene ricondotta al tentativo; tra questi vi rientrano i delitti di danneggiamento informatico avverso dati o sistemi «di pubblica utilità» *ex* art. 635 *ter* e *quinquies* c.p.[50].

Secondo un'altra autorevole dottrina, il principio del *ne bis in idem* sostanziale per i delitti di attentato contro la «personalità interna dello Stato» − *ex* art. 301, co. 1, c.p. − che disciplina il rapporto in ipotesi di concorso di reati identici ma positivizzati da diverse fonti, in deroga al principio della *lex specialis*,

[49] Per approfondimento si rimanda a SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 225.
[50] Cfr. PADOVANI, *La tipicità inafferrabile* cit., 172.

è estensibile anche alle fattispecie che, pur non essendovi espressamente incluse, detengono una struttura dogmatica identica[51].

Sarebbe quindi possibile, se non anche giuridicamente doveroso, applicare in via ermeneutica alle fattispecie di delitti di attentato sopra indicate, includendo certamente anche i delitti *ex* artt. 635 *ter* e *quinquies* c.p., i requisiti di tipicità previsti per il "fatto di tentativo" dei reati dolosi che designano un corrispondente, ma non parimenti qualificato, evento dallo stesso contenuto[52].

I delitti di attentato della menzionata categoria devono, quindi, presentare gli stessi requisiti propri delle fattispecie tentate dei corrispondenti delitti "comuni"; questi sono l'"univocità" e l'"idoneità", che devono essere accertate in sede processuale dal giudice sulla base di una valutazione *ex ante*[53].

Applicando tali osservazioni e riflessioni alle fattispecie di danneggiamento informatico c.d. "pubblico", si deve ritenere che, includendoli nell'alveo di norme a cui si applica la previsione dell'art 301 c.p. in via estensiva, essi possono essere qualificati come "speciali" rispetto ai "comuni" tentativi dei delitti di danneggiamento di dati o sistemi c.d. "privati" − *ex* artt. 635 *bis* e *quater* c.p. − dovendosi, quindi, ritenere, in via interpretativa, che la soglia di punibilità dei primi, cioè i delitti di attentato, coincida con quella prevista per il delitto tentato dei secondi.

Rileveranno, quindi, ai fini della configurazione dei delitti in parola, solo gli atti oggettivamente idonei, in modo non equivoco, a creare un concreto pericolo per il bene tutelato, da valutarsi sulla base del criterio di prognosi postuma[54].

Un'ulteriore valutazione che può effettuarsi rispetto alla struttura dei delitti di attentato, rapportata alle fattispecie di danneggiamento informatico *ex* artt. 635 *ter* e *quinquies* c.p., attiene alla sussistenza, o meno, dei presupposti per il legittimo ricorso alla tecnica normativa dei delitti a consumazione anticipata.

---

[51] Così PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, 193 s.
[52] Sul punto cfr. PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, 193 s.
[53] Per approfondimento v. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 226, che riprende la posizione di PICOTTI, *Il dolo specifico* cit., 194.
[54] Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 227.

La medesima dottrina che ha effettuato le considerazioni di cui sopra si è posta la questione, cercando di individuare, in prima istanza, quali possano essere i presupposti che giustifichino la scelta del legislatore di adottare una struttura per reati che, come abbiamo avuto modo di sottolineare, anticipano sensibilmente il momento consumativo, e quindi, la tutela offerta al bene giuridico, per poi valutarne la sussistenza nel caso dei delitti di danneggiamento informatico "pubblico"[55].

Il ricorso alla struttura dei delitti di attentato può trovare ragione, innanzitutto, in esigenze politico-criminali di sanzionare ipotesi assimilabili al tentativo con l'applicazione di pene uguali, se non anche più gravi, rispetto a quelle previste per il reato consumato, in deroga alla generale disciplina del delitto tentato − *ex* art. 56 c.p. Altre volte è la natura dell'evento che richiede di anticipare il momento in cui si attiva la tutela penalistica al bene giuridico, dal momento che qualora il delitto fosse effettivamente consumato, e quindi si raggiunga il fine a cui è diretta la condotta, il soggetto agente si potrebbe assicurare la completa impunità.

In questo senso si intuisce la ragione per cui si è soliti far ricorso a tale tecnica normativa per i reati contro la personalità dello Stato; se il legislatore subordinasse la punibilità degli atti al verificarsi dell'evento lesivo, «non solo si rischierebbe di assicurare l'impunità al reo, ma si metterebbe in pericolo la stessa esistenza dell'assetto politico-istituzionale»[56].

Nessuno dei due presupposti individuati si verificherebbe nelle ipotesi di danneggiamento avverso dati o sistemi informatici «di pubblica utilità»; infatti, non vi è sicuramente il rischio che al verificarsi dell'evento perseguito dal soggetto attivo questo si assicuri impunità, né, tantomeno, che determini una compromissione dell'assetto democratico dello Stato. Allo stesso modo non si riscontrano particolari ragioni di politica criminale che giustifichino

[55] Per approfondimento v. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 228.
[56] Cfr. SALVADORI, *ibidem*. Che ricorre a riflessioni precedentemente effettuate da GALLO, *Il delitto di attentato nella teoria generale del reato*, Milano, 1966.

l'applicazione, ad ipotesi di attentato, di un trattamento sanzionatorio maggiore rispetto a quello del tentativo[57].

Si può aggiungere poi che l'*iter* ermeneutico effettuato, che identifica i requisiti − impliciti − di "idoneità" e "univocità" dei delitti di attentato avverso dati o sistemi informatici, non sempre riuscirebbe ad arginare, se non l'indeterminatezza, quantomeno l'incertezza, delle condotte rientranti nei reati *ex* artt. 635 *ter* e *quinquies* c.p., in riferimento alle quali non sempre risulta agevole individuare lo «spartiacque» tra gli atti esecutivi − penalmente rilevanti − e quelli meramente preparatori[58].

La contestualizzazione delle condotte che sono oggetto di valutazione circa l'univocità − o anche direzione non equivoca − è fondamentale per riconoscere, o meno, rilevanza penale alle stesse. Gli atti, considerati autonomamente, pur potendone riconoscere l'idoneità offensiva, non devono necessariamente − non essendone in grado − rivelare la direzione finalistica e l'intenzione dolosa del soggetto agente; se così fosse risulterebbe impossibile, infatti, determinare la non equivocità a commettere un determinato delitto. Dovrà, invece, valutarsi l'"univocità" sulla base di un legame causale e finalistico, obbiettivamente rilevante, con la commissione dell'evento. Solamente dopo aver identificato il delitto verso cui è proiettata la condotta, sarà possibile stabilire se tali atti siano, o meno, concretamente e finalisticamente proiettati alla realizzazione dello stesso[59]. Ne consegue che saranno "diretti in modo non equivoco" gli atti tipici, previsti dalla norma, o quelli che siano di stretta anticipazione rispetto a questi ultimi[60].

---

[57] Ancora SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 229.

[58] A titolo esemplificativo si consideri la condotta di un *hacker* il quale, nascondendosi dietro all'identità di un utente legittimo, spedisce all'*account* di un ufficio pubblico dei messaggi di posta elettronica contenenti un *malware* autoeseguibile opportunamente occultato; in questi casi l'attitudine offensiva − idoneità − della condotta rispetto al bene giuridico non dovrà valutarsi astrattamente, ma in concreto, *ex ante*, in termini di adeguatezza alla prosecuzione dell'*iter criminis*, mentre l'univocità dovrà essere accertata sulla base della sua prossimità alla consumazione del reato perseguito. In altre parole i criteri dei reati a consumazione anticipata devono necessariamente essere oggetto di una valutazione inserita nel contesto in cui si realizzano e in rapporto al la commissione dell'evento cui sono indirizzati.

[59] Per approfondimento si veda SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 230.

[60] Così cfr. MANTOVANI, *Diritto penale. Parte generale* cit., 441.

In conclusione, tanto il requisito dell'idoneità offensiva, quanto quello della univocità degli atti, non andranno apprezzati in astratto bensì in concreto, tenendo conto - nel caso in cui questi non siano tipizzati dalla norma - anche del piano criminoso del soggetto attivo[61].

5. L'elemento soggettivo: il problema della compatibilità tra tentativo e dolo eventuale

Entrambi i delitti sottoposti ad analisi nel presente capitolo sono puniti a titolo di dolo generico; sarà, quindi, sufficiente, per l'integrazione dell'elemento soggettivo, che vi sia la volontà del soggetto attivo di commettere atti − concretamente idonei e diretti in modo non equivoco a cagionare uno degli eventi di danno, nonché la coscienza della qualifica "pubblica" degli oggetti materiali su cui agiscono le condotte[62].

Merita di essere sottolineata una differenza rispetto alla previsione della fattispecie *ex* art 420 c.p., che i delitti in esame hanno sostituito dopo la riforma del settore dei *cybercrimes* operata dalla l. 48/2008; infatti, quando le fattispecie erano ancora collocate nella parte del codice dedicata ai «delitti contro l'ordine pubblico», la dottrina manifestava l'esigenza che l'elemento soggettivo fosse integrato dalla coscienza di compiere un atto in grado di mettere in pericolo l'ordine pubblico. In ragione della nuova collocazione sistematica della norma, tale requisito non può più essere richiesto; tuttavia, in linea con i principi generali, si richiede che il soggetto attivo abbia piena consapevolezza di agire contro beni materiali di «pubblica utilità»[63].

Un tema generale ed estremamente dibattuto che riguarda l'elemento soggettivo, valutato rispetto alla più ampia categoria dei delitti a consumazione

---

[61] Si veda SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 231.

[62] Si veda sul punto CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 804.

[63] Per approfondimento cfr. BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza* cit., 1148; l'Autore, a sua volta, riprende le posizioni di varia ed autorevole dottrina, tra tutti si segnala FIANDACA, MUSCO, *Diritto penale. Parte speciale*, I, cit., 7 ss.

anticipata, in quanto punibile già al livello del tentativo, consiste nella compatibilità con la figura del dolo eventuale[64].

La questione può essere affrontata anche in una diversa prospettiva, cioè se l'elemento soggettivo del tentativo − necessariamente doloso − sia perfettamente identico al dolo del reato consumato; in caso di risposta affermativa sarà possibile, se non anche obbligatorio, includere il dolo eventuale nelle forme di dolo configurabili nell'ambito del delitto tentato e, per quanto attiene al tema del presente paragrafo, in quanto compatibile, nell'ambito dei delitti di attentato − *ivi* incluse le fattispecie di danneggiamento informatico "pubblico" *ex* artt. 635 *ter* e *quinquies* c.p.

La dottrina, così come la giurisprudenza, si è divisa in due opposti schieramenti che adducono alle loro posizioni diverse motivazioni teoriche ed ermeneutiche.

Una parte minoritaria della dottrina, la quale opta per l'inclusione del dolo eventuale nelle figure dei delitti tentati, muove dal presupposto che nell'ordinamento nazionale penale non è riscontrabile alcuna norma che effettui un'esplicita distinzione tra l'elemento soggettivo doloso del tentativo e quello

[64] Brevissimi cenni sulla, già di per sé controversa, figura del dolo eventuale: si tratta dell'ipotesi margine dell'elemento soggettivo doloso − terza "sottocategoria", che si aggiunge al dolo diretto e al dolo intenzionale − la cui problematicità emerge dal suo collocarsi concettualmente in una zona limite con la c.d. "colpa cosciente"; senza ripercorrere tutto l'i*ter* giurisprudenziale e le diverse posizioni in dottrina, si recupera qui la più rilevante, nonché recente, pronuncia delle Sezioni Unite che, tra le altre e numerose questioni, si è espressa anche in riferimento al dolo eventuale: Cass. Pen., Sez. Un., 18.09.2014, n. 38343, in *Foroplus*, *https://www.foroplus.it/home.php.*, anche nota come sentenza Thyssenkrupp; come anticipato, uno dei punti più importanti della sentenza in commento attiene alla distinzione tra dolo eventuale e colpa cosciente, secondo cui «in ossequio al principio di colpevolezza la linea di confine tra dolo eventuale e colpa cosciente va individuata considerando e valorizzando la diversa natura dei rimproveri giuridici che fondano l'attribuzione soggettiva del fatto di reato nelle due fattispecie»; spiegano i giudici che, nel caso della colpa cosciente, il rimprovero mosso verso il soggetto attivo riguarda un malgoverno di un rischio, della mancata adozione di cautele idonee ad evitare l conseguenze pregiudizievoli; si tratta di inadeguatezza rispetto al «dovere precauzionale». In tale figura manca l'elemento della volontà. Diversamente, nel dolo eventuale vi si deve includere anche l'elemento volitivo; in particolare i giudici hanno affermato che «nel dolo eventuale [...] un atteggiamento interiore assimilabile alla volizione dell'evento e quindi rimproverabile, si configura solo se l'agente prevede chiaramente la concreta, significativa possibilità di verificazione dell'evento e, ciò non ostante, si determina ad agire, aderendo a esso, per il caso in cui si verifichi. Occorre la rigorosa dimostrazione che l'agente si sia confrontato con la specifica categoria di evento che si è verificata nella fattispecie concreta». Sul punto, per approfondimento si rimanda a MARINI, *Thyssenkrupp: quella sottile linea di confine tra dolo eventuale e colpa cosciente*, in *Altalex*, 2014, *https://www.altalex.com/documents/news/2014/10/06/thyssenkrupp-quella-sottile-linea-di-confine-tra-dolo-eventuale-e-colpa-cosciente* nella manualistica si rimanda a FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 379 ss.; MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 393 ss.

degli illeciti consumati. Le differenze che sono individuate dalle norme tra queste due figure attengono esclusivamente alla struttura "oggettiva" delle stesse, ricavandone che, il dolo, proprio dell'elemento "soggettivo" delle fattispecie, sia quello del tentativo che quello della consumazione, non possono che coincidere[65].

Sempre alla medesima conclusione si arriva, secondo tale dottrina, se si considera che il requisito dell'"univocità" debba intendersi secondo una concezione strettamente oggettiva: si sostiene, cioè, che la direzione non equivoca delle condotte, si riferisca esclusivamente all'elemento oggettivo della fattispecie di tentativo, non potendosi riflettere anche sull'elemento soggettivo sotto forma di intenzione diretta a commettere il fatto[66].

Tale orientamento, considerato dalla dottrina maggioritaria come eccessivamente rigoroso, è motivato da due ragioni di fondo. Da un lato emerge la preoccupazione general-preventiva che spinge la giurisprudenza ad applicare il trattamento sanzionatorio più rigoroso, in ipotesi in cui esso pervenga dalla configurazione di un delitto tentato doloso − come ad esempio il «tentato omicidio» − in luogo di un altro reato realizzato, a cui conseguono pene più lievi − per proseguire nell'esempio appena riportato, sarebbe il caso del delitto di «lesione dolosa». Dall'altro vi sono ragioni di semplificazione probatoria: i giudici di un tempo, che optavano in favore dell'inclusione del dolo eventuale, di fronte a comportamenti particolarmente equivoci, «non si sforzavano nell'effettiva ricerca dell'intenzione dell'agente», accontentandosi di presumere che il soggetto attivo fosse consapevole del rischio, o della possibilità, di cagionare eventi maggiormente lesivi rispetto a quelli direttamente voluti[67].

---

[65] Ricostruzione offerta, ma non condivisa, da FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 493.

[66] In questo senso sono riscontrabili anche pronunce delle Sezioni Unite che, però, non sono state in grado di imporre un orientamento alle sezioni inferiori: Cass. Pen., Sez. Un. 18.06.1983, n. 6309, in *Cassazione penale*, II, 1984; Cass. Pen., Sez. Un., 14,05,1996, n. 2, in *Altalex*, *https://www.altalex.com/documents/news/2004/10/19/cassazione-penale-ss-uu-sentenza-14-02-1996-n-2*

[67] Così si esprime FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 493. Tra i maggiori esponenti della tesi espressa si segnala MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 564. L'Autore in questione, in particolare, accogliendo l'argomento dell'"univocità" sopra esposto a sostegno della sua posizione, chiarifica le sue disquisizioni con un esempio pratico che si riporta: il caso di un soggetto che, fuggendo dal luogo dove aveva commesso una rapina, spara in direzione degli inseguitori per farli desistere dall'inseguimento, non al fine di uccidere ma per sottrarsi dalla cattura, pur rappresentandosi la possibilità − ed

La tesi opposta, che ritiene incompatibili la figura dei delitti tentati − e quelli di attentato − e il dolo eventuale, trova maggior sostegno in dottrina ed ha vissuto una progressiva affermazione anche nella giurisprudenza di legittimità[68].

A sostegno, si potrebbe affermare, in diretta inversione rispetto alla posizione di cui sopra, la concezione strettamente soggettiva, e probatoria, dell'"univocità" quale requisito del tentativo; in questo senso si ridurrebbe la "non equivocità" delle condotte alla necessità di provare in giudizio l'intenzione criminosa dell'agente, coincidendo, quindi, questa con «la prova di una volontà intenzionale a commettere il reato»; richiedendosi una «volontà intenzionale», è inevitabile escludere il dolo eventuale dall'elemento soggettivo delle fattispecie di tentativo. Ad ogni modo la concezione soggettiva dell'"univocità" è da tempo stata superata[69].

La tesi dell'incompatibilità può, comunque, poggiarsi su altre argomentazioni. In primo luogo, l'autonomia strutturale del tentativo, rispetto alla corrispondente consumazione, giustificherebbe una diversa connotazione peculiare anche per l'elemento soggettivo doloso. Dall'altro rimane comunque ferma l'incompatibilità tra il dolo eventuale − caratterizzato da un costante stato di dubbio concettuale[70] − e il requisito dell'"univocità", pur abbracciando la concezione oggettiva.

In conclusione si può anche rilevare che, conformemente al modo di ritenere il tentativo nel generale senso comune, si dovrebbe riconoscere che comunque le condotte devono essere orientate verso uno scopo, vale a dire la realizzazione dell'evento lesivo, e non la «accettazione del rischio di un evento possibile o probabile»[71].

La dottrina maggioritaria sostiene, in sintesi, che la direzione finalistica della condotta deve essere certa sia sul piano materiale, che su quello dell'elemento soggettivo, ovvero psicologico. Una condotta che sia realizzata non

---

accettandone il rischio − di uccidere qualcuno; in questo caso l'Autore afferma che il reo possa sicuramente rispondere per il delitto di tentato omicidio.

[68] Si segnalano tra tutte: Cass. Pen., Sez. VI, 16.04.2012, n. 14342, in *Foroplus, https://www.foroplus.it/home.php.*; Cass. Pen., Sez. I, 23.12.2019, n. 51870, in *Foroplus, ivi;* Cass. Pen., Sez. I, 17.01.2020, in *Foroplus, ivi.*

[69] Cfr. FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 493

[70] Sul punto si veda MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 564.

[71] Per approfondimento v. FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 493.

verso la realizzazione di un evento, ma solo per la mera accettazione del rischio che si verifichi, non può di certo dirsi "univoca", né dal punto di vista oggettivo, né tantomeno da quello soggettivo[72].

Orientando nuovamente l'attenzione ai delitti di danneggiamento di dati o sistemi informatici di «pubblica utilità» *ex* artt. 635 *ter* e *quinquies* c.p., in considerazione della particolare ampiezza degli eventi e della difficoltà, sopra riportata, di definire la soglia minima di rilevanza del tentativo, la dottrina maggioritaria di settore sembrerebbe proiettata verso la tesi che nega la rilevanza del dolo eventuale[73].

6. Gli eventi "aggravatori" e le altre circostanze aggravanti specifiche

Entrambe le fattispecie *ex* artt. 635 *ter* e *quinquies* c.p. prevedono, al secondo comma, un sensibile aumento della cornice sanzionatoria «se dal fatto» derivi l'evento verso cui le condotte − concretamente idonee − sono dirette in modo non equivoco. Quello che viene configurato dalle disposizioni appena indicate è un'ipotesi di evento aggravatore rispetto alla fattispecie principale, alla cui verificazione è collegata la minaccia, da parte dell'ordinamento, di un trattamento sanzionatorio decisamente più elevato.

Prima di valutare il preciso contenuto delle disposizioni in parola, è necessario affrontare i temi sviluppatisi in dottrina che si legano indissolubilmente alla generale figura dei reati aggravati dall'evento. Innanzitutto, si identificano come "aggravati dall'evento" quei reati che prevedono un aumento di pena al verificarsi di un evento che sia ulteriore rispetto ad un fatto che già autonomamente costituisce reato[74].

In un tempo ormai passato, agli albori della disciplina penalistica nazionale, la figura del reato aggravato dall'evento costituiva un esempio classico di responsabilità oggettiva, l'espressione più tipica dell'antico principio «*qui in re*

[72] A sostegno si segnala MANTOVANI, *Diritto penale. Parte generale* cit., 461 ss.; allo stesso modo sembrerebbe orientarsi FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 494.
[73] Cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 805.
[74] Così FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 688.

illicita versatur tenetur etiam pro casu»[75]: alla stregua di suddetto principio, l'evento aggravatore si legava alla condotta dell'agente solo attraverso un rapporto di causalità materiale (il nesso causale). L'evoluzione dogmatica che ha certamente subito la figura in parola[76] ha, ad oggi, riconsegnato un'incerta e problematica categoria nozionistica[77].

Le ricostruzioni di autorevoli Autori, consentono di suddividere le fattispecie di reati aggravati dall'evento in tre diverse categorie, basandosi sul rapporto che intercorre tra la volontà colpevole del soggetto agente e l'evento stesso[78]. La prima fa riferimento ad ipotesi in cui l'evento aggravatore non possa, o non debba, essere voluto dal soggetto agente, potendoli indicare come reati "necessariamente involontari", in ragione del fatto che la diretta volontarietà determinerebbe la configurazione di una diversa fattispecie − si pensi ad esempio agli artt. 571 e 572 c.p., rubricati rispettivamente «abuso dei mezzi di correzione o di disciplina» e «maltrattamenti contro familiari o conviventi»[79].

Un secondo gruppo include i reati rispetto ai quali l'evento aggravatore si pone in rapporto di "indifferenza psicologica", essendo del tutto ininfluente che questo sia voluto o meno dal soggetto attivo; in questi casi dalla volontarietà dell'agente non scaturirebbe alcuna variazione del titolo imputato − un esempio in tal senso è il reato di «calunnia» *ex* art. 368 c.p., rispetto al quale il fatto che dalla

[75] Noto brocardo latino, letteralmente «chi si trova in condizione di illiceità è responsabile anche per il caso fortuito».

[76] Su tutti di può citare l'evoluzione storica avvenuta in riferimento al principio di rango costituzionale di colpevolezza, in ragione del quale, come si vedrà con precisione in seguito, si tende ad escludere ipotesi di mera responsabilità oggettiva.

[77] Cfr. FIANDACA, MUSCO, *ibidem.*

[78] La categorizzazione qui riportata è indicata da SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 232; altri autori offrono suddivisioni che, seppur qualificate a livello terminologico diversamente, sul piano contenutistico si allineano. Su tutti FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 689, il quale individua 2 gruppi, a seconda che sia indifferente o meno che la volontà del soggetto agente ricopra anche l'evento più grave. MANTOVANI, *Diritto penale. Parte generale* cit., 395, suddivide invece i reati in parola in 4 gruppi: quelli in cui l'evento non può essere voluto; quelli in cui non può che essere voluto; quelli in cui non deve essere voluto, quelli in cui può essere o non essere voluto.

[79] I delitti riportati a titolo esemplificativo, prevedono, entrambi, eventi aggravatori, consistenti, in estrema sintesi, nella lesione o nella morte delle persone su cui ricadono le condotte principali; se suddetti eventi fossero direttamente voluti, e quindi coperti dall'elemento psicologico doloso, si configurerebbero le rispettive e più gravi fattispecie autonome. Ne consegue che, per rimanere entro i confini degli artt. 571 e 572 c.p., sarà necessario che l'evento aggravatore non sia voluto dal soggetto attivo.

condotta calunniosa derivi una condanna, non determina modifiche se non in relazione al trattamento sanzionatorio[80].

L'ultima categoria si riferisce ai reati aggravati dall'evento in cui quest'ultimo deve essere necessariamente voluto dal soggetto attivo; in questo gruppo vengono, solitamente, ricondotti i delitti a consumazione anticipata, principalmente quelli diretti contro la personalità dello Stato, ma sicuramente includendovi anche i delitti di danneggiamento informatico avverso dati e programmi «di pubblica utilità»[81].

Invero, in dottrina è discussa l'assimilazione dei reati in cui l'evento qualificante debba necessariamente essere voluto dall'agente − e quindi i delitti di attentato − alla generale categoria dei delitti aggravati dall'evento; secondo alcuni autori, l'inclusione nella suddetta categoria sarebbe solo apparente, avendo, i delitti "necessariamente volontari", in comune con questa solo il dispositivo normativo − «se dal fatto deriva» − ma non anche la struttura tipica[82].

A differenza delle prime due categorie, correttamente etichettate come delitti aggravati dall'evento, in cui questo può essere non voluto o comunque del tutto irrilevante, nella terza la necessaria volontarietà dell'evento ulteriore deriva dalla − di nuovo necessaria − dolosità, e quindi volontarietà, che costituisce l'elemento soggettivo della fattispecie di attentato. In altre parole, essendo che le condotte, le quali configurano pienamente il delitto di attentato, concretamente idonee e dirette in maniera non equivoca a cagionare l'evento, devono essere coperte dall'elemento soggettivo doloso, l'eventuale realizzarsi del suddetto evento non può che essere altrettanto voluto.

---

[80] Sulla categorizzazione rispetto a questi primi due gruppi, autorevole dottrina sostiene che essa, piuttosto che rispecchiare differenze strutturali dei reati aggravati dall'evento, persegue l'esigenza di disciplinare ipotesi di «interferenza» tra le fattispecie in questione e le altre norme di illeciti penali presenti nell'ordinamento. La questione, quindi, atterrà ai problemi sul "concorso di norme", risolvibili attingendo ai criteri del diritto penale sostanziale in materia di concorso apparente. Cfr. FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 689.

[81] Cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 232.

[82] Così SALVADORI, *ibidem*, citando una più datata autorevole dottrina: GALLO, *Delitti aggravati dall'evento e delitti di attentato*, in *Giur. it.*, n. 11, 1990, 1001 ss. L'Autore afferma infatti che «la tecnica che il legislatore può avere usata sarà magari identica a quella utilizzata per configurare i delitti aggravati dall'evento ma, se è certo che l'evento aggravatore è voluto, come lo sono l'azione dolosa o l'evento che precedono, l'assimilazione di queste forme a quelle dei delitti aggravati dall'evento è di pura apparenza, dato che in realtà la sostanza è tutt'altra».

Fatte le dovute premesse, la questione centrale consiste nell'identificare la corretta natura giuridica dei reati in esame, in assenza di un'espressa previsione legislativa, da cui dipendono una serie di importanti conseguenze pratiche sul piano della disciplina giuridica penalistica.

Se al momento della prima emanazione del codice penale era del tutto fuori discussione che la categoria dei delitti aggravati dall'evento rientrasse integralmente nelle ipotesi di responsabilità oggettiva − ritenendo, quindi, che l'evento aggravatore fosse attribuibile al soggetto attivo solo per il tramite del nesso di causalità − ad oggi le diverse posizioni della dottrina nel dibattito teorico individuano due alternative: l'inquadramento formale dei reati in esame tra le figure di reato circostanziato, ovvero tra le fattispecie autonome di reato[83].

Messa in questa prospettiva, già in tempi lontani l'opinione prevalente sosteneva che i delitti aggravati dall'evento fossero tutti da ricondurre ai reati circostanziali[84]. Altra parte della dottrina, invece, riconosceva la mancanza di una natura unitaria, potendosi, quindi, rinvenire sia ipotesi di reati circostanziali, sia fattispecie autonome di reato.

Secondo la dottrina contemporanea, superando l'approccio della dogmatica astratta e privilegiando il terreno dei criteri di imputazione della responsabilità soggettiva dei fatti di reato, si dovrebbe favorire, oggi la soluzione che tende a rendere i delitti in esame compatibili con il principio di colpevolezza[85]. Una tale soluzione può facilmente raggiungersi riconducendo i reati aggravati dall'evento alla categoria delle fattispecie circostanziate, sopratutto alla luce della riforma avvenuta per il tramite della l. 19/1990 che ha rimodulato il modello di imputazione delle circostanze aggravanti del reato, estendendovi formalmente il principio della «*nulla poena sine culpa*»[86].

---

[83] Sul punto si rimanda a FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 690. Per la disciplina generale dei reati circostanziati, vale a dire fattispecie su cui incidono elementi accessori − circostanze − che determinano una variazione quantitativa o qualitativa della pena, nella manualistica si veda tra tutti FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 433 ss.; MARINUCCI, DOLCINI, GATTA, *Manuale di Diritto Penale. Parte Generale* cit., 655 ss.; MANTOVANI, *Diritto penale. Parte generale* cit., 395 ss.

[84] Cfr. RICCIO, *I delitti aggravati dall'evento*, Napoli, 1936, 122.

[85] Per approfondimento si veda FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 690.

[86] Con la legge 7.02.1990 n. 19 il legislatore ha, tra le altre cose, modificato il testo dell'art. 59 c.p., stabilendo ora al comma 2 che «le circostanze che aggravano la pena sono valutate a carico dell'agente soltanto se da lui conosciute ovvero ignorate per colpa o ritenute inesistenti per errore

Si venne così a configurare, per le circostanze aggravanti, una logica di responsabilità basata su «qualcosa di simile alla colpa», intesa come coefficiente minimo, sottoforma di conoscenza o conoscibilità dell'elemento che integra la circostanza. Ovviamente a tale regime di responsabilità soggettiva delle circostanze non si sottraggono gli eventi ulteriori e successivi di fattispecie autonome aggravate dall'evento[87].

Rimangono, comunque, presenti forme di perplessità rispetto ad altri profili derivanti dal predetto inquadramento; si fa particolare riferimento all'art. 69 c.p., il quale contiene la norma che regola il bilanciamento degli aumenti e delle diminuzioni di pena a seguito dell'applicazione di elementi circostanziali. Per questo motivo rimane ancora aperta la questione circa la qualificabilità della categoria dei reati aggravati dall'evento che, in attesa di una presa di posizione da parte del legislatore, dovrà risolversi caso per caso[88].

Ritornando ad incentrare l'analisi sui delitti di cui al secondo comma degli artt. 635 *ter* e *quinquies* c.p., si può dire che essi rientrerebbero − pur segnalando a riguardo, ancora una volta, i dubbi di diversi autori[89] − nella categoria dei delitti aggravati dall'evento, in cui questo risulti necessariamente investito dalla volontarietà del soggetto agente.

Non è, quindi, oggetto di dubbi o contestazioni in dottrina il grado di imputazione soggettiva − evidentemente dolosa − del verificarsi dell'evento verso cui sono dirette le condotte punite ai sensi dei commi 1 delle norme in parola; ciò che, invece, rimane tema di dibattito è la qualificazione delle disposizioni *ex* artt. 635, co. 2, *ter* e *quinquies* c.p., da cui si determinerebbe l'applicabilità, o meno, dell'art. 69 c.p.

Si segnala che la dottrina maggioritaria considera le norme in esame come fattispecie autonome di reato, considerando quindi il realizzarsi della «distruzione, deterioramento, ecc.» di dati o sistemi informatici di «pubblica utilità» non come

---

determinato da colpa»; con preciso riguardo alle circostanze aggravanti si è passati da un regime di imputazione oggettiva ad uno di imputazione soggettiva.

[87] Così sul punto FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 690; l'autore aggiunge poi che in riferimento agli eventi aggravatori, più che conoscenza o conoscibilità si dovrà richiedere al soggetto agente «rappresentazione o rappresentabilità, ovvero anche previsione o prevedibilità».

[88] Cfr. FIANDACA, MUSCO, *Diritto penale. Parte generale* cit., 691.

[89] Sul punto GALLO, *Delitti aggravati dall'evento e delitti di attentato* cit.; ma anche più recente SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 232.

elemento «circostanziale», ma come elemento costitutivo di un autonoma fattispecie di reato; da ciò ne conseguirebbe che, come già affermato, non possa eseguirsi l'operazione di bilanciamento *ex* art. 69 c.p., né applicarsi la generale disciplina dei reati circostanziati *ex* art. 59 c.p.[90].

Un Autore in particolare, presenta alcuni elementi che facciano ritenere plausibile che il legislatore abbia voluto considerare le disposizioni in esame come autonoma fattispecie di reato: innanzitutto l'aumento «esorbitante» di pena previsto dal comma 2 degli artt. 635 *ter* e *quinquies* c.p., non previsto come aumento della sanzione di cui al comma 1, ma stabilito in modo indipendente e autonomo. Altro elemento sarebbe costituito dalla locuzione di apertura «se dal fatto deriva», sebbene si segnala che tale espressione è propria della maggior parte dei reati aggravati dall'evento. Infine, la conclusione sarebbe rafforzata dal raffronto con il terzo comma delle norme, che prevede in entrambi i casi, la configurazione di due circostanze aggravanti ad effetto comune, sicuramente applicabili, secondo l'Autore, sia alle ipotesi del primo comma, che a quella del secondo[91].

Si segnalano, comunque, in dottrina posizioni che sostengono la qualificazione delle disposizioni in esame quali circostanze aggravanti, etichettando gli artt. 635 *ter* e *quinquies* c.p. come reati circostanziati, riconoscendo l'applicazione della generale disciplina *ex* art, 59 c.p., ed in particolar modo, il giudizio di bilanciamento disposto dall'art. 69 c.p.[92].

A livello strettamente contenutistico, riguardo quali a siano gli eventi aggravatori rilevati dalle norme, l'art. 635 *ter*, co. 2, c.p. effettua un perfetto parallelismo rispetto alle ipotesi base del primo comma, giacché sono previsti gli stessi cinque eventi, vale a dire la «distruzione», il «deterioramento», l'«alterazione», la «cancellazione» e la «soppressione» di dati, informazioni o programmi informatici di «pubblica autorità».

---

[90] A sostegno su tutti SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 232; MANTOVANI, *Diritto penale. Parte speciale II* cit., 155. Pur ricostruendo in maniera approfondita la questione, non si espone, invece CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 806.

[91] Così si esprime PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715.

[92] A sostegno si segnalano FIANDACA, MUSCO, *Diritto penale. Parte speciale* cit., 150; BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza* cit., 1147.

Nell'art. 635 *quinquies*, co. 1, c.p., invece, non si rinviene il medesimo parallelismo, essendo previsti come eventi aggravatori solamente la «distruzione» il «danneggiamento» e la «procurata, totale o parziale inservibilità» di sistemi informatici o telematici di «pubblica utilità», escludendo, senza apparente motivo, l'ipotesi del «grave ostacolo al funzionamento»[93].

Al comma 3 degli artt. 635 *ter* e *quinquies* c.p. sono, invece, inserite le due circostanze aggravanti, specifiche, ad effetto comune; esse prevedono un trattamento sanzionatorio più grave se il fatto è commesso «mediante violenza alla persona o con minaccia», ovvero per l'aver «abusato della qualità di operatore di sistema». Essendo perfettamente identiche alle circostanze aggravanti delle fattispecie di danneggiamento di dati o sistemi informatici "privati", per la loro analisi contenutistica e per la risoluzione di questioni controverse, si rimanda al paragrafo dedicato nel precedente capitolo[94].

7. Il trattamento sanzionatorio e la procedibilità

Avendo a riguardo il tema del trattamento sanzionatorio, si segnala che il legislatore ha previsto per entrambi gli artt. 635 *ter* e *quinquies* c.p. le medesime pene: la reclusione da uno a quattro anni nell'ipotesi base di attentato, di cui al comma 1; la reclusione da tre a otto anni laddove si realizzino gli eventi verso cui le condotte sono dirette, *ex* co. 2 artt. 635 *ter* e *quinquies* c.p.

Circa le scelte del legislatore riguardanti la cornice sanzionatoria dei reati in parola, diversi esponenti della dottrina si sono pronunciati in senso critico. Sia per le previsioni di attentato che per quelle di evento le pene previste determinano un'evidente incoerenza sistematica rispetto alle altre fattispecie di danneggiamento informatico c.d. "privato": la pena della reclusione da uno a quattro anni, per il danneggiamento di dati, informazioni e programmi di «pubblica utilità» risulta, infatti, «solo» lievemente superiore rispetto a quella prevista dalla corrispettiva fattispecie "privata", mentre per il danneggiamento di sistemi informatici e

[93] Per approfondimento si veda CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 806.
[94] Si veda *supra* Cap. 2, par. 6.

telematici, l'ipotesi di attentato dispone un trattamento sanzionatorio addirittura più lieve rispetto al sabotaggio informatico *ex* art. 635 *quater* c.p.[95].

In questo modo non può dirsi raggiunto l'obbiettivo di creare un regime "speciale", sensibilmente più severo dal punto di vista sanzionatorio, che offrisse maggior tutela al bene giuridico, in ragione della qualificabilità "pubblica", attraverso l'adozione della struttura di delitti a consumazione anticipata; il medesimo, se non migliore, effetto si sarebbe raggiunto strutturando gli artt. 635 *ter* e *quinquies* c.p., al pari degli artt. 635 *bis* e *quater* c.p., come fattispecie di danno, potendo comunque conservare la punibilità a titolo di tentativo[96].

Allo stesso modo, in controsenso rispetto alla volontà di creare una coerenza sistematica tra i delitti di danneggiamento, le pene dedicate alle ipotesi di delitto consumato di cui al comma 2 degli artt. 635 *ter* e *quinquies* c.p., vale a dire la reclusione da tre a otto anni, risultano essere di molto più gravi, forse anche eccessivamente severe, sia in sé considerate, sia rapportate all'economia del complesso dei delitti di danneggiamento[97].

Ulteriore elemento suscettibile di contestazione, sempre in contrasto con la sistematicità dei delitti in esame, è la previsione delle medesime pene per i due articoli di danneggiamento informatico "pubblico". A voler trovare una giustificazione alla scelta del legislatore di applicare lo stesso trattamento sanzionatorio, si può notare come, probabilmente, questo sia un vecchio retaggio dell'abrogato testo dell'art. 420, co. 2 e 3, c.p., convertito negli artt. 635 *ter* e *quinquies* c.p.[98] tuttavia non ci si può esimere dal sottolineare che una siffatta scelta di politica criminale non tenga minimamente conto della differenza di

[95] Per approfondimento cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 808.
[96] In questo modo si esprime PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715.
[97] Così CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 808. Allo stesso modo si esprime PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa* cit., 715; l'Autore tenta di giustificare il vertiginoso aumento delle pene rispetto ai corrispettivi danneggiamenti "privati" in considerazione del fatto che, nel primo caso, e non nel secondo, ci si trovi di fronte a delitti a consumazione anticipata. Nella stessa direzione si muovono i commenti rilasciati da SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 237.
[98] Cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 808.

disvalore tra gli attacchi a «meri» dati, informazioni e programmi informatici, e i sistemi informatici o telematici, «di pubblica utilità»[99].

Parimenti, la previsione normativa di un medesimo trattamento sanzionatorio per entrambe le fattispecie analizzate risulterebbe in evidente, seppur implicito, contrasto con le fonti sovranazionali. Non sarebbero, infatti, rispettate le disposizioni indicate dalla Convenzione del Consiglio d'Europa in materia di criminalità informatica, la quale, come già affermato, prevede due articoli diversi per le ipotesi di danneggiamento − *ex* artt. 5 e 6 − distinti sulla base del diverso bene materiale oggetto delle condotte − da una parte dati, informazioni, dall'altra i sistemi. Il legislatore avrebbe dovuto adempiere a questa differenziazione in tutti gli aspetti delle norme incriminatrici, *ivi* incluso il trattamento sanzionatorio[100].

In ultima battuta si segnala che entrambe le fattispecie, previste dagli artt. 635 *ter* e *quinquies* c.p., sono sempre procedibili d'ufficio.

8. Il rapporto tra reati

Affrontando il tema del rapporto tra reati, parallelamente rispetto a quanto detto sui delitti *ex* artt. 635 *bis* e *quater* c.p., questo può valutarsi in due direzioni: sia rispetto al "microsistema" dei delitti di danneggiamento informatico, sia verso fattispecie esterne.

Sul primo punto si segnala che anche l'art. 635 *ter* c.p., parimenti alle due norme di danneggiamento "privato", contiene, in apertura di disposizione, la clausola di salvaguardia espressa «salvo che il fatto costituisca più grave reato». La presenza di tale clausola in tre delle quattro fattispecie riconducibili al "microsistema" lascerebbe intendere la volontà del legislatore di creare uno schema di gravità progressiva, ponendo al vertice l'art 635 *quinquies* c.p., per l'appunto sprovvisto della suddetta clausola. In altre parole la clausola di salvaguardia è posta a presidio di eventuali conflitti tra le norme del

[99] Si veda a riguardo SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 237.

[100] Per approfondimento si vedano SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici* cit., 237; PICOTTI, *La ratifica della Convenzione cybercrime del Consiglio d'Europa* cit., 716; CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 808.

"microsistema" in ipotesi di concorso tra i suddetti delitti, divenuto possibile a seguito della quadruplicazione delle norme operata dalla l. 48/2008[101].

È però, altresì, vero che, in ragione dei discorsi relativi alla previsione delle medesime pene per i delitti di cui agli artt. 635 *ter* e *quinquies* c.p., risulti formalmente impossibile determinare la maggiore gravità del secondo rispetto al primo; tale risultato si può ottenere solo in via interpretativa, facendo cioè riferimento ad una logica sistematica − quando ad essere attaccati sono contemporaneamente dati e sistemi informatici − senza poter fare affidamento alla «certezza» derivante dalla clausola di sussidiarietà espressa[102].

Rispetto ai rapporti con fattispecie esterne al "microsistema" la stessa clausola garantisce l'eventuale applicabilità di delitti contro l'incolumità pubblica.

Volendo essere più dettagliati, si possono prendere a riferimento due fattispecie specifiche, esterne al sistema dei delitti di danneggiamento, rispetto alle quali potrebbero crearsi problemi legati al rapporto tra norme.

La prima riguarda il delitto *ex* art. 615 *quinquies* c.p., rubricato «detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico». Sebbene siano riscontrabili opinioni opposte, la dottrina maggioritaria afferma che l'art 615 *quinquies* c.p., costituendo una forma di reato di ostacolo alla funzione di vigilanza ai beni materiali informatici, il realizzarsi del pericolo costituirà una condotta strettamente prodromica, e quindi riassorbita rispetto a quelle sanzionate dagli artt. 635 *bis* c.p. e seguenti; così intesa la fattispecie *ex* art 615 *quinquies* c.p. non concorrerà con alcuna delle norme di danneggiamento informatico[103].

La seconda consiste nell'art. 615 *ter* c.p., segnatamente al comma 2 n. 3 e al comma 3; si è già avuto modo di valutarne le criticità rispetto ai delitti *ex* artt. 635 *bis* e *quater* c.p.[104], mentre si valuteranno ora quelle che emergono in riferimento all'art. 635 *ter* c.p. In considerazione dell'entità della pena − reclusione

[101] Cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 807.
[102] Sul punto CAPPLELLINI, *ibidem.*
[103] In questo senso, su tutti, cfr. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 817. In direzione opposta arrivano le analisi di BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza* cit., 1167.
[104] V. *supra* Cap. 2, par. 8.

da tre a otto anni per l'ipotesi aggravata *ex* art. 615 *ter*, co. 3, c.p. − vi è chi ha sostenuto che la fattispecie di accesso abusivo aggravato dalla qualifica dell'oggetto materiale fosse speciale rispetto al delitto di danneggiamento in parola, includendovi, appunto, anche il bene materiale di «dati pubblici», con la conseguenza che quest'ultimo finirebbe per essere assorbito dal comma 3 *ex* art. 615 *ter* c.p.[105].

Tuttavia la presenza della clausola di chiusura «o comunque di interesse pubblico» porrebbe dei legittimi dubbi circa la specialità dell'oggetto materiale della presente disposizione rispetto al danneggiamento *ex* art. 635 *ter* c.p.; in aggiunta si consideri che, pur ammettendo tale regime di specialità «si assisterebbe al paradosso per cui l'offesa a oggetti materiali meno rilevanti, perché non rientranti nel novero degli speciali *ex* art. 615 co. 3, *ter*, sarebbe punita più gravemente mediante il concorso tra l'art. 635 *ter* e l'ipotesi base di accesso abusivo a sistema informatico»[106].

La probabile soluzione andrebbe ricercata nella differenza del regime di imputazione (anche non doloso) dell'evento aggravatore. Per cui, se l'evento fosse doloso, si applicherebbe il concorso tra la norma *ex* art 635 *ter* c.p. e la fattispecie base di accesso abusivo a sistema informatico; laddove, invece, il delitto fosse non doloso, ma almeno prevedibile o conoscibile in concreto, si applicherebbe esclusivamente l'ipotesi dell'art. 615 *ter* c.p. aggravata dalla realizzazione dell'evento previsto al terzo comma[107].

[105] Così BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza* cit., 1149 s.
[106] In questo senso si esprime CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici* cit., 817.
[107] Cfr. CAPPELLINI, *ibidem*.

CAPITOLO IV

LA TUTELA DELL'INTEGRITÀ DEI DATI E DEI SISTEMI INFORMATICI QUALE IMPRESCINDIBILE ESIGENZA DEGLI ENTI SOVRANAZIONALI, NAZIONALI E PRIVATI

1. Cyberterrorismo: definizione e contrasto sovranazionale

Nel presente capitolo si approfondiranno alcuni dei principali settori in cui emerge, in maniera prevalente, la necessità di tutelare l'integrità dei dati e dei sistemi informatici nonché, più in generale, di arginare il c.d. "rischio *cyber*"[1].
I soggetti, chiamati ad adoperare gli strumenti ed attuare le modalità organizzative e preventive, che sono rese disponibili, se non anche obbligatorie, dalle discipline di settore, in quanto concretamente idonee alla suddetta tutela, verranno di volta in volta identificati, a seconda dell'ambito in cui ci si muove.

In queste prime pagine si tratterà l'ampio fenomeno terroristico, il quale, negli ultimi due decenni, ha subito un mutamento sostanziale[2]; non vi è qui l'intenzione di fornire un'analisi del terrorismo, considerato nella sua generale essenza, né tantomeno dal punto di vista strettamente storico-evolutivo, piuttosto si vogliono considerare le numerose e diverse implicazioni della tecnologia e del mondo *cyber*. L'evoluzione alla quale si fa riferimento può giustificarsi per due ordini di ragioni: da una parte l'adozione delle organizzazioni terroristiche, di strutture militari e, conseguentemente, di strategie tipiche dei comandi militari; dall'altra, invece, l'implementazione e il crescente utilizzo delle tecnologie informatiche, sia per le fasi preparatorie ed organizzative, sia per quelle strettamente esecutive, o successive, di attentati, attraverso lo sfruttamento di informazioni, programmi informatici, ovvero notizie pubblicate su testate giornalistiche online.

---

[1] V. *supra* Cap. I, par. 1.
[2] È possibile individuare un'evoluzione a partire dalla fase dei più noti attentati di inizio millennio − New York nel 2001 o Londra nel 2005 − rispetto a quelli propri della più recente ondata terroristica di provenienza "mediorientale" − a partire dall'attentato alla sede di Charlie Hebdo nel 2015 o comunque quelli perpetrati dalla nota organizzazione terroristica dell'ISIS (*Islamic State of Iraq and Sirya*) cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia*, in WENIN, FORNASARI (diretto da), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, 2015, 325.

Con il passare del tempo e, sopratutto, in ragione del progresso tecnologico ed informatico, il terrorismo ha adottato con eccezionale precisione quelle caratteristiche di indeterminatezza e volatilità che hanno complicato in maniera esponenziale le strategie e le capacità di contrasto degli Stati nazionali e delle organizzazioni internazionali, ma ancor di più ha dimostrato un'incredibile flessibilità nello sfruttare i più sofisticati strumenti della rivoluzione informatica, nonché le numerose "aperture" della complessa società occidentale create attraverso la digitalizzazione[3]. Tutto ciò ha portato la c.d. "guerra asimmetrica"[4] anche nel *cyber* spazio.

Internet, la struttura del *web* e la nuova dimensione del *cloud*[5] hanno, poi, fatto in modo che il fenomeno terroristico assumesse dimensioni e caratteristiche del tutto nuove, proprie dei c.d. *cyber crimes*, in una scala esponenzialmente più grave: dalla delocalizzazione delle risorse, alla "detemporalizzazione" delle attività che possono essere pianificate, programmate, eseguite da remoto, se non anche automatizzate; si perde la necessità del collegamento diretto o fisico tra il soggetto e il sistema informatico, e si garantisce la "deterritorializzazione" dell'utente, che ha così la facoltà di compiere operazioni complesse "trovandosi presente virtualmente" in diversi "spazi informatici" contemporaneamente[6].

Si deve poi tener conto che la maggior parte degli utenti conosce, o quantomeno utilizza, solo una piccola parte di tutto ciò che la rete è in grado di offrire; si fa riferimento al c.d. *deep web*, ossia uno spazio virtuale colmo di risorse non indicizzate dai numerosi motori di ricerca, a cui è possibile accedere

---

[3] Per approfondimento si rimanda a VIGNERI, *Cyberterrorismo: realtà o finzione? Profili problematici di definizione e contrasto*, in *Altalex*, 2018, *https://www.altalex.com/documents/news/2018/09/06/cyberterrorismo-profili-problematici-di-definizione-e-contrasto*.

[4] Così viene etichettato il tipico conflitto tra stati nazionali ed organizzazioni terroristiche. Su tutti si segnala GAGLIANO, *La guerra asimmetrica e la strategia moderna*, in *Osservatorio globalizzazione*, 2019, *https://osservatorioglobalizzazione.it/osservatorio/guerra-asimmetrica-gagliano-giuseppe/*. L'Autore effettua riflessioni sul concetto elaborato da BAUD, *la guerre asymétrique ou la défaite du vainqueur*, 2003.

[5] Il termine nella sua interezza si identifica come *cloud computing*, letteralmente "nuvola informatica"; «termine con cui ci si riferisce alla tecnologia che permette di elaborare e archiviare dati in rete. In altre parole, attraverso *internet* il c.c. consente l'accesso ad applicazioni e dati memorizzati su un *hardware* remoto invece che sulla *workstation* locale» così in *enciclopedia Treccani online*, *https://www.treccani.it/enciclopedia/cloud-computing*. Per una spiegazione strettamente tecnica si rimanda a FURTH, ESCALANTE, *Handbook of Cloud Computing*, Berlino, 2018.

[6] Sul punto si veda FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 326.

solo attraverso determinati programmi o *software*, all'interno del quale è concesso compiere ogni tipo di attività − legale o illegale − al di fuori di qualsiasi controllo pubblico[7]. In questo complesso panorama si innesta il c.d. *cyber*-terrorismo.

La forte dipendenza del moderno assetto sociale, economico e politico dalla digitalizzazione e dalla rete globale rende particolarmente allarmante la minaccia del *cyber* terrorismo. Tale fenomeno, anche se non ben definito, è sicuramente rappresentativo del ruolo che la tecnologia informatica svolge nel pianificare o eseguire attacchi terroristici. Si pensi poi che gli stessi sistemi informatici o le banche dati nazionali, pubbliche o private, ovvero anche i dati in esse contenuti possono costituire i *target* designati degli attacchi.

Il primo passo della presente analisi definirà i contorni concettuali della nozione di *cyber* terrorismo, tentando di fornirne in via indiretta una definizione, pur sapendo che non ne è riscontrabile alcuna in nessuna fonte normativa nazionale o sovranazionale.

Innanzitutto, per ragioni di stretta strumentalità alla ricostruzione che ci si appresta a compiere, parrebbe opportuno accogliere, tra le molteplici definizioni di terrorismo, quella che, sul piano fenomenico, risulta essere la più ampia e generica, la quale lo identifica come «l'uso illegale della forza o della violenza, o la minaccia di tale uso, connotati da fini politici, ideologici o religiosi, contro persone o beni, per intimidire o coartare un governo o la popolazione civile, anche sul piano psicologico»[8]; in questo modo si ricomprende anche la definizione di «atti aventi finalità terroristica» riscontrabile nel codice penale italiano all'art. 270 *sexies* c.p., secondo cui le condotte sono connotate dalla suddetta finalità se, per loro natura o il loro contesto, possono arrecare grave danno ad un Paese o un'organizzazione internazionale, ovvero se sono realizzate allo scopo di intimidire o costringere Stati o le medesime organizzazioni a compiere atti volti a

[7] Per approfondimento sul tema si rimanda a RIJTANO, *Cosa sono il Deep Web e il Dark Web, cosa si trova e come si accede: tutte le istruzioni*, in *Cybersecurity360*, 2022, *https://www.cybersecurity360.it/cultura-cyber/cose-il-deep-web-e-il-dark-web-cosa-si-trova-e-come-si-accede-tutte-le-istruzioni/*.

[8] Così FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 330.

distruggere o destabilizzare le strutture politiche, costituzionali, economiche o sociali[9].

Al fine del discorso in parola, poi, è possibile suddividere in tre categorie gli atti che sono generalmente ricondotti al *cyber* terrorismo, ciascuna caratterizzata da elementi propri: innanzitutto ci si riferisce agli atti che vengono realizzati tramite la rete telematica o altre tecnologie, che possono cagionare il danneggiamento o l'alterazione di sistemi informatici o telematici sensibili, propri dello Stato o altri enti pubblici, ovvero anche il danneggiamento di dati o informazioni *ivi* archiviati. In secondo luogo si fa riferimento ad atti di publicizzazione o divulgazione di contenuti illegali, attraverso la rete *web*, per la diffusione di opinioni o ideologie di stampo razzista o xenofobo, nonché per effettuare propaganda al fine di reclutamento, ovvero anche di raccolta fondi. Da ultimo si include il gruppo di atti che, attraverso l'uso di *internet* e altre tecnologie, permettono comunicazioni tra gruppi o individui terroristici, nel completo anonimato o attraverso la delocalizzazione del flusso di dati, nonché della sensibile diminuzione delle tempistiche della comunicazione[10].

Altra classificazione del fenomeno si basa sul ruolo della tecnologia e dell'*internet*. In primo luogo si riconoscono i casi in cui le tecnologie informatiche sono solo uno dei mezzi attraverso i quali si realizzano gli attacchi terroristici, potendo ciò accadere sia nella fase preparatoria che in quella esecutiva. Nel secondo gruppo, invece, si riconducono le ipotesi in cui gli strumenti informatici risultano essenziali per la realizzazione dell'attacco terroristico, oppure ne costituiscono l'obbiettivo, vale a dire l'oggetto su cui tali attentati ricadono − a titolo esemplificativo si può immaginare un attacco realizzato per forzare le

[9] Per approfondimento sul punto su tutti si rimanda a FIANDACA, MUSCO (a cura di), *Diritto penale. Parte speciale*, *Volume I*, 7ª ed., 2015, Bologna, 17 ss. Tra l'altro si segnalano brevemente alcuni rilievi critici, riscontrati in dottrina circa la previsione nel nostro ordinamento di atti aventi finalità di terrorismo, in ragione del fatto che la definizione sopra riportata abbraccia solamente la prima parte della disposizione contenuta nella Decisone quadro 2002/475/GAI, sostituita poi, in definitiva, dalla direttiva UE/541/2017, tralasciando poi l'elenco degli «atti intenzionali» che, secondo la decisione quadro, sarebbero dovuti essere i soli a meritare la qualifica di "reati terroristici", quando, cioè, «per la loro natura o contesto possono arrecare grave danno a un paese o a un'organizzazione internazionale» e siano commessi al fine di «intimidire gravemente la popolazione, costringere indebitamente i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto, o destabilizzare gravemente o distruggere le strutture politiche fondamentali, costituzionali, economiche o sociali di un paese o un'organizzazione internazionale», cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 332.
[10] Per approfondimento v. FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 333 s.

misure di sicurezza di un sistema informatico, minando l'integrità e la segretezza, nonché la sicurezza, dei *computer systems* e dei dati *ivi* contenuti[11].

Su quest'ultima categorizzazione si è basato un dibattito che, in ambito accademico, ha posto e sviluppato la questione definitoria del *cyber* terrorismo. La maggior parte della dottrina accoglie la posizione c.d. *target oriented*, secondo cui possono effettivamente considerarsi atti di terrorismo informatico quelli che, attraverso l'utilizzo di *internet* o altre tecnologie informatiche, danneggiano o compromettono i sistemi informatici o le infrastrutture informatiche critiche di un dato Paese o di un'organizzazione internazionale; la rete costituirebbe, quindi, l'obbiettivo e l'arma dell'attentato. L'altra e diversa posizione, invece, ritiene di dover includere anche tutte le condotte c.d. *tool oriented*, dove la rete risulta "solo" uno strumento di supporto, inerente, come si è detto, ad attività di organizzazione, propaganda, comunicazione o proselitismo. Sarebbe quindi qualificabile come *cyber* terrorismo qualsiasi utilizzo di *internet* o altre tecnologie informatiche da parte di organizzazioni terroristiche[12].

Volendo orientarsi verso la prima posizione è individuabile, nella dottrina internazionale che la sostiene, una possibile definizione del fenomeno in parola, la quale prevede che per terrorismo informatico si intenda «*the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage*»[13]. Si intenderebbe quindi per *cyber* terrorismo, un attacco, o una minaccia di attacco, avverso i *computer*, le reti e le informazioni in essi memorizzati, eseguito con lo scopo di intimidire o costringere uno Stato, ovvero anche un'organizzazione internazionale, ad assoggettarsi ad obbiettivi politici o sociali; tale attacco dovrebbe poi caratterizzarsi per violenza contro persone o cose, o comunque per il fatto di essere in grado di arrecare danni ingenti, tali, come minimo, da alimentare paura[14].

---

[11] Cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 333.
[12] Contributo offerto da VIGNERI, *Cyberterrorismo: realtà o finzione?*, cit.
[13] Così DENNING, *Activism, hacktivism, and cyberterrorism: the internete as a tool for influencing foreign policy*, in ARQUILLA, RONFELDT (a cura di) *Networks and netwars. The future of terror, crime and militancy*, Santa Monica, 2001.
[14] La medesima dottrina afferma che «*an example would be penetrating an air traffic control system and causing two planes to collide*», cioè ipotesi che portano a morte o lesioni, ma anche

L'elemento caratterizzante degli atti qualificabili come *cyber* terroristici sarebbe, quindi, il causare, o il poter causare, mediante violenza avverso individui o proprietà fisiche, danni sufficienti per incutere un diffuso senso di paura tra la popolazione; in sostanza, l'attenzione viene posta sull'impatto che tali azioni terroristiche raggiungono, individuabile in relazione all'obbiettivo perseguito mediante l'attentato. Se, infatti, gli attacchi avessero ad oggetto servizi non essenziali, o causassero danni lievi, di piccola entità, non potrebbero considerarsi alla stregua di azioni terroristiche avverso infrastrutture critiche[15].

Quella appena analizzata rimane comunque una questione aperta, posto che non vi è alcuna formale definizione del fenomeno del *cyber* terrorismo nelle varie discipline di settore, nazionali o sovranazionali. È tuttavia a queste che si volgerà adesso l'attenzione. In particolare, l'Unione Europea si è dotata, attraverso una serie di provvedimenti, di un asseto normativo pensato ed elaborato per la lotta contro il terrorismo, includendovi articoli e disposizioni dedicate specificamente al fenomeno terroristico *online*[16].

Si segnala preventivamente che, con l'entrata in vigore del trattato di Lisbona − nel 2007 − sia la criminalità informatica che il terrorismo sono stati inseriti nelle materie ricomprese dall'art. 83, par. 1, TFUE, inserendole, quindi tra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione ha competenza Penale[17]. È però da ben prima delle modifiche apportate dal trattato di Lisbona che l'Unione Europea ha dimostrato attenzione verso i suddetti temi, emanando già nel 2002 il primo provvedimento dedicato alla repressione del fenomeno terroristico: la decisione quadro 2002/475/GAI.

---

attacchi ad infrastrutture critiche, incluse quelle informatiche, a seconda dell'impatto. Cfr. DENNING, *Activism, hacktivism, and cyberterrorism* cit.

[15] Per approfondimento cfr. VIGNERI, *Cyberterrorismo: realtà o finzione?*, cit. Secondo l'Autore è, infatti, importante non confondere il fenomeno di «vero e proprio» *cyber* terrorismo, connotato da violenza fisica cagionata attraverso strumenti informatici nel *cyberspace* sfruttandone la capacità offensiva, con un utilizzo degli stessi con "mere" finalità terroristiche, quali proselitismo o propaganda. Essi sono fenomeni palesemente diversi; una condotta qualificata come *cyber* terroristica, manifesta la sua specificità ben oltre la sola presenza dell'organizzazione sul *web*.

[16] Bisogna rilevare che, relativamente alle condotte di *cyber* terrorismo c.d. *target oriented*, ancora non si sono verificati eventi così classificabili, sebbene l'utilizzo della rete da parte delle organizzazioni terroristiche avvenga giornalmente; sarà quindi sulle condotte e sugli effetti c.d. *tool oriented* che incideranno le legislazioni relative all'utilizzo di tecnologie informatiche da parte delle suddette organizzazioni. Cfr. VIGNERI, *Cyberterrorismo: realtà o finzione´* cit.

[17] V. *supra* Cap. I, par. 3.2.

Riguardo all'indicata decisione quadro si segnalano alcuni punti rilevanti per il tema che si sta affrontando in questa sede: innanzitutto all'art. 1 vincola gli Stati membri ad adottare le misure necessarie affinché siano considerati atti terroristici quelli indicati dall'elenco contenuto nel medesimo articolo; tra questi vi si ricomprende anche la «distruzione di vasta portata di [...] infrastrutture, compresi i sistemi informatici»[18]; all'art. 4 del medesimo provvedimento si obbligano gli Stati alla criminalizzazione del tentativo e dell'istigazione di ciascuno dei reati previsti dall'art. 1, par. 1; circa il profilo sanzionatorio, gli Stati vengono obbligati ad adottare sanzioni penali «effettive, proporzionali e persuasive»[19], prevedendo poi, per fatti riconducibili a reati terroristici, una reclusione più severa rispetto a quella che verrebbe applicata in caso di medesime condotte in assenza della finalità terroristica.

Un provvedimento successivo, la direttiva 2017/541/UE, che sostituisce tutte le precedenti decisioni quadro in materia di normativa anti-terrorismo, sembrerebbe aver colto maggiormente quella "convergenza" tra *cyberspace* e terrorismo di cui si parlava poc'anzi. Tra le nuove disposizioni che aggiornano la disciplina alle nuove manifestazioni di crimini terroristici si segnalano: l'obbligo degli Stati membri di criminalizzare «se compiuta intenzionalmente, la diffusione o qualunque altra forma di pubblica divulgazione di un messaggio, con qualsiasi mezzo, sia online che *offline*, con l'intento di istigare alla commissione di uno dei reati [...] di terrorismo»[20]; si specifica poi, nel *considerandum* n. 10, che nei reati riconducibili alla pubblica provocazione per commettere delitti di terrorismo vi è inclusa «la diffusione *online* e *offline* di messaggi o immagini, comprese quelle riguardanti le vittime del terrorismo, quale mezzo per raccogliere sostegno alle cause dei terroristi o intimidire gravemente la popolazione»[21].

Sempre in riferimento alla strumentalizzazione di tecnologie informatiche per fini terroristici, segnatamente alla diffusione di materiale di stampo terroristico *online*, una grande novità della direttiva in esame, consiste nella previsione di una serie di disposizioni relative alla rimozione alla fonte − comma

[18] Art. 1, par. 1, lett. d), decisione quadro 2002/475/GAI.
[19] Art. 5, par. 1, decisione quadro 2002/475/GAI.
[20] Art. 5, par. 1, direttiva 2017/541/UE.
[21] *Considerandum* n. 10, direttiva 2017/541/UE.

1 − ovvero, laddove ciò non fosse possibile, all'obbligo − comma 2 − di adottare misure per bloccare l'accesso a tali contenuti in rete − *ex* art. 21 direttiva 2017/541/UE. Il terzo comma del medesimo articolo richiede poi che «le misure relative alla rimozione e al blocco devono essere stabilite secondo procedure trasparenti e fornire idonee garanzie, in particolare, al fine di assicurare che tali misure siano limitate allo stretto necessario e proporzionate e che gli utenti siano informati del motivo di tali misure»; vi si include anche la possibilità di ricorrere per via giudiziale, a tutela delle garanzie connesse alla rimozione o al blocco dei materiali di cui sopra[22].

La centralità del tema dei contenuti divulgati online a sfondo propagandistico si rileva facilmente ponendo attenzione al fenomeno dei c.d. "lupi solitari"; si tratta di soggetti estremisti che operano isolatamente negli stessi paesi occidentali in cui vivono, organizzandosi autonomamente o in gruppi ridotti e destrutturati, rispetto ai quali i materiali divulgati *online* giocano un ruolo centrale: sia per la propaganda terroristica che tende a radicalizzarli e indurli alla commissione di attentati, così come anche per l'ottenimento di informazioni meramente educative circa l'uso e la costruzione di armi o esplosivi[23].

Suddetta situazione ha fatto emergere una forma di responsabilità sociale delle piattaforme *online* per la protezione degli utenti dall'esposizione a contenuti terroristici; la maggior parte degli enti privati operanti nel settore di divulgazione informatica hanno messo in atto una serie di misure volontarie per contrastare i contenuti terroristici sui loro servizi[24]. Tali sforzi delle piattaforme informatiche, grazie anche a una maggiore cooperazione tra i soggetti privati e quelli pubblici,

[22] Art. 21, par. 3, direttiva 2017/541/UE.

[23] Per approfondimento si rimanda a MARTORANA, PINELLI, *Terrorismo sul web e contenuti online: il nuovo regolamento UE*, in *Altalex*, 2021, *https://www.altalex.com/documents/news/2021/05/25/terrorismo-web-contenuti-online-nuovo-regolamento-europeo.*

[24] Si pensi ad esempio al Forum Internet dell'Unione Europea, avviato nel 2015 ed inserito periodicamente nell'agenda europea sulla sicurezza informatica e *governance* aziendale, che prevede la partecipazione di diverse autorità nazionali nonché dell'Unione stessa, oltre a numerose piattaforme online, partner internazionali e ricercatori. Cfr. *Forum dell'UE su Internet: responsabilità condivise di governi e piattaforme per garantire la sicurezza online*, in *Rappresentanza in Italia*, 2022, *https://italy.representation.ec.europa.eu/notizie-ed-eventi/notizie/forum-dellue-su-internet-responsabilita-condivise-di-governi-e-piattaforme-garantire-la-sicurezza-2022-12-07_it.*

hanno sicuramente portato ad un oggettivo miglioramento che, però, non ha risolto il problema.

La Commissione dell'Unione Europea ha rilevato, come tre le cause del successo parziale delle suddette misure adottate dagli enti privati si individua principalmente quella del carattere volontario di questa forma di cooperazione, «da cui è disceso il numero complessivamente ridotto dei prestatori di servizi coinvolti nella collaborazione, nonché la lentezza e la parzialità del processo di rimozione dei contenuti illeciti»[25]. A tali valutazioni hanno dato seguito il Consiglio ed il Parlamento Europeo, dapprima con un accordo provvisorio per l'adozione di un nuovo regolamento relativo alla diffusione di contenuti terroristici *online* nel 2020, per poi arrivare all'approvazione definitiva del suddetto regolamento UE 784/2021.

Il nuovo provvedimento introduce un più chiaro ed armonizzato quadro giuridico, definendo le responsabilità degli Stati membri e gli obblighi dei prestatori di servizi di *hosting*[26] di individuare e rimuovere, rapidamente ed in modo efficace, i contenuti terroristici *online* dalle loro piattaforme[27].

Tra le numerose previsioni del regolamento in parola si segnalano: l'introduzione dello strumento dell'ordine di rimozione − art. 3 − che obbliga i prestatori di servizi, operanti nel territorio dell'Unione indipendentemente dalla sede principale dell'attività, verso cui è rivolta la disciplina, a rimuovere i contenuti terroristici *online*, ovvero a disabilitarne l'accesso entro il termine massimo di un ora, a pena di imposizione di sanzioni; l'obbligo per ciascuno Stato membro di individuare almeno una autorità competente − artt. 12 e 13 − per l'emanazione degli ordini di rimozione, individuare e segnalare i contenuti di stampo terroristico, sorvegliare l'attuazione delle misure imposte ai *providers* e,

[25] Per approfondimento sul punto si rimanda a PEZZUTO, *Contenuti terroristici on line: l'unione europea lavora a nuove norme per prevenirne la diffusione*, in *Diritto penale contemporaneo*, 2019, *https://archiviodpc.dirittopenaleuomo.org/d/6603-contenuti-terroristici-on-line-l-unione-europea-lavora-a-nuove-norme-per-prevenirne-la-diffusione*.

[26] Individuati dalla disposizione dell'art. 2 reg. UE 784/2021 − che richiama esplicitamente la definizione di cui all'articolo 1, lettera b), della direttiva (UE) 2015/1535 − secondo cui sono "servizi di *hosting*" quelli che «consistono nel memorizzare le informazioni fornite dal fornitore di contenuti su richiesta di quest'ultimo» così art. 2, reg. UE 784/2021. Per approfondimento sugli *internet service provider* cfr. IASELLI, *Internet Service Provider. Guida all'ISP: cos'è, regime e tipologie di responsabilità* cit., si veda pure *supra* Cap I, par. 1.

[27] Per approfondimento v. MARTORANA, PINELLI, *Terrorismo sul web e contenuti online: il nuovo regolamento UE* cit.

più in generale, monitorare il rispetto delle disposizioni previste dal regolamento. Numerosi obblighi sono poi previsti per gli operatori di servizi di *hosting*, tra cui l'esecuzione dell'obbligo di rimozione − art. 4 − la valutazione delle segnalazioni − art. 5 − l'adozione di misure proattive e di trasparenza − art 6 − e la conservazione dei materiali rimossi − art. 7.

Sempre indirizzato ai soggetti prestatori dei servizi di *hosting* vi è un generale obbligo di diligenza, consistente nell'adottare misure adeguate, ragionevoli e proporzionate, finalizzate a garantire la sicurezza dei propri servizi; tale obbligo non è comunque da considerarsi come un generale obbligo di vigilanza in capo ai *providers*[28].

Da ultimo si segnalano una serie di misure atte a salvaguardare e garantire il pieno rispetto delle libertà fondamentali degli utenti, su tutti la libertà di pensiero, di espressione ed informazione, tra cui: l'obbligo di informare l'utente nel caso in cui un suo contenuto venga rimosso − art. 11 − e la previsione di efficaci meccanismi di reclamo e ricorso giudiziario − artt. 9 e 10[29].

1.1. Cyberterrorismo e diritto penale nazionale

Volgendo ora l'attenzione all'ordinamento interno, segnatamente al diritto penale, si segnala in via preventiva che non si rinviene una fattispecie che tipizzi in senso unitario il fenomeno del *cyber* terrorismo. Si accoglie in questa sede la definizione fornita dalla dottrina internazionale, precedentemente individuata, che individua l'elemento centrale del *cyber* terrorismo nella "convergenza tra *cyberspace* e condotte terroristiche"[30] − ricoprendo anche le operazioni di attacco informatico mosso da motivazioni politiche, realizzate per causare gravi danni alle istituzioni, all'economia e all'integrità fisica.

Lo specifico disvalore del fenomeno terroristico informatico, quindi, sembrerebbe riscontrarsi nella combinazione tra due elementi: da un lato l'atteggiamento psicologico, di natura politica, ideologica, religiosa, ecc.; dall'altro la direzione offensiva dell'attacco, che dovrebbe avere come obbiettivo la società

[28] Per il più generale tema della individuabilità di una posizione di garanzia in capo agli ISP nel *cyberspace* si veda *supra* Cap. I, par 1.
[29] Per una completa ricostruzione del contenuto del reg. UE 784/2021, si veda MARTORANA, PINELLI, *Terrorismo sul web e contenuti online: il nuovo regolamento UE* cit.
[30] Cfr. DENNING, *Activism, hacktivism, and cyberterrorism* cit., 241.

civile[31]. La combinazione di questi due fattori, vale a dire la "convergenza" di cui sopra, influenza le scelte di politica criminale, sicurezza interna e politica estera, determinando l'adozione di misure preventive nonché l'emanazione di fattispecie applicabili[32].

Allo stesso modo la "convergenza", che rappresenta il fulcro del fenomeno, permette di adottare una duplice prospettiva di analisi, rispetto alla disciplina di diritto penale nazionale, applicabile al terrorismo informatico: da un lato la normativa dei *cyber crimes*, dall'altra la legislazione "tradizionale" antiterroristica.

Al fenomeno del *cyber* terrorismo, ovvero a una qualsiasi delle componenti fenomeniche ad esso ricollegate − ad es. diffusione di messaggi a scopo propagandistico o ai fini di addestramento − possono, potenzialmente, trovare applicazione, in quanto compatibili, diverse fattispecie incriminatrici proprie della categoria dei *cyber crimes*.

Si può, ad esempio, pensare ad un attacco informatico diretto a danneggiare, distruggere, cancellare, ecc., dati o programmi informatici utilizzati dallo Stato o altro ente pubblico, che integrerà i delitti *ex* artt. 635 *ter* e *quinquies* c.p.; il medesimo discorso può effettuarsi in ipotesi di accesso abusivo a sistema informatico con l'obbiettivo di sottrarre informazioni per poter, successivamente, commettere un attentato, in tal caso sarà applicato l'art. 615 *ter* c.p.

In sostanza, non sembrerebbero rinvenibili particolari lacune, in considerazione del fatto che il nostro ordinamento si è dotato di un livello minimo di strumenti normativi, nel settore della criminalità informatica, di prevenzione e contrasto, che possono essere inquadrate nel fenomeno del *cyber* terrorismo[33]. Tuttavia la medesima dottrina richiede un eventuale intervento legislativo riguardante l'impianto sanzionatorio rispetto a fatti realizzati con "finalità di terrorismo" e, per questo, considerati particolarmente gravi[34].

---

[31] Così FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 335.
[32] Sul punto si rimanda a DENNING, *Activism, hacktivism, and cyberterrorism* cit., 288.
[33] Per approfondimento FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 340.
[34] Si veda FLOR, *ibidem.* Anche altri Autori condividono questa riflessione, riscontrando una situazione di «irrazionalità sanzionatoria» rispetto a diverse ipotesi di reati informatici, quando commessi con finalità terroristiche, e quindi avendo ad oggetto sistemi informatici che risultano essere fondamentali nella società dell'informazione «in settori strategici, legati al mantenimento della pace sociale» cfr. VIGNERI, *Cyberterrorismo: realtà o finzione?*, cit.

Anche la disciplina interna in materia di antiterrorismo può trovare applicazione al fenomeno qui analizzato, seppur con non poche difficoltà ermeneutiche. Si prenda a riferimento l'art. 270 *quinquies* c.p. − «addestramento ad attività con finalità di terrorismo anche internazionale» − il quale rivolge il trattamento sanzionatorio non solo a chi addestra o fornisce informazioni per la realizzazione di attentati, ma anche alla persona che viene addestrata, nonché a chi ha acquisito, anche autonomamente, le istruzioni per il compimento di atti «univocamente finalizzati alla commissione delle condotte di cui all'art. 270 *sexies*»[35].

Rispetto alle modalità del *cyber* terrorismo, la fattispecie risulta astrattamente applicabile sia a colui che, con finalità di terrorismo, attraverso il *web*, fornisce informazioni − si pensi a materiale informativo, circa la realizzazione di ordigni, divulgato nel c.d. *deep web*[36] − sia a chi, tramite ricerche nella rete, assume autonomamente un *know-how* funzionale alla realizzazione di attentati, se gli atti sono univocamente finalizzati alla realizzazione delle condotte *ex* art. 270 *sexies* c.p.[37].

L'inserimento dell'ultima clausola contenente il riferimento all'art. 270 *sexies* c.p., secondo parte della dottrina, dovrebbe evitare atti diretti al mero ottenimento di informazioni; una siffatta lettura ermeneutica, tuttavia, sembrerebbe in contrasto con l'evidente intenzione del legislatore di sanzionare anche condotte di "auto addestramento". La disposizione, infatti, fa riferimento a qualsiasi comportamento − «avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo» ovvero anche «ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di

[35] Si aggiunge il secondo comma che prevede un trattamento sanzionatorio più grave se il fatto di cui al primo comma è commesso attraverso strumenti informatici o telematici, ma con esclusivo riferimento al soggetto che «addestra o istruisce». In realtà la dottrina tende a criticare la previsione di questa circostanza aggravante, non comprendendo la scelta del legislatore di prevedere un aumento di pena per l'utilizzo di strumenti − quelli informatici − che, nel panorama della modernità, risultano tutt'altro che straordinari. Cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 346 s. in aggiunta, l'Autore afferma che «da un lato, tale scelta è apparentemente giustificata dalle potenzialità offerte dalla rete», d'altra parte però si prevede così «*ex lege* una presunzione di maggiore offensività del mezzo impiegato, che prescinde dalla verifica della concreta idoneità della condotta a integrare o provocare la commissione dei delitti».

[36] Si veda *supra* par. 1.

[37] L'art. 270 *sexies* c.p. è rubricato «condotte con finalità di terrorismo» e contiene la generale definizione dell'ordinamento nazionale penale della "finalità terroristica", di cui si è già parlato nelle pagine precedenti; v. *supra* par. 1.

servizi pubblici essenziali, con finalità di terrorismo» − soggettivamente rivolto a commettere delitti con finalità di terrorismo, consentendo l'incriminazione di qualsiasi atto preparatorio alla realizzazione di tale fine[38].

Se si tiene conto del fatto che la disposizione contenuta nell'art. 270 *sexies* c.p. esprime una nozione − quella di «finalità di terrorismo» − notoriamente ampia e indeterminata, si colgono le ragioni per cui la dottrina maggioritaria si esprime, riferendosi alle disposizioni in commento, parlando di «esasperazione repressiva», includendo potenzialmente anche attività di mera raccolta di informazioni sul *web*.

In ogni caso, si richiede al giudicante un impegno nell'accertare in concreto l'univocità della finalità terroristica, compito da considerarsi assai complesso, sopratutto in considerazione della previsione «fuori dei casi di cui all'art. 270 *bis*» − rubricato «associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico». Tale finalità dovrà trovare un riscontro concreto in elementi oggettivi che dimostrino l'idoneità dei comportamenti esaminati e, allo stesso tempo, la pericolosità dell'informazione − divulgata o ricercata − si dovrà valutare guardando, non solo alla sua natura, ma anche al contesto in cui si inserisce, ed al modo in cui è veicolata[39].

Dal punto di vista del *cyber* terrorismo, essendo l'ipotesi di cui all'art. 270 *quinquies* c.p. classificabile anche come reato informatico − inserito, sul piano sistematico, tra i reati informatici c.d. "impropri"[40] − l'interpretazione della condotta di acquisizione di informazioni, "univocamente finalizzata", deve essere adattata anche al contesto tecnologico. Anche in questo caso il fulcro del disvalore sociale, e quindi la soglia di punibilità delle condotte, consiste nell'astratta

[38] Tale riflessione è condivisa da FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 342 s. Allo stesso modo si pronuncia anche VIGNERI, *Cyberterrorismo: realtà o finzione?*, cit.

[39] Cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 344. È possibile riscontrare anche pronunce della Suprema Corte di Cassazione relativamente a questo tema. Su tutte Cass. Pen., Sez. I, 9.09.2015, n. 40699. In riferimento all'art. 270 *quater* c.p. la Corte afferma che per la nozione di "arruolamento" si deve «escludere che nell'ipotesi prevista dall'art. 270 quater sia necessario l'inquadramento dell'arruolato in una vera e propria struttura di tipo militare, dovendosi invece ritenere, anche alla luce dell'espresso riferimento operato dalla norma incriminatrice alle finalità di terrorismo, che il concetto di "arruolamento" corrisponda a quello di "ingaggio", inteso come il raggiungimento di un "serio accordo" tra il soggetto che propone il compimento, in forma organizzata, di più atti di violenza o di sabotaggio, con finalità di terrorismo, ed il soggetto chiamato ad aderire ad una tale proposta».

[40] Sulle classificazioni dei reati informatici si rimanda a *supra* Cap. I, par. 2

idoneità delle informazioni e delle istruzioni alla realizzazione di quei fatti indicati dall'art. 270 *sexies* c.p., congiuntamente con la concreta comprensione delle stesse da parte dell'autore, affinché egli possa realizzare i fatti indirizzati alle condotte di cui al medesimo articolo[41].

Adottando questa impostazione ermeneutica si è in grado di valorizzare il tentativo del legislatore di delimitare l'area di punibilità delle condotte − specificamente − *ex* art. 270 *quinquies* c.p., nonché, in generale, delle fattispecie della disciplina nazionale di anti-terrorismo. In questo senso la scelta politico-criminale appare certamente condivisibile, in quanto tutte le condotte − incluse quelle di mero ottenimento di informazioni di stampo terroristico − risulteranno idonee purché sussista il «decorso causale» tra informazioni, comprensione, assimilazione ed utilizzo[42].

Viceversa, la semplice detenzione o memorizzazione, nella memoria di un sistema informatico o di un qualsiasi *device*, di istruzioni relative, ad esempio, alla realizzazione di un ordigno esplosivo, non assumono di per sé rilevanza penale; non saranno quindi sufficienti all'integrazione della fattispecie *ex* art. 270 *quinquies* c.p.

Un discorso analogo può effettuarsi anche in riferimento all'art. 270 *bis* c.p. − «associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico» − il quale punisce chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si pongono come obbiettivo il compimento di atti con finalità di terrorismo. Tali condotte possono, infatti, eseguirsi mediante tecnologie informatiche, ovvero ricorrendo ad *internet* e *social networks*; si richiederà, però, che la struttura organizzativa abbia un grado di effettività tale da rendere possibile l'attuazione del progetto criminoso, e da giustificare così la valutazione di pericolosità, congiuntamente con l'idoneità della struttura al compimento dei reati per la cui realizzazione l'associazione terroristica è stata istituita[43].

In conclusione, è possibile cogliere come il *cyber* terrorismo sia un fenomeno ibrido, al quale, in Italia, è applicabile sia la disciplina anti terrorismo,

[41] Sul punto si veda VIGNERI, *Cyberterrorismo: realtà o finzione?*, cit.
[42] Cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 345.
[43] In questo modo si esprime FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 346.

sia quella sui reati informatici. In merito a questo rapporto, autorevole dottrina ha colto come «la disciplina italiana, se applicata al fenomeno cyber-terrorismo, sembra però sconfinare verso una demonizzazione della rete e degli strumenti informatici, che rischia di limitare in modo sproporzionato le libertà individuali costituzionalmente protette»[44]. È, infatti, vero che l'attenzione del legislatore in materia di *cyber* terrorismo è stata incentrata nella necessità di anticipare la soglia della rilevanza penale, per fornire una risposta preventiva e tempestiva alle esigenze di tutela rispetto a condotte terroristiche, includendovi e sanzionando, però, in questo modo, anche quelle meramente prodromiche.

Si deve necessariamente evitare che l'arretramento della soglia di punibilità sconfini verso la repressione di forme di manifestazione del pensiero e della libertà di espressione, che in *internet* trovano un ambiente estremamente favorevole; in questo contesto il giudice ricopre un ruolo centrale per scongiurare tale rischio. Per poter adempiere adeguatamente a questa responsabilità e costituire un più efficace contrasto al *cyber* terrorismo, sia il legislatore che il giudice, devono superare il limite di una «condizione di inferiorità cognitiva, che nel peggiore dei casi si traduce in un approccio casistico culturalmente arretrato»[45].

2. Reati informatici e responsabilità degli enti: D.Lgs. 231/2001

Il decreto 231[46], come è ben noto, ha rappresentato una novità dirompente nel sistema penale italiano, superando il tradizionale principio *societas delinquere non potest*, configurando una forma di responsabilità dipendente da reato che, per la prima volta, si rivolge agli enti collettivi[47].

---

[44] Cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia* cit., 354.
[45] Riflessioni espresse da VIGNERI, *Cyberterrorismo: realtà o finzione?*, cit.
[46] Decreto legislativo 8 giugno 2001, n. 231, recante «disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica», a norma dell'art. 11, legge 29 settembre 2000, n. 30.
[47] La produzione manualistica in riferimento alla disciplina del decreto 231 è sterminata; su tutti si segnalano GROSSO, PADOVANI, PAGLIARO (a cura di), *Trattato di diritto penale. Parte generale*, Vol IV, Milano, 2008, 1 ss.; LATTANZI (a cura di), *Reati e responsabilità degli enti: guida al d.lgs. 8 giugno 2001, n. 231*, 2 ed., Milano, 2010, 1 ss.; PELISSERO, *Responsabilità degli enti*, in ANTOLISEI, *Manuale di diritto penale. Leggi complementari*, Vol II, Milano, 2018, 741 ss.; LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti: diritto sostanziale*, Vol 1, Torino, 2020.

In estrema sintesi[48], con il decreto 231/2001 viene introdotto un nuovo paradigma punitivo[49], che determina l'applicabilità di una vasta gamma di sanzioni nei confronti di un ente collettivo − rientrante tra i possibili destinatari della disciplina[50] − laddove uno dei c.d. "reati presupposto", individuati dal medesimo decreto[51], sia stato commesso, nel suo interesse ovvero a suo vantaggio, da parte di un soggetto appartenente alla sua organizzazione, che ricopra una posizione apicale o subordinata[52]; è altresì necessario che sussista la c.d. "colpa di organizzazione", articolata nelle diverse forme previste dagli artt. 6 e 7 del decreto[53], ove assume un ruolo focale l'adozione e l'efficace attuazione di un idoneo modello organizzativo di gestione e controllo del rischio di reato[54].

---

[48] La ricostruzione degli elementi fondamentali della disciplina 231 che seguirà non ha alcuna pretesa di essere ritenuta completa o esaustiva; l'obbiettivo è quello di fornire dei brevi cenni volti alla comprensione del tema centrale del presente paragrafo, vale a dire l'evoluzione ed il rapporto tra la suddetta disciplina e quella relativa ai reati informatici, applicabile alla prima, *ex* 24 *bis* d.lgs. 231/2001.

[49] Un elemento estremamente dibattuto, sul quale numerosi autori si sono espressi, attiene alla qualifica della responsabilità imputabile agli enti collettivi, potendosi qualificare come una responsabilità di natura penale, amministrativa o un *tertium genus*. Per una esaustiva ricostruzione del tema qui posto si rimanda a LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 161 ss.

[50] Ai sensi dell'art. 1, d.lgs. 231/2001, tale paradigma di responsabilità è indirizzato, ed applicato, a «enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica». A norma del comma 3 del medesimo articolo rimane, invece, esclusa l'applicazione della suddetta disciplina «allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale».

[51] I reati presupposto, indicati dagli artt. 24 ss., rappresentano un *numerus clausus* di fattispecie penali, dal momento che, a norma dell'art. 2 − recante «principio di legalità» − la responsabilità di un soggetto collettivo può derivare esclusivamente dalla commissione di un reato in relazione al quale la responsabilità amministrativa dell'ente e le relative sanzioni siano stati previsti da una norma entrata in vigore prima della commissione del fatto.

[52] Tale passaggio fa riferimento ai criteri di imputazione oggettiva della responsabilità dell'ente, disciplinati dall'art. 5 d.lgs. 231; la disposizione riporta che «l'ente e' responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a). L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi».

[53] Il centro nevralgico della disciplina 231 e del paradigma di responsabilità qui analizzato è rappresentato dalla colpa di organizzazione. Consente, infatti, di permettere la convivenza tra una responsabilità (sostanzialmente) penale con il fondamentale principio sancito dall'art. 27, primo comma, della Costituzione, rappresentante il divieto di responsabilità per fatto altrui e il divieto di responsabilità oggettiva. Permette infatti che il reato presupposto, nonostante sia materialmente commesso da persona fisica diversa dall'ente, quest'ultimo ne risponde in ragione della c.d. "immedesimazione organica". In estrema sintesi, si intende così che il soggetto attivo del reato presupposto, stante la sua appartenenza all'organizzazione e la direzione della sua azione a realizzare un interesse o vantaggio per l'ente, agisca in quanto organo di quest'ultimo, rendendo così il reato imputabile al soggetto collettivo. Si aggiunga poi che, poiché la realizzazione del fatto di reato è resa possibile da un *deficit* di natura organizzativa imputabile, ancora, all'ente, si

Come è facile intuire, l'elemento di questo paradigma di responsabilità per i soggetti collettivi che permette l'integrazione della disciplina *ex* d.lgs. 231/2001 con altri settori specifici del diritto penale consiste proprio nel catalogo dei reati presupposto. In linea generale, si tratta di un elenco assai ampio e variegato, essendo stato oggetto di numerosi interventi normativi di aggiornamento ed espansione. Si può segnalare che, in origine, l'intenzione del legislatore fu quella di costituire un sistema indirizzato a colpire le principali forme di criminalità da profitto nei rapporti con la Pubblica Amministrazione. Erano, infatti, nella prima stesura, previsti solamente due articoli dedicati all'enucleazione delle fattispecie rilevanti ai sensi del decreto, vale a dire gli artt. 24 e 25 – che contenevano l'indicazione dei reati presupposto, menzionando, esclusivamente, i delitti di indebita percezione di erogazioni, truffa ai danni dello Stato o di altro ente pubblico, ovvero per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico, concussione e corruzione[55].

Tra le numerose novelle di ampliamento ed aggiornamento del catalogo dei reati presupposto, al fine di continuare sulla linea tematica del presente capitolo, merita di segnalarsi l'introduzione dell'art. 24 *bis* del decreto 231 − riportante «delitti informatici e trattamento illecito di danni» − inserita nel pacchetto di novità apportate all'ordinamento penale nazionale con la legge di ratifica della Convenzione del Consiglio d'Europa in materia di criminalità informatica − l. 48/2008[56].

Riportando brevemente l'attenzione sulle disposizioni contenute nella Convenzione di Budapest, si può sottolineare come una parte della stessa fosse esplicitamente dedicata alla responsabilità delle persone giuridiche. Infatti, l'art. 12 della Convenzione, rubricato proprio «responsabilità delle persone giuridiche», obbliga gli Stati aderenti ad «adottare le misure legislative o di altra natura che

considera rispettato, quantomeno, il livello minimo del principio della personalità della responsabilità penale, in ragione del quale il reato deve potersi addebitare al suo autore almeno a titolo di colpa. Per approfondimento si rimanda a DI GIOVINE, *il criterio di imputazione soggettiva*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 203 ss.

[54] Sui modelli organizzativi si rimanda a GULLO, *i modelli organizzativi*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 241 ss.

[55] Per una cognizione delle riforme di ampliamento del catalogo dei reati presupposto si rinvia a PIERGALLINI, *I reati presupposto della responsabilità dell'ente e l'apparato sanzionatorio*, in LATTANZI, *Reati e responsabilità degli enti: guida al d.lgs. 8 giugno 2001, n. 231* cit., 211 ss.

[56] Per una più approfondita disamina nell'*iter* di introduzione e delle maggiori novità apportate dalla l. 48/2008 si rimanda a *supra* Cap. I, par. 3.1 e 3.3.

dovessero essere necessarie affinché le persone giuridiche possano essere ritenute responsabili di un reato in base a questa Convenzione»[57].

Il legislatore del 2008, dovendo ratificare la Convenzione sul *cybercrime*, (con riferimento alle disposizioni contenute nell'art. 12), non ha dovuto far altro che aggiornare il suddetto catalogo, inserendovi l'art. 24 *bis*.

Proseguendo nell'analizzare la norma in parola, si deve segnalare preventivamente che essa non include alcuna ipotesi criminosa in materia di *privacy*, nonostante vennero inserite nelle prime formule dell'*iter* legislativo che portò all'emanazione della l. 48/2008[58]. Invero parte della dottrina ha sottolineato come sia stata "un'occasione mancata" per integrare una disciplina − quella della *privacy* − che, come si vedrà[59], si basa fortemente sul modello di responsabilizzazione delle strutture organizzative, attraverso obblighi di *compliance* aziendale[60].

Per quanto riguarda l'impianto normativo dell'art. 24 *bis*, la disposizione individua tre ambiti di presidio: al primo, dedicato, in linea generale, alla tutela della riservatezza informatica, si ricollega, innanzitutto, il delitto di accesso abusivo ad un sistema informatico − *ex* art. 615 *ter* c.p. − fattispecie, questa, che nella generale disciplina sui *cyber crimes* trova ampia applicazione; si consideri che, di regola, un attacco informatico, a prescindere dall'obbiettivo e dalla modalità attraverso cui si realizza, presuppone sempre un accesso non autorizzato. Nel medesimo gruppo rientrano il delitto di «detenzione e diffusione abusiva dei codici di accesso a sistemi informatici o telematici» − *ex* art. 615 *quater* c.p. − che

[57] Art. 12 co. 1, Convenzione del Consiglio d'Europa sulla criminalità informatica. Il prosieguo dell'articolo in commento prevede obblighi di disporre le misure necessarie affinché la persona giuridica possa ritenersi responsabile anche nel caso in cui il mancato controllo o sorveglianza di una persona fisica, membro dell'organizzazione, abbia reso possibile la commissione dei reati, di cui al primo comma, per conto della persona giuridica stessa. In conclusione lascia libertà agli Stati aderenti per determinare la natura di suddetta responsabilità, la quale «può essere penale, civile o amministrativa».

[58] Per questa ragione sono state mosse aspre e severe critiche al legislatore, avendo provveduto ad eliminare il richiamo alla disciplina della *privacy* cfr. SARZANA DI S. IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. e proc.*, 2008, 1572.

[59] V. *infra* par. 3.

[60] Peraltro il legislatore non ha ritenuto di voler rimediare a questa lacuna nella disciplina del d.lgs. 231 neppure con la successiva emanazione del decreto legislativo 101/2018. Sul punto si rimanda a GULLO, *I reati informatici*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 384. Secondo l'autore la ragione di una tale scelta da parte del legislatore risiede nel fatto che l'integrazione nei reati presupposto della disciplina in materia di *privacy* avrebbe comportato immediati e gravosi obblighi sotto il profilo operativo.

sanziona una condotta strettamente prodromica alla realizzazione di un accesso abusivo. Da ultimo, vi si inseriscono i delitti di cui agli artt. 617 *quater* e *quinquies* c.p., rispettivamente «intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche» e «installazione di apparecchiature atte ad intercettare impedire o interrompere comunicazioni informatiche o telematiche», che genericamente ricondotti ai delitti a tutela del segreto, assicurano la punizione dell'intercettazione abusiva di comunicazioni informatiche, nonché di comportamenti ad essa preliminari[61].

Al secondo ambito si ricollegano i delitti posti a tutela dell'integrità dei dati informatici; si fa evidente riferimento, così come la norma stessa, ai delitti *ex* artt. 635 *bis*, *ter*, *quater*, e *quinquies* c.p., appartenenti all'ormai noto "microsistema" dei delitti di danneggiamento informatico, tema centrale del presente elaborato e oggetto di approfondita analisi nei capitoli precedenti[62]. Oltre a questi, si inserisce nel medesimo gruppo anche l'art. 615 *quinquies* c.p. − «diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico» − che tende a sanzionare condotte che, nella prassi, si inseriscono preliminarmente rispetto alla commissione dei delitti di danneggiamento informatico[63].

Al terzo, ed ultimo, ambito di tutela si ricollegano due fattispecie: l'art. 491 *bis* c.p., il quale estende la − precedente − disciplina in tema di falso anche al documento informatico − riporta infatti «falsità in un documento informatico pubblico o avente valore probatorio» − nonché l'art. 640 *quinquies* c.p. − «frode informatica del certificatore di firma elettronica» − il quale, nonostante la rubrica evochi il delitto di frode informatica, rientra nell'alveo dei reati avverso la fede pubblica[64].

L'art. 24 *bis* del d.lgs. 231/2001 non esaurisce i rapporti tra la disciplina della responsabilità degli enti dipendente da reato e quella relativa ai *cyber crimes*.

---

[61] Si rimanda a SICIGNANO, *Problemi attuali in tema di responsabilità «da reato» degli enti per i delitti informatici. l'interesse e il vantaggio. i modelli di comportamento*, in *Rivista 231*, II, 2022, 281.
[62] Si veda *supra* Cap. II e Cap. III.
[63] Inquesto modo si esprime GULLO, *I reati informatici*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 385.
[64] Cfr. GULLO, *I reati informatici*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 386.

Diversa ed autonoma collocazione hanno, infatti, due fattispecie rientranti nella generale categoria dei reati informatici, evidentemente inserite nel decreto 231 in un momento diverso rispetto alla legge di ratifica della Convenzione di Budapest. Il primo riguarda il delitto di frode informatica − *ex* art. 640 *ter* c.p. − in grado di innescare la responsabilità dell'ente ove sia commesso ai danni dello Stato o di un ente pubblico, inserito, già alla prima emanazione del decreto 231/2001, nel catalogo dei reati presupposto, individuati dall'art. 24. Il secondo riguarda, invece, una fattispecie di recente introduzione, prevista dall'art. 1, comma 11 *bis*, d.l. n. 105 del 2019 − convertito nella l. 133/2019 − istitutivo del "perimetro di sicurezza nazionale cibernetica", la quale sanziona la falsa, ovvero l'omessa, comunicazione, entro i termini prescritti, di informazioni, dati, o elementi informativi e dei servizi informatici impiegati, o per lo svolgimento di ulteriori attività indicate dal decreto, allo scopo di ostacolare l'esecuzione di specifici procedimenti ovvero attività ispettive e di vigilanza attribuite alle autorità competenti[65].

L'art. 24 *bis* modula anche la risposta sanzionatoria, classificando le fattispecie sopra individuate secondo criteri di omogeneità e disvalore astratto[66].

[65] Per un'approfondita analisi della fattispecie si rimanda a PICOTTI, VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in *Sist. pen.*, 2019. La presente analisi è tratta da GULLO, *I reati informatici*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 387. Si segnala, in aggiunta, che, ai fini dell'operatività della figura delittuosa in parola, bisognerà attendere la completa emanazione delle norme secondarie di attuazione, che definiscono i contorni e i termini di adempimento degli obblighi giuridici la cui violazione è penalmente sanzionata.

[66] In questo modo, per i reati posti a tutela della riservatezza dei dati e per i delitti di danneggiamento informatico si prevede la sanzione pecuniaria da 100 a 500 quote, nonché le sanzioni interdittive di cui all'art. 9 let. a) − «interdizione dall'esercizio dell'attività» − b) − «sospensione, revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito» − ed e) − «divieto di pubblicizzare beni o servizi». Per i delitti di cui agli artt. 615 *quater* e *quinquies* c.p., che assicurano una protezione anticipata ad interessi tutelati, come si è visto, anche da atre fattispecie sopra richiamate, si applica la sanzione pecuniaria sino a 300 quote, individuando il minimo in quello indicato dall'art. 10 del decreto, mentre le sanzioni interdittive saranno quelle richiamate dall'art. 9 lett. b) ed e). Ai delitti a tutela della fede pubblica − artt. 491 *bis* e 640 *quinquies* c.p. − nonché alla fattispecie di cui all'art. 1, co. 11 *bis* d.l. 108/2019, si applica la sanzione pecuniaria fino a 400 quote, e le sanzioni interdittive *ex* art. 9, lett. c) − «divieto di contrarre con la pubblica amministrazione» − d) − «esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi» − ed e). Cfr. GULLO, *I reati informatici*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 387.

2.1. Misure di prevenzione e *compliance* aziendale

L'elemento che più di tutti costituisce l'architrave del sistema di responsabilità degli enti *ex* d.lgs. 231/2001 è rappresentato dai modelli di organizzazione, gestione e controllo[67]. La centralità è testimoniata dal fatto che i modelli, non solo rivestono una funzione primaria per la configurazione dell'illecito − infatti, *ex* artt. 6 e 7 d.lgs. 231/2001, per non incorrere in responsabilità l'ente deve avere adottato ed efficacemente attuato un modello organizzativo idoneo a prevenire la commissione dei reati previsti dalla normativa − ma anche nelle c.d. "dinamiche riparatorie", essendo il perno delle meccaniche premiali individuabili in diverse disposizioni del decreto[68].

Il testo del provvedimento prevede l'adozione del modello, finalizzata alla circoscrizione della c.d. "colpa di organizzazione", in due disposizioni separate, suddividendole sulla base della qualifica del soggetto attivo del reato presupposto, basandosi cioè sulla diversa ipotesi che esso sia apicale − art. 6 − o subordinato, ovvero sottoposto all'altrui direzione − art. 7. Si prevede che, se ad agire è un soggetto apicale, l'ente non risponde se prova che: a) sia stato adottato, prima della commissione del reato presupposto, un modello di organizzazione e di gestione, idoneo a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo[69]; c) le

---

[67] Per una panoramica generale dei Modelli organizzativi si rimanda a GULLO, *i modelli organizzativi*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 241 ss. Per una più circoscritta valutazione dei modelli e delle tecniche di prevenzione e *compliance* aziendale, relativamente ai reati informatici ci si affida a SICIGNANO, *Problemi attuali in tema di responsabilità «da reato» degli enti per i delitti informatici. l'interesse e il vantaggio. i modelli di comportamento*, in *Rivista 231*, II, 2022. 297 ss.

[68] Su tutti si segnalano due articoli che attribuiscono tale funzione al modello organizzativo: l'art. 12, recante «casi di riduzione della sanzione pecuniaria», che al comma 2 prevede la riduzione, da un terzo alla metà, della sanzione pecuniaria se ricorrano congiuntamente due condizioni: l'integrale risarcimento del danno con l'eliminazione delle conseguenze dannose, insieme all'adozione di un modello organizzativo idoneo alla prevenzione di reati della specie di quello verificatosi. Il secondo è l'art. 17, recante «riparazione delle conseguenze del reato», che impedisce l'applicazione delle sanzioni interdittive nell'ipotesi in cui concorrano tre requisiti: il risarcimento del danno e l'eliminazione delle conseguenze dannose; l'aver messo a disposizione il profitto per la confisca; l'adozione e l'attuazione di idoneo modello organizzativo per la prevenzione di reati della medesima specie di quello commesso.

[69] Su una generale panoramica relativa agli Organismi di vigilanza (anche solo OdV) si veda GULLO, *i modelli organizzativi*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 275 ss. Si segnala che, *ex* art 6 d.lgs. 231/2001, commi 4 e 4 *bis*, negli enti di piccole dimensioni i compiti di vigilanza possono essere svolti direttamente dall'organo dirigente, mentre nelle società

persone hanno commesso il reato eludendo fraudolentemente i modelli; d) non vi è stata omessa o insufficiente vigilanza da parte dell'OdV. Se invece a commettere il reato presupposto è un soggetto subordinato, vale a dire sottoposto al controllo altrui, emerge la responsabilità dell'ente se la commissione del reato sia stata resa possibile dalla inosservanza degli obblighi di direzione e vigilanza. In ogni caso è esclusa l'inosservanza dei suddetti obblighi se l'ente, prima della commissione del fatto, ha adottato ed efficacemente attuato, un modello di organizzazione, gestione e controllo, idoneo a prevenire i reati della stessa specie di quello commesso.

Le caratteristiche essenziali che i modelli devono possedere, vale a dire il contenuto minimo, sono anch'essi individuati dagli artt. 6 e 7 d.lgs. 231/2001[70]. Si prevede che essi debbano contenere, innanzitutto un'adeguata mappatura delle attività in cui si radica maggiormente il rischio del reato ed una disamina delle principali modalità attraverso le quali vengono commessi gli illeciti previsti nel catalogo dei reati presupposto. Al fine di tale mappatura sarà necessario prendere in considerazione, oltre alle dimensioni, alla tipologia dell'attività svolta e all'articolazione dell'assetto normativo, anche la storia giudiziaria pregressa dell'ente, nonché le dinamiche criminose tipiche del settore commerciale di riferimento, riferibili a strutture imprenditoriali analoghe[71]. È, inoltre, necessario prevedere protocolli che definiscano i processi decisionali ed operativi dell'ente, predisporre flussi informativi nei confronti dell'OdV, nonché organizzare meccanismi di controllo interni con un sistema disciplinare, con conseguenti procedure che facciano emergere eventuali comportamenti illeciti[72].

Sembrerebbe opportuno dividere il modello in due parti: nella prima, definibile "parte generale", saranno indicati i sistemi di *governance* e i sistemi

---

di capitali le funzioni dell'ODV possono essere svolte dal Collegio sindacale, Consiglio di sorveglianza e dal Comitato per il controllo della gestione.

[70] In dottrina si è segnalato come il legislatore abbia fornito esigue indicazioni circa il contenuto e le caratteristiche dei modelli organizzativi. Cfr GULLO, *La responsabilità dell'ente e il sistema dei delitti di riciclaggio*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Diritto penale dell'economia*, Milano, 2019, 3509. L'Autore ipotizza di «procedere, per settori di disciplina, a una positivizzazione di questo tipo di cautele che dovrebbero assurgere a fonte legislativa o regolamentare in modo che la relativa tipologia di colpa si caratterizzi quale colpa specifica nella forma della colpa per inosservanza di leggi».

[71] In questo modo si esprime in dottrina SCOLETTA, *Art. 6 - profili penalistici*, in CASTRONUOVO, DE SIMONE, GINEVRA, LIONZO, NEGRI, VARRASO (a cura di) *Compliance. Responsabilità da reato degli enti collettivi*, Milano, 2019, 141.

[72] Così SICIGNANO, *Problemi attuali in tema di responsabilità «da reato» degli enti per i delitti informatici* cit., 300.

organizzativi e di controllo dell'ente, oltre alla distribuzione dei garanti e dei poteri, nonché le procedure di gestione delle aree amministrative e contabili. A tutto ciò si aggiunge anche il codice etico, il sistema disciplinare e le rispettive, ed eventuali, sanzioni, le modalità di rilevamento delle violazioni e l'istituzione, composizione e funzionamento dell'OdV; la "parte speciale", invece, conterrà la descrizione della struttura dei reati, la mappatura delle attività a rischio reato, le funzioni coinvolte nelle aree di rischio, i principi generali di comportamento e il rinvio ai controlli di gestione[73].

Una lettura, fornita da altra dottrina, riassume i contenuti indicati dagli artt. 6 e 7 d.lgs. 231/2001 in quattro *step*: mappatura del rischio, procedimentalizzazione, flussi finanziari e flussi informativi. Nell'*iter* di costruzione del modello, l'ente dovrebbe eseguire un'operazione di *risk assesment*, attraverso tre diverse e progressive fasi: l'identificazione del rischio, valutata in relazione alla struttura, dimensione e contesto operativo dell'ente; l'analisi normativa, vale a dire la ricognizione del quadro di disciplina dei reati presupposto, e un esame delle possibili modalità di esecuzione; la definizione del livello di rischio tollerabile, partendo dall'assunto che «non esiste rischio zero»[74].

Anche questa dottrina condivide la divisione del modello in parte generale e parte speciale. La prima risponde all'esigenza di riflettere all'esterno la fisionomia dell'organizzazione − efficacemente paragonata ad una «carta d'identità dell'ente» − contenendo la struttura, la forma ed il sistema di deleghe del soggetto collettivo, nonché il c.d. sistema normativo − vale a dire la rappresentazione formale della *governance* − il sistema di controllo interno − l'OdV − ed il codice etico. La parte speciale contiene la mappatura del rischio e le previsioni dei protocolli.[75].

---

[73] In questo modo cfr. PIERGALLINI, *I modelli organizzativi*, in LATTANZI (a cura di), *Reati e responsabilità degli enti* cit., 158 s.

[74] Ricostruzione ed analisi offerta da GULLO, *i modelli organizzativi*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 254 s.

[75] In questo modo GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 264 ss. In particolare, per la parte speciale, si tratta di incrociare le ipotesi di reato presupposto con l'operatività del soggetto collettivo; tale operazione può effettuarsi "per fattispecie" − nelle singole sezioni, muovendo dalle fattispecie di reato, si delineeranno le loro astratte modalità di integrazione, si identificheranno, successivamente, le aree di rischio e, solo in conclusione, in base alla concreta operatività dell'ente, valutando le specifiche possibilità di realizzazione dei rati, si stabiliranno gli *standard* di controllo − o "per processi" − si parte dal

Quello che emerge in maniera chiara è l'obbiettivo, perseguito attraverso il modello organizzativo, di predeterminare e tipizzare tutti i procedimenti decisionali, comunicativi e produttivi. La formazione e l'attuazione di ogni decisione deve seguire il metodo protocollare individuato dal − e nel − modello. Le procedure devono essere caratterizzate dalla c.d. "segregazione delle funzioni", cioè la divisione delle fasi di assunzione di una decisione, la sua esecuzione e il successivo controllo in capo a tre soggetti diversi. Dal modello, poi, dovrebbe scaturire una visione necessariamente realistica ed economica dei fenomeni aziendali dell'ente, e non esclusivamente a carattere giuridico[76].

L'attuazione delle strategie e degli indirizzi del modello organizzativo, e quindi delle strategie di prevenzione e gestione del rischio, con la conseguente esclusione della responsabilità da reato dell'ente − ovvero anche l'applicazione delle conseguenze premiali in ambito sanzionatorio − derivano da una corretta costruzione del modello stesso. Una fase fondamentale, come si è appena visto, consiste nel valutare la concreta pericolosità di configurazione delle astratte fattispecie di reato presupposto, e la conseguente identificazione dei sistemi di prevenzione e gestione del rischio, in relazione, anche, alla struttura ed alla attività dell'ente. Ciò significa che, circoscrivendo l'analisi a determinate categorie di reati, comunque previste dal decreto 231, è possibile − se non anche necessario per l'ente − individuare specifiche tecniche di *compliance* aziendale.

In questa sede si guarda alle fattispecie di reati informatici, individuati, come analizzato in precedenza, dall'art. 24 *bis* del d.lgs. 231/2001. La prevenzione di tali reati rientra pienamente nella copertura del sistema di gestione della sicurezza. Va da sé che il modello organizzativo non può non occuparsi della sicurezza informatica.

In prima battuta, è necessario comprendere che un effettivo sistema di gestione della sicurezza, indirizzato anche alla prevenzione, deterrenza, contenimento e risposta dei delitti informatici, rientranti nell'alveo dei reati presupposto − *ex* art. 24 *bis* − si basa sicuramente, ma non esclusivamente, sulla

processo in esame e si enucleeranno i reati presupposto pertinenti, per poi eseguire l'operazione, sopra indicata, per stabilire gli *standard* di controllo.

[76] Cfr. SICIGNANO, *Problemi attuali in tema di responsabilità «da reato» degli enti per i delitti informatici* cit., 300.

tecnologia; risulta, altresì, di fondamentale importanza che si includa e ci si concentri anche sull'analisi del fattore umano e l'efficacia delle procedure che lo sorreggono[77]. Una corretta costruzione di tale sistema passa attraverso un processo di analisi del rischio dinamica, determinando l'individuazione di idonee misure di natura organizzativa, procedimentale e regolatoria; si tratterà, quindi, di adottare presidi di natura tecnologica, congiuntamente con interventi che incidano direttamente sulla formazione, informazione e sulla consapevolezza dei soggetti che compongono la comunità aziendale dell'ente.

Una specifica dottrina ha cercato di elaborare un metodo per un'efficace costruzione ed esecuzione di un sistema di prevenzione e gestione del rischio *cyber*; in tal modo si eviterebbe che il sistema stesso risulti un mero «simulacro formale, definito al solo scopo di creare un'apparente sovrastruttura formale, senza alcuna capacità di incidere nei processi dell'organizzazione stessa»[78].

In primo luogo la *governance*, proiettata alla gestione del rischio *cyber*, dovrebbe ottenere effettività e supporto da parte della direzione dell'organizzazione. Non solo si richiede una formale approvazione dal vertice aziendale, ma anche un aperto e continuo sostegno, nonché la piena e diretta adesione. Tale sostegno e tale adesione dovrebbero, poi, essere manifestate con atti formali[79].

Sarebbe poi necessaria una corretta e precisa definizione dei ruoli e delle responsabilità all'interno dell'organizzazione aziendale. Tale organizzazione, commisurata alle dimensioni dell'ente, dovrà, successivamente, essere comunicata all'esterno; la necessità di comunicare la chiara esistenza di ruoli di controllo e di protezione è parte integrante del sistema di prevenzione e dissuasione, e contribuisce a manifestare l'intenzione dell'ente di costruire un'efficace linea di difesa provvista di poteri e compiti. A ciò si accompagna necessariamente l'effettiva capacità ed idoneità dei soggetti destinati a ricoprire l'impiego, che

[77] Concetto espresso in maniera chiara da DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti*, Milano, 2022, 149 s.
[78] Cfr. da DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti* cit., 159.
[79] In DI MAIO, *ibidem*.

abbiano, perciò, attitudine, conoscenze e competenze finalizzate al processo di tutela[80].

Ulteriore elemento, che si pone come principale fondamento operativo nei processi di *information security*, consiste nella "gestione del rischio" − ovvero *risk managment*[81]. Si tratta di operazioni che hanno come presupposto il c.d. *risk assesment*, già in precedenza segnalato come elemento essenziale dei modelli − *ex* artt. 6 e 7 d.lgs. 231/2001 − che, in un'ottica estremamente pratica, consiste nella identificazione dei beni da proteggere, del loro valore e della loro priorità all'interno dell'organizzazione aziendale, associandovi le possibili minacce derivanti dal contesto ed eventuali ulteriori vulnerabilità. Le operazioni di "gestione del rischio", relativamente ai reati informatici, partono sicuramente, ma non si esauriscono, in processi tecnologici; in questa ottica la gestione ha come riferimento le tre fondamentali nozioni − nonché anche obbiettivi − propri della generale disciplina della *information security*, vale a dire riservatezza, integrità e disponibilità dei dati[82], avendo come obbiettivo quello di prevenire le potenziali compromissioni che possano cagionare un pregiudizio ai suddetti elementi.

Invero, si può sottolineare che la gestione del rischio non ha natura esclusivamente tecnologica; l'aspetto strettamente tecnico può, addirittura, passare in secondo piano se si considera che, nella prassi, la maggioranza degli incidenti di sicurezza informatica deriva causalmente dall'inefficienza del fattore umano. Il catalogo dei rischi, quindi, dovrà tenere conto anche dei pericoli di *compliance* scaturenti dalla deliberata azione dell'uomo. Di conseguenza, le operazioni di *risk managment* dovranno essere rivolte anche alla gestione del personale, elaborando misure che si dimostrino strutturalmente idonee a prevenire la commissione di reati presupposto le quali, nel settore della sicurezza informatica, assumeranno forme «del tutto particolari»[83].

---

[80] Cfr. DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti* cit., 160 s.

[81] Elaborazioni concettuali estremamente diffuse; su tutti si rimanda a QUARANTA, *Compliance risk: come gestire il rischio in modo efficace*, in *Teknoring*, 2020.

[82] Anche noti come parametri RID, richiamati anche dalla direttiva UE 1148/2016, meglio conosciuta come direttiva NIS. In questo elaborato già, brevemente, analizzata. Si veda *supra* Cap. I, par. 1. In dottrina si rimanda a SCHIAVONE, *I diversi aspetti della sicurezza dei dati personali*, in *Cyberlaws*, 2022, *https://www.cyberlaws.it/2022/sicurezza-dati-personali/*.

[83] Cfr. DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti* cit., 163 s. e 165 s. Secondo

Si vogliono segnalare, brevemente, alcune misure pratiche che, secondo la dottrina, i modelli di organizzazione dell'ente dovrebbero prevedere, in funzione della prevenzione dei reati informatici. I principali settori su cui si dovrebbe incidere sono quelli relativi alla *email* istituzionale, all'accesso alla rete aziendale ed alla sicurezza[84]; in primo luogo, attraverso uno specifico ed efficace sistema di controlli interni, nonché con la previsione di un codice etico − che esprima principi vincolanti – ed in secondo luogo, di un codice disciplinare − che preveda sanzioni a carico di coloro che violano le prescrizioni interne.

Si ritiene che l'ente debba vietare l'utilizzo della posta elettronica aziendale per motivi personali e consentire l'accesso alla navigazione sulla propria rete solo previa accettazione del *firewall* dell'organizzazione. Circa la navigazione in rete dovrebbe, poi, essere inibito l'accesso ai siti non connessi all'attività lavorativa e, per evitare violazioni del diritto d'autore, sarà necessario vietare, anche, l'installazione di *software* non autorizzati[85].

Inoltre, considerando che uno degli aspetti critici della disciplina dei *cyber crimes* consiste nella difficoltà di identificare gli autori delle varie condotte, al fine di agevolare l'accertamento delle responsabilità individuali, si suggerisce la predisposizione, entro i limiti della normativa in materia di *privacy*, di una rete informatica che preveda la registrazione delle attività svolte da ciascun utente.

Infine, potrebbe essere funzionale alla prevenzione la pianificazione delle iniziative da adottare in caso di attacco informatico, ad esempio, vietando di pagare eventuali richieste di riscatto, in caso di *ransomware*[86] − rischiando altrimenti di integrare uno dei reati societari previsti dall'art. 25 *ter* d.lgs.

---

l'Autore, tra i fattori di successo di questi programmi merita di essere segnalato il coinvolgimento di tutti i lavoratori nella salvaguardia delle capacità produttive dell'ente, e quindi, il perseguimento anche di interessi individuali.

[84] In questo senso cfr. GALDIERI, *Il diritto penale dell'informatica: legge, giudice, e società*, Torino, 2021, 222. L'Autore identifica i seguenti divieti, i quali dovrebbero essere previsti dal modello: non connettere *computer* esterni ai sistemi informatici interni; non modificare la configurazione *software* di postazioni informatiche aziendali senza autorizzazione; non divulgare le *password* di accesso; non accedere a un sistema informatico in disponibilità di terze parti.

[85] Tale contributo è offerto da SICIGNANO, *Problemi attuali in tema di responsabilità «da reato» degli enti per i delitti informatici* cit., 304.

[86] A proposito di questa specifica categoria di *cyber attack* si veda *supra* Cap. I par. 2.

231/2001 − istituzionalizzando, invece, una procedura di denuncia obbligatoria alla polizia giudiziale[87].

Quanto appena detto rappresenta solo una parte delle indicazioni che pervengono dalla dottrina di settore circa la strutturazione di un efficace sistema di prevenzione e controllo del rischio informatico, operata attraverso la costruzione di un modello di organizzazione dell'ente, funzionale all'esonero della responsabilità dipendente da reato dello stesso. La complessità della materia della sicurezza informatica non può che riflettersi sui sistemi di controllo, determinando l'elaborazione di numerose ed articolate misure di prevenzione; la ricognizione che in queste pagine è stata effettuata si è posta l'obbiettivo di fornire una ricostruzione di massima delle principali linee guida inerenti alla concreta attuazione della disciplina *ex* d.lgs. 231/2001, relativamente alla *cybersecurity*.

3. Tutela della *Privacy*: Regolamento (UE) 679/2016 (GDPR)

Il concetto di "*privacy*", come è noto, è stato elaborato ed isolato dalla dottrina nord americana sul finire del XIX secolo[88], definendolo, in prima battuta, come il "diritto ad essere lasciati soli". La concezione moderna del diritto alla *privacy* è frutto di una lunga evoluzione concettuale, avvenuta nel corso del tempo attraverso molteplici vicende giuridiche; viene oggi definito, in via generica, come il diritto alla riservatezza delle informazioni personali e della vita privata − anche solo diritto alla riservatezza. Volendo estendere la portata della nozione, può intendersi il diritto alla riservatezza come la facoltà, in capo ad una persona fisica, di impedire che le informazioni che la riguardano possano essere trattate da altri, salvo che il soggetto non abbia prestato il proprio consenso, ovvero anche la potestà di esercitare un controllo sull'uso dei propri dati personali.

È facile intuire come l'avvento delle nuove tecnologie informatiche abbia aperto un nuovo scenario certamente ricco di spunti problematici, uno su tutti la necessità di una specifica tutela normativa che avesse ad oggetto il complicato rapporto tra diritto alla riservatezza e l'uso delle tecnologie. In altre parole la

[87] Cfr. SICIGNANO, *Problemi attuali in tema di responsabilità «da reato» degli enti per i delitti informatici* cit., 306.
[88] I due noti autori Warren e Brandeis elaborarono per primi il concetto del «*right to be left alone*». Cfr. IASELLI, *La normativa di riferimento*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, II ed., Milano, 2022, 1.

crescita esponenziale di nuovi servizi e tecnologie, determinata dal progressivo sviluppo delle comunicazioni elettroniche, ha sollecitato i legislatori nazionali e sovranazionali ad elaborare ed adottare adeguate discipline normative che potessero regolamentare efficacemente la delicata questione del diritto alla *privacy*. In questa sede si aaprofondirà la più recente disciplina, formatasi in sede europea e, successivamente, introdotta nell'ordinamento nazionale[89].

Prima di procedere, sembrerebbe opportuno fornire alcuni brevi cenni all'elaborazione della nozione centrale: di base, il diritto alla riservatezza consiste nell'interesse alla non divulgazione di dati, informazioni o notizie che riguardano un individuo o, per dirla conformemente alla prima elaborazione americana, la conoscenza esclusiva delle proprie vicende. Un'attenta dottrina, tuttavia, ha riconosciuto come il concetto di "non divulgazione" debba essere intesa in modo conforme alla dimensione sociale che lo scambio di informazioni personali ha assunto; non sembrerebbe più idoneo il mero «*right to be alone*»[90], che esprime una forma di libertà negativa, ma si dovrebbe valutare la *privacy* nella sua proiezione sociale, quale interesse diffuso che mira a salvaguardare il diritto degli individui a mantenere il controllo delle informazioni private che li riguardano[91].

Ecco che il significato minimale del diritto alla riservatezza non includerà più solamente lo *ius excludendi alios* dalla conoscenza delle informazioni private, ma altresì il diritto positivo al controllo dei propri dati personali. Nella prospettiva dell'informatizzazione e del *web*, poi, non può che essere questa la concezione del diritto alla *privacy*, essendosi abbandonato ormai da tempo il *target* della segretezza dei dati, in favore del controllo sulla corretta utilizzazione. Si consideri, poi, che la recente esigenza di tutelare la segretezza dei dati degli utenti è sorta proprio in ragione della massiva divulgazione delle informazioni personali a soggetti che, in linea di massima, trattano professionalmente suddetti dati; in tale contesto risulterebbe anacronistico limitare il diritto alla riservatezza alla mera conoscenza esclusiva delle proprie vicende.

---

[89] In questo senso si veda IASELLI, *La normativa di riferimento*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 3 ss.

[90] Invero l'evoluzione concettuale della *privacy* ha investito anche il concetto nella dottrina nord americana, venendo oggi conosciuto come «*the individual's ability to control the circulation of information relating to him*».

[91] Cfr. RODOTÀ, *Intervista su privacy e libertà*, Bari, 2005, 18 ss.

Senza voler approfondire ulteriormente le questioni ermeneutiche riguardanti il concetto di *privacy*, si vuole ora adottare una prospettiva strettamente normativa. Si segnala che nel nostro ordinamento giuridico non esiste una norma che preveda espressamente e definisca il diritto alla riservatezza. Le varie discussioni che hanno alimentato il dibattito dottrinale hanno fatto emergere diverse teorie proiettate ad attribuire rilievo costituzionale *de iure condito* alla riservatezza, individuando la fonte in principi riconosciuti dalla Costituzione, ovvero in previsioni di diritto sovranazionale[92].

In particolare, si sono riscontrati dei possibili riferimenti, in senso lato, al diritto in questione all'interno di diverse disposizioni contenute negli articoli della Carta Costituzionale: nell'art. 2, il riconoscimento e la garanzia dei diritti inviolabili dell'uomo, se interpretate come clausola aperta, possono rappresentare una cornice entro cui ricondurre le manifestazioni della vita privata degli individui di rilievo costituzionale; l'art. 13, affermando l'inviolabilità della libertà personale di ogni individuo, inibisce ogni interferenza indebita nella sua sfera psichica e fisica; allo stesso modo l'art. 14 che afferma l'inviolabilità del domicilio protegge la sede principale in cui la vita privata dei cittadini si svolge; medesimo discorso può effettuarsi circa l'art. 15 che afferma la libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione privata; infine l'art. 21 che afferma la libertà di manifestazione del pensiero, interpretato *a contrario*, parrebbe potersi porre a tutela della pretesa di non rendere di pubblico dominio la conoscenza delle informazioni private[93].

Dal punto di vista strettamente disciplinare, il nostro ordinamento ha conosciuto una prima sistemazione normativa della materia con la l. 675/1996 − riportante «tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali» − che ha recepito la direttiva 95/46/CE. Questo primo intervento è stato abrogato e interamente sostituito dal successivo d.lgs. 196/2003 − «codice in materia di trattamento di dati personali», anche solo codice della *privacy*. Con tale norma il legislatore ha riordinato le disposizioni in materia di trattamento dei dati personali, e ha fissato una serie di principi di ordine generale validi per il

[92] In questo modo IASELLI, *La normativa di riferimento*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 2.
[93] Cfr. IASELLI, *ibidem.*

trattamento dei dati, in tutti i settori, prevedendo anche un'appendice sanzionatoria di carattere sia amministrativo che penale[94].

Il punto di arrivo di questo *iter* legislativo, qui riassunto in poche righe, è pervenuto, dopo anni di rinvii e proposte, dall'Unione Europea. Nel maggio del 2016 venne pubblicato nella Gazzetta UE il regolamento 2016/679 − anche noto come GDPR − relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, abrogando contestualmente la precedente direttiva 95/46/CE. Tale provvedimento rappresenterebbe il raggiungimento di un'armonizzazione delle discipline nazionali in ambito di *privacy* e trattamento dei dati personali, introducendo regole più chiare in materia di informativa e consenso, individuando limiti e principi del trattamento automatizzato dei dati, imponendo obblighi di notificazione in caso di *data breach* e attribuendo particolare rilievo alla autodisciplina ed alla *compliance* aziendale[95].

Volendo approfondire maggiormente il provvedimento in parola, si può partire dai contributi definitori, contenuti nell'art. 4; tra tutti quelli *ivi* previsti, quelli probabilmente più significativi sono due, vale a dire la definizione di «dato personale» e quella di «trattamento». Il primo consiste in «qualsiasi informazione riguardante una persona fisica identificata o identificabile»[96], sottolineando, così, che i dati delle persone giuridiche non possano considerarsi "dati personali" al fine del presente regolamento. Il secondo, invece, viene definito come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali»[97],

[94] Per un'approfondita disamina della disciplina del codice della *privacy* si rimanda in dottrina a BRIGANTI, *Il codice della privacy*, in *Altalex*, 2005, *https://www.altalex.com/documents/news/2007/01/31/il-codice-della-privacy*; nella manualistica si segnala ELLI, ZALLONE, *Il nuovo Codice della privacy : commento al d.lgs. 30 giugno 2003 n. 196, con la giurisprudenza del Garante*, Torino, 2004.

[95] Cfr. IASELLI, *La normativa di riferimento*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 9 ss.

[96] La norma prosegue affermando che «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» *ex* art. 4, co. 1, Reg. UE 2016/679.

[97] Prosegue la disposizione «[...] come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la

evidenziando la volontà di includervi ogni genere di attività che abbia ad oggetto dati personali.

Il regolamento prevede poi sette principi fondamentali: a norma dell'art. 5, co. 1, del reg. UE 2016/679, i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, raccolti per determinate finalità, esplicite e legittime, e successivamente trattati in compatibilità con le medesime; i dati raccolti devono essere limitati ed adeguati alla finalità perseguita, nonché sempre aggiornati ed esatti, dovendosi, per questo, prevedere specifici meccanismi di eventuale aggiornamento e cancellazione; la conservazione deve essere idonea all'identificazione degli interessai e limitata ad un arco temporale non superiore al conseguimento della finalità; infine, il trattamento deve essere eseguito in maniera tale da garantire un'adeguata sicurezza dei dati, compresa l'adozione di adeguati strumenti e misure tecnico-organizzative[98].

Il secondo comma del medesimo articolo esprime un ultimo principio, legato al *considerandum* 74[99], secondo cui il titolare del trattamento[100] è responsabile e competente per il rispetto dei principi di cui al comma 1 − c.d. "principio di responsabilizzazione" del titolare del trattamento. Tale principio, espresso in maniera più ampia nel suddetto *considerandum*, rappresenta uno dei perni della disciplina del GDPR, vale a dire l'*accountability*[101], a cui è dedicato l'intero capo IV del regolamento. L'obbiettivo è quello di responsabilizzare i titolari del trattamento dei dati personali degli utenti per farli vigilare sulla corretta esecuzione ed adempimento delle disposizioni contenute nel provvedimento.

---

comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

[98] In dottrina le disposizioni analizzate sono sintetizzate nei sette principi così espressi: "liceità e correttezza", "trasparenza", "limitazione delle finalità dei trattamenti", "minimizzazione", "esattezza", "limitazione della conservazione" e "integrità e riservatezza".

[99] Si prevede che «il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure».

[100] Attingendo nuovamente all'art. 4, si definisce titolare del trattamento «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». Per approfondimento si rimanda a MARINO, *I soggetti privacy*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 49 ss.

[101] Nozione già sottoposta ad analisi nei capitoli precedenti. V. *supra* Cap. I, par. 1. Si riporta la definizione del nucleo essenziale del concetto, vale a dire «la responsabilizzazione delle strutture organizzative, vincolandole al raggiungimento di determinati obbiettivi».

L'art. 24, che apre il capo IV, dedicato al titolare del trattamento dei dati, prevede, infatti, che, tenendo conto di tutti i numerosi fattori − quali l'ambito, le finalità, i pericoli e la natura del trattamento dei dati − inerenti ai diritti e alle libertà dei soggetti coinvolti, questi devono «mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento». In altre parole si stabilisce la responsabilità generale del titolare per qualsiasi trattamento da quest'ultimo effettuato direttamente o che altri abbiano effettuato per suo conto[102].

Si richiede ai titolari di tener conto della tutela alla *privacy* sin dal momento della progettazione dei sistemi con cui verranno eseguiti i trattamenti dei dati, anticipando i rischi delle loro iniziative − c.d. *privacy by design*[103] −, eseguendo una complessa operazione di *privacy impact assesment*, cioè un approccio di gestione del rischio che si proietta alla valutazione degli effetti che i sistemi possono avere sulla riservatezza dei dati, a causa dei trattamenti[104]. L'art. 25 del GDPR a tal fine propone la c.d. "pseudonomizzazione": vale a dire un meccanismo per il quale i dati non possono essere attribuiti ad un interessato specifico senza informazioni aggiuntive; tali informazioni devono, necessariamente, essere conservate in sicurezza, separatamente, in modo tale da rendere impossibile l'identificazione attraverso i dati oggetto di trattamento[105].

Ulteriore elemento centrale riguarda il "consenso al trattamento": esso viene identificato, dall'art. 6 del regolamento, come una delle condizioni di liceità del trattamento dei dati[106]. Se, quindi, quest'ultimo si basa sul consenso dell'interessato, il titolare dovrà essere in grado di dimostrare che questo vi abbia

---

[102] Sul punto, per maggiore approfondimento cfr. MARINO, *I soggetti privacy*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 58 ss.

[103] Per maggiore approfondimento si veda BARDARI, *Sicurezza dei dati e valutazione dei rischi*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 179 s.

[104] Sul punto, tra tutti, si rimanda a CLARKE, *Privacy impact assessment: Its origins and development*, in *Computer law & security review*, 25, 2009, 123 ss.

[105] Per un'approfondita analisi della nozione in parola cfr. IASELLI, *Pseudonomizzazione*, in *Altalex*, 2018, *https://www.altalex.com/documents/altalexpedia/2018/06/04/pseudonomizzazione*.

[106] *Ex* art. 6, reg. UE 2016/679, il trattamento si considera lecito se ricorre almeno una delle seguenti condizioni: l'interessato ha espresso il consenso; il trattamento è necessario per adempiere ad obblighi contrattuali; il trattamento è necessario per adempiere ad obblighi scaturenti da legge, a cui è soggetto il titolare; il trattamento è necessario per la salvaguardia degli interessi vitali del titolare o di altra persona fisica; il trattamento è necessario per lo svolgimento di un'attività di interesse pubblico; o nell'esercizio di pubblici poteri; il trattamento è necessario al fine di perseguire un interesse legittimo del titolare.

acconsentito. L'interessato ha il diritto, in ogni momento, di revocare il consenso, che comunque non pregiudicherà il trattamento eseguito prima della presentazione della revoca.

Volendo sintetizzare i requisiti del consenso, ai sensi del GDPR, si può affermare che quest'ultimo debba necessariamente essere: informato, perché deve esserci un'adeguata informativa sulle finalità e sui metodi del trattamento; libero; specifico, in quanto il consenso deve essere espresso in relazione a una o più specifiche finalità, potendo scegliere tra ciascuna di esse; inequivocabile, vale a dire espresso mediante un'azione deliberata o comunque in modo attivo; dimostrabile; revocabile; espresso o esplicito − non è consentito il consenso desunto da fatti concludenti[107]. Come è chiaro, la validità del consenso dipende da un considerevole numero di fattori, la cui rigorosa verifica precede necessariamente ogni trattamento − che sia basato, per l'appunto, sul consenso.

In conclusione si può, brevemente, analizzare il capo III del regolamento, dedicato al diritto dell'interessato. Quest'ultimo è suddiviso in cinque sezioni, cioè «trasparenza e modalità», «informazione ed accesso ai dati personali», «rettifica e cancellazione», «diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche»[108].

In estrema sintesi l'interessato ha diritto ad essere informato, ovvero ad avere accesso a: l'esistenza di trattamenti di dati personali che lo riguardano; le finalità del trattamento; l'identità dei soggetti che svolgono il trattamento e quella dei loro collaboratori; l'identità di soggetti terzi a cui i dati potrebbero pervenire; il periodo di conservazione; l'eventuale obbligo di comunicazione dei dati e le conseguenti sanzioni in caso di violazione; eventuale automatizzazione dei processi del trattamento e le logiche per essa utilizzate; l'origine dei dati; gli altri diritti esercitabili dall'interessato in relazione ai dati. A questi si aggiungono il diritto di rettifica dei dati inesatti, senza ingiustificato ritardo; il diritto alla cancellazione − anche noto come diritto all'oblio − secondo cui, su richiesta dell'interessato, il titolare del trattamento è tenuto all'immediata cancellazione dei

[107] Per una più approfondita analisi si veda SCUDIERO, *Il consenso come condizione di liceità*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 109 ss.

[108] Sul punto si segnala MARINO, *I diritti degli interessati*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 73 ss.

dati; il diritto alla limitazione delle operazioni che riguardano il trattamento, sempre su richiesta del soggetto a cui si riferiscono le informazioni; infine, il diritto alla portabilità, cioè il diritto di ricevere, in un formato comune e leggibile, i dati per poterli trasmettere ad un altro titolare di trattamento[109].

Non presente nel capo III, poiché dotato di altra collocazione sistematica, è il diritto alla comunicazione di una violazione dei dati, *ex* art. 34 reg. UE 2016/679 − anche noto come *data breach*. Con suddetto termine si intende una violazione della sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la non autorizzata divulgazione o l'accesso ai dati personali. Nella medesima ipotesi, il titolare dovrà altresì effettuare comunicazione della violazione anche alle autorità di controllo − *ex* art. 33[110].

Questa breve disamina delle principali caratteristiche del regolamento UE 2016/679 è ben lungi dal potersi definire completa ed esaustiva. Si è, però, tentato di analizzare ed indicare i fondamenti ed i lineamenti principali dell'attuale normativa, in quanto può sicuramente considerarsi una delle principali discipline dalla generale materia della *cybersecurity*.

3.1. Data breach e reati informatici

La nozione di *data breach*, sopra brevemente identificata, ha molteplici possibilità di manifestazioni empiriche. La definizione individuata dal regolamento UE 2016/679 − *ex* art. 4, n. 12 − ipotizza due possibili, e generiche, alternative di «violazione di scurezza», accidentalmente ovvero in modo illecito. Si aggiunga, poi, che le conseguenze dirette di tale violazione, sempre identificate dalla disposizione in parola, consistendo nella «distruzione, modifica, perdita, ecc.», determinerebbero una compromissione della riservatezza, integrità o disponibilità dei dati.

Non sfuggirà che, salvo eventi naturali catastrofici, ovvero episodi meramente fortuiti o involontari, tra le cause di un *data breach* si possono

[109] Sia il diritto all'oblio che il diritto alla portabilità dei dati sono considerati i 2 "nuovi diritti", previsti per la prima vola in un testo normativo. Cfr. MARINO, *I diritti degli interessati*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 98 ss.

[110] Per maggiore approfondimento si rimanda a GALLUS, *La notificazione e la comunicazione di una violazione di dati personali*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR* cit., 245 ss.

annoverare sicuramente le fattispecie di reati informatici. In altre parole, le ipotesi di trattamento illecito dei dati, trattandosi di un comportamento doloso, volto alla realizzazione di una violazione dei dati, il più delle volte informatici, o comunque gestiti da sistemi informatici o telematici, appaiono del tutto compatibili con le varie manifestazioni di *cyber crimes*[111].

Posta in questa prospettiva risulta evidente che, in caso di violazione dei dati personali, ove cagionata dalla commissione di una fattispecie penale informatica, si potrebbero verificare gravi conseguenze dannose, materiali o immateriali, per i soggetti interessati, che vanno ben oltre la − comunque rilevante − violazione del diritto alla riservatezza; si pensi, ad esempio, a possibili danni finanziari, furti di identità, discriminazione, o comunque qualsiasi altro danno economico o sociale significativo[112].

È proprio in ragione di queste conseguenze gravemente pregiudizievoli, tra l'altro potenzialmente indirizzate verso un'ampia platea di utenti, che in caso di verificazione di un *data breach* per il titolare del trattamento dei dati sorgono molteplici obblighi e adempimenti, ai sensi del regolamento UE 2016/679.

In particolare, si prevede che, ove possibile, senza ingiustificati ritardi, il titolare dovrà notificare al Garante per la protezione dei dati personali la violazione, salvo che gli risulti improbabile che detta violazione comporti un rischio per i diritti e le libertà delle persone fisiche[113]. La comunicazione deve essere inviata entro un termine massimo di 72 ore dalla scoperta, attraverso l'apposito modello messo a disposizione dal Garante sul sito *web*, tramite posta elettronica sottoscritta digitalmente, ovvero con firma autografa.

Quanto al contenuto, a norma dell'art. 33, co. 3, il titolare deve fornire con la comunicazione le seguenti informazioni: la descrizione della natura della violazione dei dati, contenente, ove possibile, le categorie ed il numero approssimativo di persone e di dati personali; il nome e i contatti del responsabile alla protezione dei dati, se designato, o comunque di un referente in grado di fornire informazioni; una descrizione delle possibili conseguenze della violazione;

[111] In questi termini si esprime MASSARO (a cura di), *Diritto penale e privacy*, Pisa, 2020, 186 s.
[112] Tale possibile situazione consequenziale rispetto ad un *data breach* era stata già prevista dal GDPR, nel *considerandum* n. 85.
[113] Tale obbligo di notifica alle autorità è previsto dall'art. 33 reg. UE 2016/679.

una descrizione delle misure adottate, o di cui ci si intende dotare, per porre rimedio alla violazione o mitigarne gli effetti[114].

Il Garante, dopo aver esaminato la segnalazione da parte del titolare del trattamento, può rivolgere ammonimenti e prescrivere al titolare, o al responsabile se designato, l'adozione di misure correttive, laddove rilevasse la violazione di disposizioni del regolamento, anche per ciò che attiene l'adeguatezza delle misure di sicurezza tecniche ed organizzative applicate ai dati oggetto del trattamento[115]. A seguito della comunicazione di *data breach*, al Garante compete anche la comminazione delle sanzioni pecuniarie previste dal GDPR, all'art. 83.

Ulteriore obbligo, già sopra precedentemente segnalato, riguarda la comunicazione, quando la violazione dei dati può comportare un rischio elevato per i diritti degli individui, imposta al titolare, a tutti gli interessati, con linguaggio chiaro ed utilizzando i canali più idonei; detta comunicazione non è, tuttavia, necessaria se ai dati personali oggetto di violazione erano state applicate misure idonee a garantire un elevato livello di protezione − *ex* art. 34, co. 3. Si dovrà, invece, procedere alla comunicazione pubblica ogni qual volta l'esecuzione agli interessati implicasse sforzi sproporzionati[116].

In conclusione, nel valutare le implicazioni derivanti dalla congiunzione tra la disciplina del GDPR e quella dei *cyber crimes*, non ci si può esimere dal riconoscere una sostanziale sovrapponibilità tra le casistiche di trattamento illecito di dati − *ex* reg. UE 2016/679 − e le fattispecie dei delitti informatici inseriti nel catalogo dei reati presupposto della disciplina sulla responsabilità degli enti dipendente da reato − *ex* d.lgs. 231/2001. Tale sovrapponibilità determina una necessaria convergenza tra le due normative, non solo, evidentemente, dal punto

[114] In riferimento ai contenuti della comunicazione al garante è dedicato anche il *considerandum* 88 del GDPR, secondo cui «nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali».

[115] *Ex* art. 58, co. 2, reg. UE 2016/679.

[116] Per approfondire le questioni relative alle conseguenze di un *data breach* si veda MASSARO (a cura di), *Diritto penale e privacy* cit., 184 ss.

di vista del diritto penale sostanziale − essendo richiamate le medesime fattispecie di reato − ma anche e sopratutto sul piano della prevenzione[117].

Si pensi, ad esempio, ad un'ipotesi di *data breach*, consistente in un delitto di danneggiamento di dati informatici − *ex* art. 635 *bis* c.p. − ravvisabile nella condotta di un dipendente che elimini dagli archivi digitali dati aziendali "compromettenti" in occasione di un accertamento dell'Autorità; se fossero riscontrati i presupposti oggettivi e soggettivi[118], tale situazione determinerebbe sia la responsabilità dell'ente, con la conseguente applicazione di tutte le possibili sanzioni, pecuniarie, interdittive, la confisca o anche la pubblicazione della sentenza − *ex* art. 9 d.lgs. 231/2001 − ma anche l'irrogazione delle sanzioni pecuniarie, economicamente molto gravose, previste dal GDPR, essendo suddetta ipotesi imputabile a violazioni del regolamento. Da qui l'esigenza, in entrambi i casi, di dotarsi di adeguate misure di sicurezza[119].

Tanto la regolamentazione in materia di *privacy* quanto la disciplina della responsabilità degli enti *ex* decreto 231/2001, seppur con le dovute differenziazioni, richiedono un approccio c.d. *risk based*, vale a dire che ogni ente, soggetto alla disciplina 231, ovvero ogni titolare del trattamento di dati personali, devono attivarsi concretamente per ridurre il rischio di condotte criminose in termini di accettabilità[120]. L'adozione di idonee misure di sicurezza, tra l'altro, è specificamente prevista dalla legge, in alcuni casi[121], per il titolare del trattamento di dati, così come avviene per l'ente − mediante l'adozione del modello organizzativo − per evitare il sorgere della responsabilità, ovvero *post factum* per ottenere una riduzione del relativo trattamento sanzionatorio.

---

[117] Cfr. MASSARO (a cura di), *Diritto penale e privacy* cit., 185.
[118] Si veda *supra* par. 2.
[119] Per approfondimento dei punti di contatto tra GDPR e d.lgs. 231/2001 si veda MONTI, *Il modello organizzativo 231 e la protezione dei dati personali*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti* cit., 225 ss.
[120] Così MASSARO, (a cura di), *Diritto penale e privacy* cit., 185.
[121] Si pensi all'art. 24 del reg. UE 2016/679, di cui si è già parlato nel paragrafo precedente, ovvero anche l'art. 32 del medesimo provvedimento, riportante «sicurezza del trattamento», secondo cui «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio».

Entrambe le normative, evidentemente, si basano sul generale principio di *accountability*, stimolando l'auto-responsabilizzazione dei soggetti coinvolti, operando sui sistemi di *compliance* aziendale[122]. In questi termini sembrerebbe possibile cogliere la mancata opportunità di intergare formalmente le due discipline, segnalata da una parte della dottrina[123]. Altra dottrina, però, ritiene che il rapporto tra protezione dei dati e il dovere di prevenzione dei reati presupposto sia fortemente condizionato dalla differenza ontologica nell'impostazione delle norme di riferimento. La disciplina del GDPR sarebbe basata su un'impostazione sostanzialmente auto-accusatoria, in funzione dell'applicazione di sanzioni pecuniarie; la normativa 231 dovrebbe, invece, essere ispirata ai principi di difesa[124].

Un ulteriore aspetto di sensibile differenza tra i due modelli organizzativi atterrebbe alla loro funzione. Il GDPR imporrebbe al titolare del trattamento di ridurre il rischio per i diritti e le libertà di soggetti terzi; il d.lgs. 231/2001, invece, chiederebbe all'ente di prevenire efficacemente i reati commessi da soggetti intranei all'organizzazione, apicali o subordinati. Ciò significherebbe da un lato di impostare una «gestione probabilistica di eventi incerti», dall'altro di garantire una "obbligazione di risultato": questi sono evidentemente due obbiettivi che hanno un perseguimento operativo del tutto differente[125].

Posta in questi termini, è evidente che l'ente-titolare del trattamento si troverebbe a vivere una condizione di *double bind*, vale a dire un doppio legame tra due messaggi, potenzialmente, contraddittori, in cui il rispondere correttamente ad uno potrebbe determinare l'omissione dell'altro − tra i vari aspetti indicativi si consideri, ad esempio, che il responsabile del trattamento dei dati e l'organismo di vigilanza non possono essere la stessa persona. Si richiederebbe, dalla citata dottrina, un intervento del Legislatore che possa risolvere tale aporia.

---

[122] Cfr. MASSARO (a cura di), *Diritto penale e privacy* cit., 193.
[123] Sul punto si veda GULLO, *I reati informatici*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti* cit., 384.
[124] In questo senso veda MONTI, *Il modello organizzativo 231 e la protezione dei dati personali*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti* cit., 248. L'Autore afferma che l'interazione tra i due modelli determinerebbe un paradosso: da una parte (GDPR) l'ente dovrebbe cooperare con l'Autorità di protezione dei dati, dall'atro lato (d.lgs. 231/2001) ha il diritto al silenzio e, dunque, alla non cooperazione con l'inquirente.
[125] In questi termini cfr. veda MONTI, *Il modello organizzativo 231 e la protezione dei dati personali*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti* cit., 248.

In questo intreccio di norme, regolamenti, modelli e procedure ciò che rimane sempre e comunque fuori da ogni forma di controllo è la tecnologia informatica, che segue in ogni caso logiche determinate da chi la crea, la controlla e la vende. Chi la usa, tuttavia, è colui il quale rimane "da solo" di fronte alle scelte di *compliance* e, successivamente ed eventualmente, all'assunzione di responsabilità[126].

[126] Spunti di riflessione offerti da MONTI, *Il modello organizzativo 231 e la protezione dei dati personali*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti* cit., 249.

CONCLUSIONI

Le strategie di contrasto alle molteplici forme di criminalità informatica − generalmente rientranti nella c.d. *Cyber security* − si sviluppano in diverse direzioni, a seconda dello specifico ambito in cui ci si muove. Le legislazioni nazionali e sovranazionali hanno, infatti, progressivamente sviluppato discipline settoriali, integralmente o parzialmente rivolte ad arginare l'aumento del rischio di commissione dei *cyber crimes*, determinato dalla crescente informatizzazione dei rapporti economici e dei processi comunicativi.

Il nucleo duro di tali forme di tutela, come si è avuto modo di sottolineare, è costituito dalla prevenzione del rischio, nella sua accezione più ampia, stimolando − se non vincolando − gli operatori economici ad adottare forme di autoregolamentazione volte alla creazione di un elevato *standard* di sicurezza.

L'esempio più significativo di tale tendenza, come si è evidenziato, è rappresentato dal paradigma della responsabilità degli enti dipendente da reato, *ex* d.lgs. 231/2001. Gli obblighi di *compliance ivi* previsti, che si manifestano nella necessaria adozione – quale condizione per l'esonero dell'ente dalla responsabilità amministrativa – di un modello di organizzazione, gestione e controllo, idoneo alla prevenzione di fattispecie penali inserite nel catalogo dei reati presupposto, rappresentano, in senso lato, una delle più forti applicazioni del generale principio di *accountability.*

L'intento perseguito dal legislatore non è quello di imporre agli enti meri divieti o obblighi di condotta ma di responsabilizzare le strutture organizzative vincolandole al raggiungimento di determinati obiettivi. Le conseguenze dell'eventuale violazione, o mancata adozione, delle fonti di autoregolamentazione, variabili a seconda della disciplina di riferimento, possono incidere direttamente sulla latitudine della responsabilità penale − trattandosi in questo caso di efficacia conformativa diretta delle fonti di autoregolazione − ovvero, come nel caso della normativa 231, escludere l'esenzione della responsabilità (c.d. efficacia conformativa indiretta).

Sarà ormai chiaro come, in questa generale prospettiva di tutela, il diritto penale, segnatamente attraverso la tipizzazione dei *cyber crime*, si inserisce nella più generica materia della *Cyber security*, caratterizzata dalla trasversalità dei temi

e delle competenze, in un rapporto genetico, aderente a una prospettiva causa-effetto dei primi sulla seconda. Il diritto penale ha, quindi, nel corso del tempo, assunto un ruolo centrale nella regolamentazione delle tecnologie informatiche e, sopratutto, di *internet*, portando dapprima il legislatore e successivamente l'interprete, a non affidarsi esclusivamente alle categorie dogmatiche tradizionali ma, attraverso l'elaborazione teorica e sistematica, a creare una nuova autonoma disciplina.

La reciprocità del condizionamento tra il diritto penale e la realtà *cyber*, che in tale contesto si è in grado di cogliere, ha portato la tradizione penalistica a riplasmarsi e adattarsi alla novità ed alla complessità dei rapporti che si svolgono nel *cyber space*. L'esperienza dell'ordinamento nazionale italiano ha pienamente dimostrato come, per contrastare efficacemente le minacce derivanti dalla realtà informatica, non sia sufficiente un perenne inseguimento legislativo o giurisprudenziale volto a colmare le lacune che progressivamente si manifestano nella prassi, attraverso l'ampliamento di esistenti fattispecie penali con circostanze aggravanti speciali, ovvero con l'applicazione estensiva o adattamenti in via ermeneutica delle stesse. La necessità è quella di delineare un quadro giuridico generale, che, adottando una prospettiva internazionale ed europeista, consenta di rendere operativi sistemi armonizzati di incriminazioni.

Si è visto, infatti, come gli impulsi alla creazione di una normativa specifica in materia di reati informatici siano pervenuti da organismi internazionali; in particolar modo, il primo e più efficace provvedimento, vincolante per i paesi aderenti, è stata la Convenzione del Consiglio d'Europa in materia di criminalità informatica del 2001 − anche nota come Convenzione di Budapest − per la cui ratifica il legislatore italiano ha emanato la legge 18 marzo 2008 n. 48, che rappresenta la più vasta riforma del sistema penale in materia di criminalità informatica.

Tra le novità introdotte dalla suddetta novella legislativa si inserisce il "microsistema dei delitti di danneggiamento informatico", tema centrale del presente elaborato, di cui si è dato conto nel secondo e nel terzo capitolo. Nel corso dell'analisi delle fattispecie *ivi* contenute − artt. 635 *bis*, *ter*, *quater* e *quinquies* c.p. −si è potuto notare come l'elaborazione di reati proiettati alla tutela

di beni inseriti in un contesto informatico, sconosciuto all'originale tradizione penalistica, abbia generato numerose complicazioni ermeneutiche che hanno richiesto il necessario intervento chiarificatore da parte della dottrina e, talvolta, della giurisprudenza; tali interventi, tuttavia, non sono sempre riusciti nell'intento di fornire una soluzione definitiva alle numerose questioni che sono state segnalate; in tali casi, pertanto, si è ritenuto opportuno offrire una ricognizione e disamina delle diverse e possibili soluzioni offerte.

La stessa dottrina, chiamata ad esprimersi sul complesso di norme costituenti il sistema dei delitti di danneggiamento informatico, ha sollevato forti e numerose perplessità, auspicandosi, in una prospettiva *de jure condendo*, che il legislatore riformuli ed armonizzi tale sistema di reati[1]. In particolare, richiamando quanto già affermato nel corpo dell'elaborato, da più parti, si sollecita la soppressione del riferimento alla "altruità" di dati, informazioni o programmi, che, in un contesto strettamente informatico, nonché nell'ambito del diritto penale, determina significative complicazioni nell'individuare la persona offesa e l'interesse protetto. La possibile alternativa, proposta dalla medesima dottrina e largamente condivisa, consisterebbe nella previsione di una clausola di illiceità espressa, costituita da locuzioni quale «senza diritto».

Parimenti, forti perplessità ha suscitato la scelta politico-criminale del legislatore di configurare i danneggiamenti di dati e programmi "pubblici" come delitti di attentato, determinando un potenziale contrasto con il principio di proporzionalità, secondo cui, in tale ambito, si richiede che vi sia proporzione tra il grado di anticipazione della tutela penale e l'importanza del bene giuridico. Risulterebbe, quindi, del tutto sproporzionato il ricorso alla tecnica dei reati a consumazione anticipata, riconoscendo nei beni giuridici tutelati dalle norme in parola un rango non particolarmente elevato, o comunque non tale da giustificare l'incriminazione di condotte sostanzialmente preparatorie, le quali, salvo casi eccezionali, non rappresentano una seria minaccia per un bene indispensabile per la sopravvivenza dell'assetto politico-costituzionale.

Pur rivestendo grande importanza, sembrerebbe corretto ritenere che, nella gerarchia dei valori propri di un ordinamento giuridico democratico, tali interessi

[1] SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici, un bilancio poco esaltante*, in *Riv. it. dir. proc. pen.*, 2012, 240.

non ricoprono ruoli di vertice, non potendosi spiegare, in questo modo, l'adozione della tecnica dei delitti a consumazione anticipata. In tal senso, sembrerebbe auspicabile che il legislatore, in linea con le prescrizioni di fonte sovranazionale, configuri le fattispecie di cui agli artt. 635 *ter* e *quinquies* c.p. quali comuni delitti di evento, consentendone comunque la punibilità a titolo di tentativo.

Nel complesso, si richiederebbe una riformulazione del "microsistema dei delitti di danneggiamento informatico", proiettata all'adesione non solo formale, ma anche e sopratutto sostanziale, alle indicazioni ed ai vincoli derivanti dall'ordinamento comunitario − identificabili nella direttiva UE 2013/40 − e dalle fonti sovranazionali − su tutte, la Convenzione di Budapest − mantenendosi però entro i solchi tracciati dai fondamentali principi costituzionali in materia penale, che non possono essere in alcun modo sacrificati per il dover adempiere, in modo frettoloso e meramente formale, alle prescrizioni degli organismi internazionali.

In conclusione, si potrebbe ritenere che, nonostante le evidenti difficoltà del legislatore nell'elaborare categorie dogmatiche idonee alla creazione di un quadro giuridico penale generale in cui collocare la materia dei reati informatici, rimanga apprezzabile il continuo sforzo in tal senso, manifestando la consapevolezza del rapporto di reciproco condizionamento tra il diritto e l'ambito *cyber*.

Le peculiarità della realtà informatica obbligano le legislazioni ad un continuo adeguamento all'incessante sviluppo tecnologico e cibernetico, sollecitato anche dalle indicazioni che derivano dalle fonti sovranazionali. È possibile pensare che, per quanto risulti difficile immaginare una soluzione definitiva per arginare i rischi derivanti dal progresso digitale, una forma di tutela più efficace derivi dalla creazione di una vera e propria armonizzazione delle legislazioni nazionali che tenga maggiormente in considerazione l'importante contributo dell'esperienza giuridica straniera, e che tragga fonte dalle organizzazioni internazionali in grado di farsi carico di tale obiettivo.

BIBLIOGRAFIA

AA. VV., *Attacco DDoS (Distributed Denial of Service): Cos'è, come fare, come difendersi*, in *Cybersecurity360, https://www.cybersecurity360.it/nuove-minacce/ddos-cosa-sono-questi-attacchi-hacker-e-come-stanno-evolvendo/.*

AA. VV., *Attacco Man-in-the-middle, tutti i modi possibili e come difenderci*, in *Cybersecurity360, https://www.cybersecurity360.it/nuove-minacce/attacco-man-in-the-middle-tutti-i-modi-possibili-e-come-difenderci.*

ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983.

ANTOLISEI, *Diritto penale, Parte speciale I*, ed. XII, Milano, 1999.

ANTOLISEI, *Diritto penale, Parte speciale I*, ed. XVII, Milano, 2022.

ANTOLISEI, *Diritto penale, Parte speciale II*, ed. XVII, Milano, 2022.

ARENA, *La Convenzione come modello di armonizzazione*, in *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*, 2021, 11 ss.

ATERNO, *Le fattispecie di danneggiamento informatico*, in LUPARIA (a cura di) *Sistema penale e criminalità informatica*, Milano, 2009.

BACCAREDDA BOY, LALOMIA, *I delitti contro il patrimonio mediante violenza*, in MARINUCCI, DOLCINI (a cura di), *Trattato di diritto penale, Parte speciale*, VIII, Padova, 2010.

BALDONI, MONTANARI (a cura di), *2015 Italian Cyber Security Report. Un Framework Nazionale per la Cyber Security*, 2016.

BARDARI, *Sicurezza dei dati e valutazione dei rischi*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, II ed., Milano, 2022.

BAUD, *la guerre asymétrique ou la défaite du vainqueur*, 2003.

BERNARDI, *La competenza penale accessoria dell'Unione Europea: problemi e prospettive*, in *Diritto Penale Contemporaneo*, 2012.

BIGOTTI, *La sicurezza informatica come bene comune. Implicazioni penalistiche e di politica criminale*, in FLOR, FALCINELLI, MARCOLINI (a cura di), *La*

giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet, in *Lab. Per. Dir. Pen.*, 2014.

BRIGANTI, *Il codice della privacy*, in *Altalex*, 2005, *https://www.altalex.com/documents/news/2007/01/31/il-codice-della-privacy*.

CADOPPI, CANESTRARI, MANNA, PAPA, *Diritto Penale*, tomo III, Milano, 2022.

CALICE, *Le principali modifiche introdotte con la Legge 18.3.2008 n. 48 di ratifica ed esecuzione della Convenzione europea sulla criminalità informatica*, in *http://www.distretto.torino.giustizia.it/documentazione/D_1967.pdf*, 2008, 9 ss.

CAMPLANI, Locus commissi delicti, *norme di collegamento e reati informatici a soggetto passivo indeterminato*, relazione al IX Corso di formazione interdottorale di diritto e procedura penale "Giuliano Vassalli", Siracusa, 2018, *https://archiviopenale.it/locus-commissi-delicti-norme-di-collegamento-e-reati-informatici-a-soggetto-passivo-indeterminato/articoli/25947*.

CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, Milano, 2019.

CASO, *sentenza 23 ottobre 1989*, in *Il Foro Italiano: giurisprudenza penale*, vol. 113, II, 1990, 461 ss.

CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, II ed., Milano, 2022.

CLARKE, *Privacy impact assessment: Its origins and development*, in *Computer law & security review*, 25, 2009, 123 ss.

CORI, *Reati informatici e data breach. La compliance aziendale tra misure tecniche ed organizzative adeguate per la sicurezza del trattamento e modelli di organizzazione e gestione idonei*, in MASSARO (a cura di), *Diritto penale e privacy*, Pisa, 2020.

CORRIAS LUCENTE, *Commento all'art. 5*, in CORASANITI, CORRIAS LUCENTE (a cura di), *Cybercrime, responsabilità degli enti e prova digitale : commento alla Legge 18 marzo 2008, n. 48*, Padova, 2009.

CORRIAS LUCENTE, *I reati di danneggiamento informatico*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Trattato di diritto penale. Parte speciale*, X, Torino, 2011.

CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, 2009.

DAMBRUSO, *Il cyberterrorismo di matrice religiosa*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, Milano, 2019.

DANIELE, *Diritto dell'Unione Europea*, 6ª ed., 2018, Milano.

DE MATTEIS, *sub artt 635 bis, ter, quater, quinquies*, in LATTANZI, LUPO (diretto da) *Codice penale*, XII, Milano, 2010.

DE MATTEIS, *L'articolo 83 TFUE e la competenza dell'unione in materia di diritto penale sostanziale*, in *Diritto Penale sostanziale e processuale dell'Unione Europea*, volume 1, 2011, Padova.

DE MINICO, *Libertà in rete. Libertà nella rete*, 2ª ed., 2020, Torino.

DENNING, *Activism, hacktivism, and cyberterrorism: the internete as a tool for influencing foreign policy*, in ARQUILLA, RONFELDT (a cura di) *Networks and netwars. The future of terror, crime and militancy*, Santa Monica, 2001.

DI GIACOMO, *Protocollo addizionale alla convenzione di Budapest sulla criminalità informatica: l'Italia che guarda al futuro*, in *diritto.it*, 2022, *https://www.diritto.it/protocollo-addizionale-alla-convenzione-di-budapest-sulla-criminalita-informatica-litalia-che-guarda-al-futuro/*.

DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti*, Milano, 2022.

DOLCINI, *L'imputazione dell'evento aggravante. Un contributo di diritto comparato*, in *Riv. it. dir. proc. pen.*,1979, 755 ss.

ELLI, ZALLONE, *Il nuovo Codice della privacy: commento al d.lgs. 30 giugno 2003 n. 196, con la giurisprudenza del Garante*, Torino, 2004.

FABBRI, *L'indagine "indice di criminalità 2021"*, in *CybersecurityItalia*, *https://www.cybersecitalia.it/cyber-crimine-800-reati-informatici-al-giorno-in-italia-nel-2021-soprattutto-nelle-citta-del-nord/14871/*.

FAGGIOLI, *Computer crimes*, 1998, Napoli.

FELLUGA, *I Computer crimes: definizioni ed elementi principali*, in *Tigor: rivista di scienze della comunicazione e di argomentazione giuridica*, IV, 2012, Trieste, 27 ss.

FIANDACA, MUSCO (a cura di), *Diritto penale. Parte generale*, 7ª ed., 2015, Bologna.

FIANDACA, MUSCO (a cura di), *Diritto penale. Parte speciale, Volume I*, 7ª ed., 2015, Bologna.

FIANDACA, MUSCO (a cura di), *Diritto penale. Parte speciale, Volume II, Tomo I* 7ª ed., 2015, Bologna.

FIANDACA, MUSCO (a cura di), *Diritto penale. Parte speciale*, *Volume II, Tomo II* 7ª ed., 2015, Bologna.

FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Diritto Penale Contemporaneo*, 2012.

FLOR, *Cyber-terrorismo e diritto penale in Italia*, in WENIN, FORNASARI (diretto da), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, 2015.

FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. Proc. Pen*, 2015, 10, 1296 ss.

FLOR, *Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti*, in SPENA, MILITELLO (a cure di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018.

FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, Milano, 2019.

FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, Milano, 2019.

FORNASARI, *Il ruolo della esigibilità nella definizione della responsabilità penale del Provider*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Milano, 2004.

FURTH, ESCALANTE, *Handbook of Cloud Computing*, Berlino, 2018.

GAGLIANO, *La guerra asimmetrica e la strategia moderna*, in *Osservatorio globalizzazione*, 2019, *https://osservatorioglobalizzazione.it/osservatorio/guerra-asimmetrica-gagliano-giuseppe/*.

GALDIERI, *Il diritto penale dell'informatica: legge, giudice, e società*, Torino, 2021.

GALLO, *Il delitto di attentato nella teoria generale del reato*, Milano, 1966.

GALLO, voce *Attentato*, in *Digesto delle discipline penalistiche*, I, 1987, 340 ss.

GALLO, *Delitti aggravati dall'evento e delitti di attentato*, in *Giur. it.*, n. 11, 1990, 1001 ss.

GALLUS, PINTUS, *Data protection impact assesment*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, II ed., Milano, 2022.

GAMBARDELLA, *L'abrogazione della norma incriminatrice*, Napoli, 2008.

GIUSTI, *Strategia UE per la cyber security e armonizzazione normativa: obiettivi e possibili conflitti*, in *Cybersecurity360*, 2022, *https://www.cybersecurity360.it/legal/strategia-ue-per-la-cyber-security-e-armonizzazione-normativa-obiettivi-e-possibili-conflitti/*.

GROSSO, PADOVANI, PAGLIARO (a cura di), *Trattato di diritto penale. Parte generale*, Vol IV, Milano, 2008.

GULLO, *La responsabilità dell'ente e il sistema dei delitti di ricilclaggio*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Diritto penale dell'economia*, Milano, 2019.

GULLO, *I modelli organizzativi*, LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti: diritto sostanziale*, Vol 1, Torino, 2020.

GULLO, *I reati informatici*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti: diritto sostanziale*, Vol 1, Torino, 2020.

IAGNEMMA, *Il reato omissivo improprio nel quadro di un approccio sistematico all'evento offensivo*, in *Criminalia*, 2020.

IANESE, *Attacchi Malware, Ransomware e DDOS: quando sono,* in *SmartIUS*, 2021, *https://www.smartius.it/data-it-law/malware-ransomware-ddos-quando-sono-reato/*.

IASELLI, *Le nuove frontiere del cyber risk*, in *Altalex*, 2017, *https://www.altalex.com/documents/news/2017/09/06/le-nuove-frontiere-del-cyber-risk*.

IASELLI, *Pseudonomizzazione*, in *Altalex*, 2018, *https://www.altalex.com/documents/altalexpedia/2018/06/04/pseudonomizzazione*.

IASELLI, *Internet Service Provider. Guida all'ISP: cos'è, regime e tipologie di responsabilità,* in *Altalex*, 2019. *https://www.altalex.com/guide/internet-service-provider*.

IASELLI, *Compliance. Sanzioni e responsabilità in ambito del GDPR*, Milano, 2019.

IASELLI, *Il Phishing*, in *Altalex*, 2020, *https://www.altalex.com/guide/phishing*.

IASELLI, *La normativa di riferimento*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, II ed., Milano, 2022.

INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, in *Diritto Penale contemporaneo*, 2012;

INGRASIA, *Le sentenze della Cassazione sul caso Google*, in *Diritto penale contemporaneo*, 2014.

INSOLERA, *Profili di tipicità del concorso : causalità, colpevolezza e qualifiche soggettive nella condotta di partecipazione*, in *Rivista italiana di diritto e procedura penale*, 1998.

LATTANZI (a cura di), *Reati e responsabilità degli enti: guida al d.lgs. 8 giugno 2001, n. 231*, 2 ed., Milano, 2010.

LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti: diritto sostanziale*, Vol 1, Torino, 2020.

LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti: diritto processuale,* Vol 2, Torino, 2020.

LEONE, *Il nuovo danneggiamento informatico*, in *Cyberspazio e Diritto*, Vol. 11, n. 1, 2010, 212 s.

LESSIG, *The Law of the Horse: What Cyberlaw Might Teach, in Harvard Law Review*, 1999, 113.

LIVI, ONORATI (a cura di*) La "Cybersecurity law"*, in *Telsy*, 2022.

MAIOLI, SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, in *Altalex*, 2012, *https://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008.*

MANTOVANI, *Danneggiamento e deturpamento di cose altrui*, in *Digesto penale,* III, Torino, 1989.

MANTOVANI, *Diritto penale. Parte generale*, ed. XI, Milano, 2020.

MANTOVANI, *Diritto penale. Parte speciale II*, ed. VIII, Milano, 2022.

MANTOVANI, *Diritto penale. Parte speciale I*, ed. VIII, Milano, 2022.

MANZARI, *La convenzione di Budapest, l'alba di una normativa di contrasto al* cyber crime, in *bptmavvocati*, *https://www.bptmavvocati.it/portfolio/i-reati-informatici-e-la-convenzione-di-budapest/.*

MARTORANA, PINELLI, *Terrorismo sul web e contenuti online: il nuovo regolamento UE*, in *Altalex*, 2021, *https://www.altalex.com/documents/news/2021/05/25/terrorismo-web-contenuti-online-nuovo-regolamento-europeo*.

MARINI, *Thyssenkrupp: quella sottile linea di confine tra dolo eventuale e colpa cosciente*, in *Altalex*, 2014, *https://www.altalex.com/documents/news/2014/10/06/thyssenkrupp-quella-sottile-linea-di-confine-tra-dolo-eventuale-e-colpa-cosciente*.

MARINO, *I diritti degli interessati*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, II ed., Milano, 2022.

MARINUCCI, DOLCINI, GATTA (a cura di), *Manuale di Diritto Penale. Parte Generale*, 11ª ed., Milano, 2022.

MARINUCCI, DOLCINI, GATTA (a cura di), *Manuale di Diritto Penale. Parte Speciale*, 11ª ed., Milano, 2022.

MARTINI, MOSCA, SPECCHIO, *Sfida accountability, così la normativa spinge il busines*, 2020, in *https://www.agendadigitale.eu/sicurezza/privacy/__trashed-24/*

MASSARO (a cura di), *Diritto penale e privacy*, Pisa, 2020.

MAZZA, *Computer Crimes e Tecnologie informatiche*, in *Rivista di Polizia*, 2007.

MAZZA, *Prevenzione e repressione in tema di reati informatici*, in *Osservatorio Penale*, 2016.

MINISTERO DI GRAZIA E GIUSTIZIA, *Schema di disegno di legge contenente modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*: *relazione*, atto Camera 2773, 1993.

MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti*, Milano, 2022.

MONTI, *Un caso di studio: il modello organizzativo 231 nei servizi di cybersecurity*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti*, Milano, 2022.

MONTI, *Il modello organizzativo 231 e la protezione dei dati personali*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti*, Milano, 2022.

OBIZZI, *I reati commessi su Internet: computer crimes e cybercrimes*, in *https://www.fog.it/corsoinformatica/reati.htm*, 2009.

OCCHIPINTI, *Criminalità informatica, il secondo protocollo addizionale alla Convenzione di Budapest*, in *Altalex*, 2022, *https://www.altalex.com/documents/news/2022/05/26/criminalita-informatica-secondo-protocollo-addizionale-convenzione-budapest*.

PADOVANI, *La tipicità inafferrabile. Problemi di struttura obiettiva delle fattispecie di attentato contro la personalità dello Stato*, in Aa. Vv., *Il delitto politico dalla fine dell'ottocento ai giorni nostri*, Roma, 1984.

PARODI, SELLAROLI, *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020.

PECORELLA, *Diritto penale dell'informatica*, Milano, 2006.

PECORELLA, *Reati informatici*, in AA. VV., *Enciclopedia del diritto. Annali X*, Milano, 2017, 707 ss.

PELISSERO, *Responsabilità degli enti*, in ANTOLISEI, *Manuale di diritto penale. Leggi complementari*, Vol II, Milano, 2018.

PEZZUTO, *Contenuti terroristici on line: l'unione europea lavora a nuove norme per prevenirne la diffusione*, in *Diritto penale contemporaneo*, 2019.

PICA, *Diritto penale delle tecnologie informatiche*, Milano, 1999.

PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993.

PICOTTI, *La responsabilità penale dei service providers in internet*, in *Dir. pen. proc*., 1999, 501 ss.

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*, Milano, 2004.

PICOTTI, *La ratifica della Convenzione* cybercrime *del Consiglio d'Europa - profili di diritto penale sostanziale*, in *Dir. Proc. Pen*, 2008, 6, 700 ss.

PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, Milano, 2019.

PICOTTI, VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in *Sist. pen.*, 2019.

PICOTTI, *Cybercrime e tutela penale dei diritti della persona e della privacy nel web*, in *AIAF*, n. 1, 2020.

PICOTTI, *I delitti informatici previsti dal g.lgs. n. 231/2001*, in MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti*, Milano, 2022.

POMANTE, *Internet e criminalità*, 1999, Torino.

RESTA, Cybercrime *e cooperazione internazionale nell'ultima legge della legislatura*, in *Corriere del merito*, 2008, n. 9, 2147 ss.

RIJTANO, *Cosa sono il Deep Web e il Dark Web, cosa si trova e come si accede: tutte le istruzioni*, in *Cybersecurity360*, 2022, *https://www.cybersecurity360.it/cultura-cyber/cose-il-deep-web-e-il-dark-web-cosa-si-trova-e-come-si-accede-tutte-le-istruzioni/*.

RODOTÀ, *Intervista su privacy e libertà*, Bari, 2005.

RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*. Bari, 2014.

SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici, un bilancio poco esaltante*, in *Riv. it. dir. proc. pen.*, 2012.

SARZANA DI S. IPPOLITO, *Criminalità e tecnologia: il caso dei computer crimes, in Rassegna penitenziaria e criminologica*, n. 1, 1979.

SARZANA DI S. IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. e proc.*, 2008, 1572.

SCHIAVONE, *I diversi aspetti della sicurezza dei dati personali*, in *Cyberlaws*, 2022, *https://www.cyberlaws.it/2022/sicurezza-dati-personali/*.

SCOLETTA, *Art. 6 - profili penalistici*, in CASTRONUOVO, DE SIMONE, GINEVRA, LIONZO, NEGRI, VARRASO (a cura di) *Compliance. Responsabilità da reato degli enti collettivi*, Milano, 2019.

SCOPINARO, *Internet e reati contro il patrimonio*, Torino, 2007.

SCUDERI, *La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea*, in *Diritto Mercato Tecnologia*, 2018.

SCUDIERO, *Il consenso come condizione di liceità*, in CASSANO, COLAROCCO, GALLUS, MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, II ed., Milano, 2022.

SEMINARA, *La pirateria su internet e il diritto penale*, in *Rivista trimestrale di diritto penale dell'economia*, 1997.

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

SICIGNANO, *Problemi attuali in tema di responsabilità «da reato» degli enti per i delitti informatici. l'interesse e il vantaggio. i modelli di comportamento*, in *Rivista 231*, II, 2022.

SOKOLSKA, *I trattati di Maastricht e di Amsterdam*, in *https://www.europarl.europa.eu/factsheets/it/sheet/3/the-maastricht-and-amsterdam-treaties.*

SPERA, *Il concorso di persone nel reato* , in *Altalex*, 2020

STEFANI, *European Cybercrime Center: come lavora e di cosa si occupa il centro europeo per il cybercrime*, in *Cybersecurity360*, 2021, *https://www.cybersecurity360.it/cybersecurity-nazionale/european-cybercrime-centre-come-lavora-e-di-cosa-si-occupa-il-centro-europeo-per-il-cyber-crime/.*

TONINI, CONTI, *Manuale di procedura penale,* ed. XXII, Milano, 2021.

TORRINI, *Cos'è un attacco informatico e quali sono le diverse tipologie*, in *UniversIT*, 2021, *https://universeit.blog/attacchi-informatici/.*

VERDE, *I reati informatici*, in *Diritto.it*, 2020, *https://www.diritto.it/i-reati-informatici/.*

VIGNERI, *Cyberterrorismo: realtà o finzione? Profili problematici di definizione e contrasto*, in *Altalex*, 2018, *https://www.altalex.com/documents/news/2018/09/06/cyberterrorismo-profili-problematici-di-definizione-e-contrasto*.

INDICE DELLE SENTENZE

Cass. Pen., Sez. Un., 19.05.1957, Toffanin e altri, in *Il foro italiano*, Vol. 81, II, 1958.

Cass. Pen., Sez. Un., 14.03.1970, p. m. c. Kofler ed altri, in *Il Foro italiano*, Vol. 94, III, 1971.

Cass. Pen., Sez. Un. 18.06.1983, n. 6309, in *Cassazione penale*, II, 1984.

Cort. App. Pen. 29.11.1990 Vincenti e altro, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. Un., 14,05,1996, n. 2, in *Altalex*, *https://www.altalex.com/documents/news/2004/10/19/cassazione-penale-ss-uu-sentenza-14-02-1996-n-2.*

Cass. Pen., Sez. Un., 9.10.1996, n. 1282, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cort. Cost 21.11.2000, n. 519, in *Foroplus, https://www.foroplus.it/home.php.*

Cass. Pen. Se. II, 11.11.2009, n. 44720, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. V, 28.06.2011, n. 25674, in *Foroplus*, *https://www.foroplus.it/home.php.*

Corte di Giustizia EU, 25.10.2011, (C-509/09, C-161-10), in *eur.lex, https://eur-lex.europa.eu/homepage.html.*

Cass. Pen., Sez. VI, 16.04.2012, n. 14342, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. V, 18.11.2012, n. 8555, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. III, 17.12.13, n. 5107, in *Foroplus*, *https://www.foroplus.it/home.php*.

Cass. Pen., Sez. I, 27.05.2013, n. 40303, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. Un., 18.09.2014, n. 38343, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. I, ord. 28.10.2014, n. 52575, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. Un. 24.04.2015, n. 17325, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. I, 9.09.2015, n. 40699, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. I, 23.12.2019, n. 51870, in *Foroplus*, *https://www.foroplus.it/home.php.*

Cass. Pen., Sez. I, 17.01.2020, n. 1767, in *Foroplus*, *https://www.foroplus.it/home.php.*