DIPARTIMENTO DI GIURISPRUDENZA

Cattedra di Diritto Penale, Parte speciale

RELATORE

Prof. Antonino Gullo

CANDIDATO

Andrea Gili

Matricola 136723

CORRELATORE

Prof. Maurizio Bellacosa

Anno Accademico 2019-2020

Danneggiamenti informatici e *dual use software*

Sommario

INTRODUZIONE

Internet è ormai diventato un luogo nel quale svolgiamo buona parte delle nostre attività quotidiane, una realtà digitale in cui immettiamo informazioni e compiamo operazioni senza considerare, spesso a causa di una desensibilizzazione generale e comune, i pericoli a cui andiamo incontro. È un mondo sentito come lontano e "fittizio" in cui pensiamo di non poter essere controllati o osservati, tuttavia l'esperienza dimostra come proprio nel *cyberspace* la criminalità sia in continua evoluzione.

L'immagine dell'*hacker* che si intrufola all'interno di sistemi informatici di grandi imprese per finalità spesso "simboliche" lascia il posto ad attività criminali vere e proprie con l'intento di procurarsi un guadagno e in alternativa o, spesso, in aggiunta di recare un danno ai propri *competitors*.

Se ciò non bastasse, muta il prototipo di autore dei reati commessi in rete: in particolare, alle persone "qualificate" per capacità e conoscenze si affiancano persone "ordinarie" che divengono i principali soggetti a commettere reati

informatici "in senso lato" o che facilitano, con i loro comportamenti, le condotte di altri soggetti.

Non ci si trova più davanti a un mondo digitale privo di regole se non quelle imposte dagli stessi utenti come all'inizio dell'era della rivoluzione digitale, il legislatore – nazionale e sovranazionale – ha deciso di dover intervenire per arginare il fenomeno dell'eccessiva anarchia informatica con una serie di atti di regolamentazione.

I reati informatici denunciati solo in Italia aumentano di anno in anno senza per questo ancora avvicinarsi ai numeri sommersi di una criminalità informatica che cresce e trova sempre nuovi modi per palesarsi.

I primi tentativi di normare la materia si sono manifestati con l'introduzione di nuovi articoli che hanno arricchito il Codice penale[1] ma si è fatta man mano più forte la consapevolezza che fosse impossibile scovare persona per persona e reato per reato in una piattaforma così vasta com'è il mondo digitale.

È così che la Convenzione di Budapest del 2001, ratificata in Italia nel 2008, ha cercato di delineare fattispecie di reato capaci di arginare condotte illecite poste in essere con l'utilizzo della realtà informatica e telematica[2].

Tuttavia, bisogna fin da subito comprendere come i *Cybercrime*s non siano la *Cybersecurity*[3], vi rientrano ma non la completano. La tutela repressiva offerta dal diritto penale classico contro i reati informatici si è rivelata insufficiente per garantire la sicurezza delle persone che esercitano le proprie attività in rete, è per questo che negli anni si è sempre più affiancata a essa una tutela preventiva mirata a potenziare le misure di sicurezza poste a garanzia dei sistemi informatici o telematici.

Una delle soluzioni che il legislatore – sia italiano che sovranazionale – ha adottato per far fronte a questa realtà è stata quella di definire le misure necessarie

[1] Come accaduto con la legge 23 dicembre del 1993, n. 547, apportante ‹‹Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica››.

[2] Sulla questione si rimanda a LUPÀRIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in Dir. Pen. e Proc., 6, 2008; PICOTTI L., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, 5, 2008; PICOTTI L., *La ratifica della Convenzione di Budapest sul Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc. 6*, 2008.

[3] La sicurezza informatica è, per definizione, ‹‹l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici››.

a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi con la disciplina contenuta nel Decreto Legislativo 18 maggio 2018, n. 65 con cui l'Italia ha dato attuazione alla Direttiva (UE) 2016/1148, c. d. Direttiva NIS. Gli obiettivi di questa Direttiva erano già stati in parte recepiti dal legislatore che si era attivato autonomamente per tutelare le infrastrutture critiche – come accaduto con il D.P.C.M. Gentiloni del 2017 e la creazione di un piano nazionale di protezione e salvaguardia che è stato solo successivamente ricompreso nel regolamento europeo detto "*Cybersecurity act*" del 2019, ampliando ulteriormente l'orizzonte normativo. Da ultimo, questi interventi legislativi sono stati d'ispirazione per l'emanazione della legge 133 del 2019 in materia di perimetro di sicurezza nazionale cibernetica al fine di assicurare un elevato *standard* di sicurezza delle reti e dei sistemi informatici della pubblica amministrazione nonché degli enti e degli operatori sia in ambito privato che pubblico.

Peraltro, il mondo dell'informatica è in costante fermento e continuamente viene ampliato o vengono prodotti o adattati nuovi strumenti che rendono possibile uno sviluppo della persona e uno sfruttamento economico simile a quello che si può avere sul piano fisico. Tra le ultime innovazioni si sono aggiunti, negli ultimi anni, proprio i *dual use software* la cui materia è ancora oggi complessa, lacunosa e non particolarmente ben delineata anche a causa del difficile inquadramento di questi programmi nelle categorie generali da sempre utilizzate nel nostro ordinamento penale come in quello di altri Paesi europei.

Nel corso di questa trattazione si analizzerà dunque l'evoluzione legislativa sopra accennata, mettendo in luce gli aspetti più critici di una disciplina in continua evoluzione e perennemente divisa tra la necessità di tutela e quella di repressione.

Nel primo capitolo ci si soffermerà sulla definizione di un sistema informatico o telematico, come esso possa essere messo in pericolo da determinate condotte e le forme di tutela che si sono adottate nel corso del tempo sia a livello internazionale che nazionale nonché la loro evoluzione per avere un quadro generale della normativa in ambito *cybercrime.* Questo apparato di fonti sarà importante per poter studiare in seguito la normativa adottata per tutelare interessi direttamente connessi alla successiva trattazione riguardante i *dual use software*.

Si affronteranno anche, in maniera approfondita, definizioni intorno alle quali ruota la discussione dottrinale e giurisprudenziale nazionale, in particolar modo gli articoli che costituiranno poi l'argomento del capitolo immediatamente seguente.

Nel corso del secondo capitolo, dopo aver trattato precedentemente le fonti normative nonché dottrinali e giurisprudenziali della materia in questione, si procederà con l'analisi di quell'insieme di articoli con cui a livello nazionale si cerca di tutelare beni giuridici interessati – direttamente o indirettamente – dalla materia dei *dual use software* e dei programmi informatici malevoli in generale. In particolar modo ci si soffermerà sull'accesso abusivo ad un sistema informatico o telematico (artt. 615-*ter* ss.), sulle intercettazioni informatiche e telematiche (artt. 617-*quater* ss.) e sulle fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635-*bis* ss.). Tutte fattispecie che normalmente vengono o possono essere perseguite tramite l'utilizzo di un programma informatico idoneo a commettere un reato e che costituiranno la base di partenza per poter successivamente trattare di una corretta incriminazione dei *dual use software*.

Nel terzo capitolo, infine, si arriverà a parlare di una nuova fattispecie introdotta nel panorama digitale internazionale (l'utilizzo dei *dual use software*) così da comprendere come il legislatore europeo e quello nazionale si siano posti nei confronti di questa nuova possibile realtà di danneggiamento informatico.

La complessità della materia, di relativamente nuova introduzione, è dovuta alla difficoltà di inquadramento di questi *software* – che costituiscono l'oggetto materiale di diversi reati – che come tutti i "*dual use goods*" possono essere utilizzati sia per fini illeciti sia per ragioni assolutamente legittime e che, anzi, vengono incoraggiate dalla comunità (soprattutto per il potenziamento delle misure di sicurezza cibernetiche).

Sul finire del capitolo si cercherà di trarre delle conclusioni sull'utilizzo di questi programmi informatici – dopo averne delineato una definizione e spiegato il funzionamento – e si proverà a suggerire un posizionamento corretto a livello di inquadramento normativo che potrebbe essere seguito per proposte di *lege ferenda*.

CAPITOLO I

IL DANNEGGIAMENTO INFORMATICO

1.1 Cos'è un sistema informatico o telematico

Le fattispecie di accesso abusivo ad un sistema informatico o telematico e di danneggiamento informatico, oggetto della presente analisi, si focalizzano sul concetto di sistema informatico o telematico, dal cui inquadramento occorre pertanto prendere le mosse. Tale operazione si rileva assai complessa dal momento che il legislatore non ha previsto una specifica definizione del concetto di "sistema informatico o telematico", con la conseguenza che il termine può prestarsi a diverse letture. Esistono, in particolar modo, due interpretazioni che devono essere tenute in considerazione.

Un'interpretazione più rigorosa suggerisce che vada inteso come "sistema" esclusivamente un complesso articolato di attrezzature o macchinari in grado di interagire tra loro; tuttavia, così facendo, risulterebbe escluso dalla tutela il singolo *personal computer*, destinato ad operare senza collegamenti, continui o occasionali, con altri elaboratori o sistemi. Se si considerasse solo questa opzione, quindi, si limiterebbe la tutela, da un lato, all'oggetto "intrinseco" dell'attività (dati, informazioni e programmi) e, dall'altro lato, alle realtà costituite da pluralità funzionali di elaboratori, con un'esclusione assolutamente illogica. Certo, tale problema potrebbe essere aggirato nello specifico caso di una singola unità informatica o telematica collegata ad un *modem* e quindi considerabile, in senso

lato, parte di un sistema telematico, tuttavia, è da sposare, per semplice efficacia fattuale nella realtà quotidiana, la teoria che ritiene il singolo elaboratore riconducibile al concetto di sistema informatico: basta intendersi come tale ‹‹un sistema di risorse, composto da dispositivi di elaborazione elettronica digitale, programmi memorizzati e gruppi di dati che, sotto il controllo dei programmi memorizzati, immette, tratta ed emette automaticamente dei dati che può memorizzare e recuperare››[4], così da estendere anche al semplice *personal computer* – inteso nella sua globalità funzionale – la tutela offerta dal Codice penale.

1.2 La riservatezza informatica

Chiarito che la presente trattazione riguarderà sia i grandi sistemi informatici o telematici sia il più comune *personal computer* è d'obbligo portare l'attenzione su uno dei beni giuridici che, comunemente, è associato ai reati informatici: la *privacy*.

Internet è nato ed è diventato sempre più nel corso degli anni un luogo in cui sono conservate informazioni provenienti da tutto il mondo e appartenenti a un novero immenso di persone fisiche e giuridiche. Il primo intento del legislatore fu quello, nell'ormai lontano 1993, di tutelare il diritto delle persone a conservare il segreto sulle proprie informazioni personali: internet veniva visto come una stanza chiusa, un domicilio virtuale che trovava la sua piena tutela nel principio contenuto all'articolo 14 della Costituzione – ‹‹il domicilio è inviolabile››[5] – e che, d'altronde, giustificava l'accostamento dell'articolo 615-*ter* e successivi agli articoli 614 e 615 del Codice penale[6]. In poche parole, l'interesse era quello di garantire lo "*ius excludendi alios*" facendo sì che le informazioni inserite all'interno del proprio computer restassero in nostro possesso, punendo ogni comportamento contrario portato da altre persone.

---

[4] Cfr. GALDIERI P. *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997.
[5] Articolo 14 della Costituzione italiana, primo comma.
[6] Come d'altronde si poteva evincere dalla stessa lettura della *Relazione di presentazione dello schema di progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penale in tema di criminalità informatica*, in *Doc. giust*., 1991, n. 9, 142 ss.

Tuttavia, internet al giorno d'oggi non è più solo una banca dati. In questo mondo digitale parallelo e interconnesso si estrinsecano le nostre vite così come i nostri interessi: possiamo cercare informazioni, inserirle o conservarle ma, allo stesso tempo, ci mettiamo in contatto con altre realtà e ci è sempre più facile poter comunicare con persone anche molto distanti ad un prezzo contenuto e popolare. Non abbiamo più uno schermo nero con scritte verdi da compilare inserendo input ed ottenendo output, un'attività spesso in passato riservata a specifici tecnici. Oramai, fin dalla più tenera età, siamo abituati ad entrare in contatto con le nuove tecnologie dell'informazione e della comunicazione che ci permettono di trattare con estrema facilità e rapidità un grande numero di dati, consentendo di manifestare liberamente la propria personalità e di poter svolgere ogni tipo di attività a livello umano o lavorativo. Dobbiamo quindi ampliare il nostro focus considerando che la tutela non possa cadere solo sulla semplice tutela della *privacy* in senso stretto bensì sulla salvaguardia generale di questo ambiente nel quale sempre più facilmente ci troviamo a muoverci[7].

Ciò è già stato recepito dal nostro legislatore, basta prendere ad esempio l'accesso abusivo ad un sistema informatico o telematico (articolo 615-*ter* c.p.) che si configura anche nel caso in cui all'interno del sistema non siano memorizzati dati personali o un qualunque *software*. Si vuole, quindi, garantire la libera, esclusiva e pacifica fruizione di tutti i nuovi spazi aperti dall'evoluzione tecnologica così da permettere la piena estrinsecazione della personalità dell'utente indipendentemente da interferenze altrui.

Questa necessità non è sentita solo a livello nazionale ma anche a livello europeo in linea con quanto stabilito dall'articolo 10 della CEDU e dall'articolo 11 della Carta di Nizza: un cammino recepito e contenuto nella Direttiva 2013/40/UE, stabilendo l'obbligo per gli Stati membri di punire l'intercettazione non autorizzata di trasmissioni "non pubbliche" di qualsiasi tipologia di dato informatico a prescindere, dunque, dal suo contenuto[8].

---

[7] Tale teoria non convince tutta la dottrina come accade, per esempio, in PECORELLA C., *Sub art 617-quater c.p.*, in DOLCINI E.-GATTA G.L. (a cura di), *Codice penale commentato*, t. III, 4ª ed., Milano, 2015,670 ss., per i quali gli articoli in materia di intercettazioni informatiche e telematiche tutelano unicamente i messaggi interpersonali.

[8] Si legga al riguardo *Cybercrime* Convention, *Explanatory Report*, n. 54.

Che ad oggi la stessa legislazione italiana non tuteli più la mera sfera di acquisizione di tali informazioni scambiate a mezzo internet ma il generico diritto di potersi muovere in una sfera protetta senza vedere le proprie attività spiate è dimostrato dalla presenza dell'articolo 617-*quater* c.p. che punisce, con lo stesso trattamento sanzionatorio, oltre "all'intercettazione illecita di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi", anche il loro impedimento o interruzione. Non entra in gioco la materiale conoscenza del contenuto delle comunicazioni quanto il fatto che tali comunicazioni incidano sulla libertà, l'integrità e la sicurezza di queste ultime[9].

Altro esempio è offerto dall'articolo 617-*quinquies* c.p. che punisce la condotta di chi "fuori dai casi previsti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico"; così come dall'articolo 617-*sexies* c.p. che tutela, prima ancora della riservatezza dei dati, la loro veridicità e l'affidabilità del contenuto dei dati informatici nel corso della loro trasmissione tra sistemi[10].

Come tale la tutela giurisdizionale è sempre più risalita a monte nel corso del tempo: non si tratta più di garantire l'inviolabilità del proprio domicilio virtuale – concetto oltretutto sfuggente e dai confini ancora oggi discussi – andando oltre alla tutela offerta dall'articolo 614 c.p.[11], né di tutelare (soltanto) la riservatezza dei dati inseriti che ben potrebbero essere già conosciuti e quindi privi di un valore specifico, quanto, piuttosto, proteggere ed assicurare a ciascuno il godimento indisturbato ed esclusivo di spazi virtuali nel quale avere libertà di estrinsecare la nostra personalità e pervenire ad uno sviluppo del nostro carattere e al soddisfacimento dei nostri interessi individuali o collettivi.

Il valore economico di ciò che facciamo nella realtà digitale si sta progressivamente spostando dalle aziende intese come poli collettori di denaro a noi, singole persone che ci muoviamo in uno spazio spesso non compreso

---

[9] A sostegno di questa visione si rimanda a CORASANITI G., *La tutela della comunicazione informatica e telematica*, in BORRUSO G.-CORASANITI G.-D'AIETTI G. (a cura di), *Profili penali dell'informatica*, Milano, 1994, 101 ss., 120; oltre che a PICOTTI L., *La tutela penale della persona*, cit., 63.

[10] Durante la così detta "fase dinamica" come si può leggere in PICOTTI L., *Commento all'art. 6 della legge 23-12-1993 n. 547*, in *Leg. pen.*, 1996, 118 ss., 124.

[11] Che nonostante tutto trova ancora oggi dei fautori come PLANTAMURA V., *Domicilio e diritto penale nella società post-industriale*, Pisa, 2017, 185 ss.

pienamente: per quanto da noi il più delle volte ignorato è una verità inconfutabile che la nostra vita abbia, nel vero senso della parola, un valore economico per le imprese che operano sia dentro che fuori il mondo digitale. Si sta parlando di pochi centesimi o di qualche dollaro al massimo ma le nostre personalità hanno un valore e vengono continuamente vendute e scambiate all'interno di un sistema immateriale ed intoccabile, cosa che dovrebbe metterci maggiormente in guardia.

Fin dai tempi di Warren e Brandeis con il saggio "*The right to privacy*", edito nel lontano 1890, l'interesse alla tutela della nostra sfera personale è stato un punto fisso di tutta la civiltà occidentale, tuttavia ad oggi è diventato sempre più difficile, per il singolo, rendersi conto di quanto tale sfera sia messa in pericolo dalle proprie stesse attività personali. Eppure, la rilevanza sociale di tale realtà ha acquistato nel corso del tempo sempre maggiore eco tanto che, attualmente, la "riservatezza informatica" è espressamente richiamata nella Convenzione *Cybercrime* del Consiglio d'Europa il cui titolo I è dedicato alla "confidenzialità dei dati e dei sistemi informatici".

Non bisogna però confondere la "riservatezza informatica" con le sfere contigue del segreto e della riservatezza domiciliare, nonché della *privacy*[12]. Dobbiamo immaginarla come un contenitore più ampio rispetto al concetto di riservatezza ordinario che normalmente viene distinta in "riservatezza" (*privatsphäre*) e "segreto" (*Geheimsphäre*), riguardando queste specificatamente gli ambiti che abbracciano il concetto tradizionale di tutela di dati ed informazioni, escludendo quanto viene trattato con mezzi informatici o telematici.

Allo stesso tempo la "*privacy*" non coincide del tutto con la "riservatezza informatica" dato che la prima viene in rilievo anche rispetto ai "trattamenti" di dati effettuati senza l'ausilio di strumenti elettronici, concentrandosi in particolar modo sulla sfera dei "dati personali" (che possono essere sensibili, giudiziari, biometrici, medici ecc.). Oltretutto la "*privacy*", intesa nel senso moderno, ricomprende quanto appena esposto ma va anche oltre concentrando la propria disciplina sulla possibilità d'esercitare il controllo quanto più forte e completo sulla circolazione dei propri dati personali e sull'accessibilità di essi da parte di

[12] PATRONO P, *Privacy e vita privata*, in *Enc. Dir*., XXXV, Milano, 1986, 557 ss. dà una buona definizione del concetto di privacy dal punto di vista penale, anche se inteso in senso restrittivo e non come diritto alla tutela dei propri dati personali.

terzi. La "riservatezza informatica", intesa come un autonomo bene giuridico da tutelare, si riferisce esclusivamente al sicuro utilizzo e accesso agli spazi virtuali anche se vuoti o privi di qualsivoglia informazione[13].

Dobbiamo quindi comprendere come il tutto sia posto a salvaguardia dell'individuale interesse del singolo utente ad avere la disponibilità esclusiva e libera delle nuove realtà tecnologiche e di spazi virtuali nel quale è facile incappare in illegittime interferenze. Se così non fosse, se non si ponesse un limite lasciando internet privo di leggi o norme come alcuni vorrebbero, si otterrebbe l'effetto contrario di scoraggiare l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione, così come la pirateria in tempi passati scoraggiava la navigazione mercantile anche a causa della facilità con cui, tenendo conto dell'interconnessione dei sistemi di informazione, sia possibile accedere e prendere coscienza dei dati e delle comunicazioni in giro per la rete.

La riservatezza informatica si eleva, dunque, ad un diritto fondamentale dell'uomo quale manifestazione del generale diritto alla personalità che ritroviamo nell'articolo 2 della Costituzione così come nell'articolo 8 della CEDU e negli articoli 8 e 9 della Carta dei diritti fondamentali dell'Unione Europea i quali si affiancano al diritto inviolabile del domicilio, al rispetto della vita privata e alla libera manifestazione del pensiero oltre che alla segretezza delle comunicazioni[14].

È chiaro, quindi, che si tratta di un interesse che in primo luogo è meritevole di tutela penale dato che quella di natura meramente contrattuale, civile o amministrativa non è in grado di fornire da sola la protezione che un bene così importante sta acquisendo nella nostra realtà quotidiana e che, allo stesso tempo, è messa in serio pericolo dalla facilità con cui è possibile ledere la signoria e la sicurezza su quegli stessi spazi virtuali che ci consentono di estrinsecare

---

[13] La nascita di questo nuovo interesse giuridico ha avuto una lunga evoluzione iniziata già ai tempi di PICOTTI L., *Reati informatici*, 20 ss.; ID., *Sistematica dei reati informatici*, cit., 77 ss.; ID., *La tutela penale della persona*, cit., 59-63; e continuata in SALVADORI I., *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica* ed in PICOTTI L. (a cura di), *La tutela penale della persona*, cit., 125 ss., 149 ss. fino ad arrivare al più recente FLOR R., *Riservatezza informatica*, in *Enc. Giur. online*, 2017, 1 ss.

[14] Gettando uno sguardo fuori dall'Italia ad una stessa conclusione è giunta anche la giurisprudenza tedesca che ha espressamente sancito il concetto in una sentenza del *BVERFG 370/2007-595/2007*, del 27.2.2008, in *Riv. trim. dir. pen. economia*, 2009, 695 ss., che attirò anche l'attenzione di FLOR R., *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online Durchsuchung.

liberamente la nostra personalità: emerge così la necessità, sempre più sentita e messa in pratica, di ricorrere allo strumento penale per garantire la fondamentale protezione a questo autonomo bene giuridico.

1.3 Profili di diritto

Stando al nostro attuale livello tecnologico questa piena rappresentazione ed estrinsecazione della personalità del singolo, prima citata, non dipendono unicamente dal livello di sicurezza delle infrastrutture critiche ma in generale dal livello di protezione comune a tutto il sistema telematico o digitale che va dal singolo *personal computer* fino ad arrivare alle nuove tecnologie dell'informazione e comunicazione (da ora in poi denominate semplicemente TIC).

Il corretto funzionamento di questo complesso sistema passa attraverso la corretta accessibilità ai siti *web*, la sicurezza dei dati e dei sistemi informatici e l'affidabilità e la disponibilità dei servizi: in poche parole la riservatezza informatica, atta a garantire la possibilità di tessere rapporti interpersonali, economici e giuridici, dipende quasi totalmente dal raggiungimento di un elevato grado di sicurezza contro comportamenti lesivi ed introduzioni illecite. È così che la riservatezza informatica deve affidarsi, prima di tutto, alla sicurezza informatica come d'altronde è già stato riconosciuto da tempo sia a livello nazionale che internazionale a partire dalla Convenzione *Cybercrime*. È chiaro, infatti, come anche la sicurezza informatica sia a sua volta dipendente dalla disponibilità, dall'autenticità, così come dall'integrità e dalla riservatezza dei dati conservati o operati da un determinato sistema. Bisogna però notare come mentre la riservatezza informatica è ormai stata elevata al grado di autonomo bene giuridico da tutelare, la sicurezza informatica risale ad un ruolo ancora più preminente in quanto destinata a tutelare la prima e dunque attribuendosi una particolare rilevanza di carattere pubblico: la sicurezza informatica deve essere garantita nell'interesse della collettività così da creare uno "*standard*" nel quale possa essere assicurato il corretto funzionamento di programmi o dispositivi sempre più

numerosi e necessari per il corretto svolgimento delle nostre vite[15]. La *Cybersecurity* nasce, nella nostra nazione, con la novella legislativa del 1993 facendo i suoi primi passi proprio nel solco dei *Cybercrime*s: ecco, dunque, presentarsi i delitti di cui all'articolo 615-*ter* e successivi del Codice penale atti a punire le condotte di accesso abusivo ad un sistema informatico o telematico tali da prevenire illecite intrusioni o permanenze all'interno di un sistema protetto da misure di sicurezza, indirettamente tutelando anche le informazioni ed i dati in esso contenuti; stessa cosa dicasi per l'articolo 617-*quater* e ss. c.p. che ancora più tutelano lo scambio dinamico di queste informazioni o dati tra un sistema e l'altro prevedendo la fattispecie di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.

Certo, ad oggi la *Cybersecurity* si è concentrata soprattutto sulla tutela di infrastrutture critiche che gestiscono sistemi informatici di interesse pubblico (protezione civile, traffico ferroviario, aereo ecc…) ma non bisogna sottovalutare la lesività di comportamenti rivolti nei confronti dei singoli: sempre più ci troviamo ad utilizzare i nostri *personal computer* per svolgere attività che possono avere una rilevanza a livello economico, sociale o giuridico e questo perché si sta mano a mano assottigliando la separazione tra sistemi che invece sono sempre più interconnessi. Quante volte, sul posto di lavoro o a casa, usiamo mezzi personali o viceversa per scambiare o conservare informazioni commerciali, professionali, dati sensibili o personali che eventualmente possono riguardare anche soggetti terzi?

Queste informazioni non hanno più una rilevanza unicamente per la persona singola o la specifica impresa, hanno acquistato una propria dimensione super-individuale che si rivolge ad una sfera indeterminata di soggetti. Dunque, prevedere la presenza di reati contro la riservatezza informatica o, in generale, reati informatici "in senso stretto" non è più sufficiente. Non si può più concentrare l'attenzione sulla tutela del singolo "*ius excludendi alios*" come si pensava un tempo, ma soltanto proteggendo il singolo si garantisce anche

[15] Ormai presente nella Direttiva 2016/1148/UE, in particolar modo i n. 3 e 6 del Preambolo. Per quanto riguarda la dottrina nazionale, invece, vedasi PICOTTI L., *Sistematica dei reati informatici*, cit. 74; ed in specie ID., *Sicurezza, informatica e diritto penale*, in DONINI M.-PAVARINI M. (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, 217 ss.

l'interesse collettivo con il regolare funzionamento, integrità e disponibilità dei sistemi.

È da questa consapevolezza che, in origine, il legislatore previde e cercò di realizzare la tutela in modo indiretto di tali nuovi interessi con la fattispecie dell'articolo 615-*quinquies* c.p. e le varie disposizioni in materia di danneggiamenti informatici (artt. 635-*bis* e successivi del Codice penale) sulle quali verterà in particolar modo la presente trattazione.

Allo stesso tempo bisogna sottolineare quanto sia complesso ricondurre la tutela di questi interessi alla mera lettera legislativa. Lessig era solito dire che la regolamentazione in questo ambito sia difficile proprio perché si assiste ad un dominio della tecnica sulla legge: alla luce di complessi codici di programmazione che seguono proprie autonome regole è quasi impossibile far ricadere il tutto nell'ambito di un diritto penale che era stato ai tempi studiato per singoli individui. Lo stesso Lessig suggerisce di concentrarsi su un espediente per aggirare la problematica: dar maggiore importanza al mezzo tecnico più efficace piuttosto che cristallizzarsi inutilmente sullo stigma penale di determinate condotte[16]. Una sempre più efficace sicurezza di reti e di sistemi d'informazione richiede una quanto più forte prevenzione del rischio di commissione di reati informatici che si esplica soprattutto attraverso la tutela e l'autotutela tecnologica: è proprio nel solco di questa evoluzione che si concluderà questa l'analisi[17].

1.4 Evoluzione legislativa a livello nazionale ed europeo

Per la complessità della materia trattata e per il gran numero di convenzioni, direttive e atti normativi che si sono susseguiti nella materia nel corso del tempo conviene trattare in primo luogo la disciplina europea ed internazionale per poi soffermarsi, nel successivo paragrafo, su come la disciplina nazionale abbia recepito e si sia evoluta sotto la s*pin*ta di queste decisioni.

[16] Cfr. LESSIG L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 2000.
[17] Cfr. *infra*, capitolo 3.

1.4.1 Livello europeo

La prima volta che il termine "*cybersecurity*" è stato utilizzato in ambito europeo era il 2008 quando fece la sua comparsa all'interno di un atto ufficiale della Comunità Europea risalente al 2003 riguardante l'implementazione della strategia europea in materia di sicurezza. Per quanto, infatti, anche prima d'allora si fosse spesso discusso dell'argomento ed anche diversi altri atti avessero trattato la questione ci si era sempre riferiti con il generico e restrittivo termine "*cybercrime*"[18] a tutela sia dei dati che delle infrastrutture.

Come si vedrà successivamente, in realtà l'attenzione europea ed internazionale sulla materia era già stata richiamata all'inizio degli anni 2000 e la Commissione europea non era rimasta inerme predisponendo la "comunicazione sul *cybercrime*" mirante a rendere le infrastrutture sicure e a combattere i reati informatici in senso stretto.

Un maggiore focus sull'argomento venne concesso nel 2001 dalla *policy* denominata "*Network and Information Security*" che per la prima volta restrinse l'attenzione a un determinato tipo di minacce: intercettazioni, accessi non autorizzati, interruzioni funzionali delle infrastrutture, usurpazione dell'identità e tutti gli altri eventi indipendenti dalla volontà dell'uomo.

I documenti "eEurope" e "eEurope 2005" sottolineando un contesto improntato all'incremento della competitività e del dinamismo sottolinearono un'importanza sempre crescente della materia nell'ambito comunitario, rappresentato anche dall'emanazione di tre precedenti direttive del 2002, ad oggi assorbite e superate dalla Direttiva Quadro del 2009 sulla materia (contenente un invito rivolto agli Stati membri a dotarsi di autonome autorità nazionali di regolamentazione).

Per tornare al punto di partenza del discorso, nel 2008 si assiste all'implementazione della strategia europea per la sicurezza del 2003: è proprio in questo documento che, per la prima volta, si può trovare l'utilizzo del termine "*cybersecurity*" in ambito europeo. Per quel che qui interessa, nel 2004 si è avuta

[18] "Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo (rispettivamente, si parla di *computer as a tool* e *computer as a target*)". Voce "*cybercrime*", in *Enc. onl. Treccani*, su www.treccani.it/enciclopedia/cybercrime_%28Lessico-del-XXI-Secolo%29/.

un'importante implementazione per la politica europea di *cybersecurity* con l'istituzione di ENISA - l'Agenzia europea di sicurezza delle reti e dell'informazione – il cui scopo principale, come asserito nel Regolamento modificativo del 2013, consiste nel «contribuire ad assicurare un elevato livello di sicurezza delle reti e dell'informazione, a migliorare la tutela della vita privata e dei dati personali e a sviluppare e promuovere una cultura in materia a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione, contribuendo in tal modo al corretto funzionamento del mercato interno»[19].

In particolar modo l'organo si impegna ad assistere la Commissione e gli Stati membri nella diffusione di una cultura cibernetica e nello sviluppo coordinato di adeguati strumenti di prevenzione e reazioni agli attacchi esterni, ponendo la creazione di *best practices* come punto focale rivolto a sostenere non solo la salvaguardia della sicurezza nella materia ma anche la denuncia di tali fattispecie criminose nel solco di un'armonizzazione comune, come ulteriormente ribadito nel 2006 da due comunicazioni della Commissione europea, in modo da combattere non solo l'ignoranza generale sulla questione ma anche il numero sommerso di reati che spesso non vengono denunciati per paura di ritorsioni di carattere economico.

Da ricordare, essendo comunque un punto focale della materia in ambito europeo, l'istituzione dello *European Cybercrime Center* (EC3) presso l'Europol[20] a partire dal 2010 per assistere i singoli cittadini ma anche le imprese e gli Stati nella comune prevenzione e repressione dei reati informatici (in particolar modo attraverso un sistema di *information sharing* e di allarme); tale organismo si è ulteriormente allargato nel corso degli anni risultando un strumento sempre più proficuo per la lotta al crimine online.

[19] Come si può leggere all'interno del Regolamento UE 526/2013 relativo all'ENISA, in abrogazione del regolamento CE 460\2004, punto 9.

[20] "Europol è l'agenzia dell'Unione europea incaricata dell'applicazione della legge, il cui obiettivo principale è quello di contribuire a realizzare un'Europa più sicura a beneficio di tutti i cittadini." Vedi "Europol" su www.europol.europa.eu/it/about-europol.

Egualmente importante in questa specifica materia è stata la Decisione Quadro 2005/222/GAI[21] del Consiglio che ha ampliato il *range* dei *cybercrimes* introducendo nuove fattispecie e tecniche comuni di prevenzione e cooperazione giudiziaria ma che va direttamente ad influenzare – come vedremo successivamente – l'inquadramento dei *dual use software* e che è stata sostituita da una nuova direttiva nel 2013 riguardante gli attacchi contro i sistemi di informazione[22].

Il cammino europeo è, in generale, maturato in questi anni continuando a scavare nel solco già precedentemente creato e che è stato sempre più ampliato. Nel 2013, sempre nell'ambito di una serie di riforme nella materia, si è istituito anche il "*Computer Emergency Response Team of the European Union*" (CERT EU, anche denominato CSIRT che è l'acronimo di "*Computer Security Incident Response Team*") che ha visto e vedrà sempre una maggiore acquisizione di poteri per via delle strategie adottate dall'Unione ai fini della sicurezza: è ormai avvenuta la comprensione che un ambiente *online* sicuro non solo permette la piena creazione della propria personalità ma porta sempre nuovi investitori, aumentando la competitività delle aziende che operano in Europa rispetto al resto del mondo.

Non è un caso che dopo queste riforme l'EDA (Agenzia Europea di Difesa) abbia inserito tra le sue priorità quelle di supportare gli Stati membri nello sviluppo di capacità di *cyber defence* relative alla *Common Security and Defence Policy*, incrementare la protezione dei *network* di comunicazione utilizzati dalle istituzioni europee, promuovere la cooperazione civile e militare con le *cyber policy*, le istituzioni e le agenzie europee, e con il settore privato e incentivare la cooperazione con partner internazionali di rilievo. Combattere la diffidenza dei singoli utenti così come promuovere una maggiore automazione e sicurezza dei singoli operatori informatici o telematici sono ad oggi punti fondamentali della nuova disciplina della *Cybersecurity*.

[21] Decisione quadro del Consiglio europeo relativa agli attacchi contro i sistemi di informazione oggi sostituita.

[22] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.

Tutte queste pressioni hanno naturalmente condotto a tre importanti risultati costituiti da una direttiva e da due regolamenti.

Il primo, in breve, è il GDPR (Regolamento Generale sulla Protezione dei Dati)[23], mentre la seconda è la direttiva NIS[24] che ha il fine ultimo di garantire un livello comune di *cyber*sicurezza in tutta l'Unione.

Il passo conclusivo e più recente nella materia è il regolamento denominato "*Cybersecurity* Act"[25]: quest'ultimo costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica mirante a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali. Tale strumento si affianca – ed è in certi suoi aspetti complementare – alla precedente Direttiva NIS. Il Regolamento si compone di due parti: nella prima vengono specificati il ruolo e il mandato dell'ENISA, i cui poteri vengono ulteriormente ampliati, mentre nella seconda viene introdotto un sistema europeo per la certificazione della sicurezza informatica dei dispositivi connessi ad Internet e di altri prodotti e servizi digitali.

In generale, in ambito europeo, è sempre più chiaro che il corretto sviluppo delle nuove tecnologie dell'informazione e della comunicazione deve passare attraverso tre gradini: il potenziamento della capacità dei singoli Stati membri di dotarsi di appositi strumenti di *cybersecurity*, il rafforzamento ed ampliamento delle modalità di cooperazione transnazionale, l'introduzione di efficienti metodi di gestione del *cyber risk* ed obblighi di notificazione all'autorità di competenza riguardo gli incidenti informatici di maggior rilievo.

1.4.2 Livello nazionale

[23] Regolamento Generale sulla Protezione dei Dati (RGPD, GDPR in inglese), ufficialmente Regolamento (UE) n. 2016/679.

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

[25] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersecurity, e alla certificazione della cybersecurity per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cybersecurity").

In ambito nazionale la repressione dei reati informatici avveniva in origine con l'applicazione analogica di determinate fattispecie di reato già esistenti. Basti pensare alla possibilità di utilizzare il delitto di truffa nelle sue diverse sfaccettature o quello di furto, per non parlare poi della violazione di domicilio. Tutte fattispecie che non erano state create né tantomeno pensate per reati commessi a mezzo internet e che dunque soffrivano delle ovvie mancanze derivate dalla loro forzosa applicazione a simili condotte.

A ben vedere, l'Italia si dotò di una propria specifica disciplina in anticipo rispetto al restante panorama europeo ed internazionale: con la legge 23 dicembre 1993 n. 547 il legislatore introdusse per la prima volta nuove fattispecie specifiche per la materia all'interno del nostro Codice penale.

Dopo questo primo e virtuosistico sforzo, però, l'interesse nazionale per la questione crebbe di pari passo con quello europeo, tant'è che tutte le successive modifiche ed integrazioni legislative sono il risultato di recepimento di direttive, atti o armonizzazioni comunitarie.

Per rendersene conto sarà sufficiente iniziare proprio con la direttiva del 2002 che recitava: «le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese. Questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse. È noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio. Lo stesso processo di innovazione tecnologica produce da un lato strumenti più sofisticati di "attacco", ma d'altro lato idonei strumenti di difesa e protezione. Assume, quindi, importanza fondamentale valutare il rischio connesso con la gestione delle informazioni e dei sistemi»[26].

Per la prima volta il legislatore aprì gli occhi sulla necessità di dotarsi di un sistema capace di tutelare in particolar modo gli interessi della pubblica amministrazione e contrastare che le informazioni o i dati in suo possesso potessero essere carpiti illecitamente da soggetti esterni alla stessa o non autorizzati.

[26] Direttiva 16 gennaio 2002 riguardante la "sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni" su www.gazzettaufficiale.it/eli/id/2002/03/22/02A03219/sg.

Il 2003 ha visto anche la nascita di due nuove entità sul panorama nazionale: l'Osservatorio permanente per la sicurezza e la tutela delle reti e delle telecomunicazioni, a cui partecipano i rappresentanti di diversi ministeri con il compito di predisporre iniziative legislative in ambito di sicurezza informatica, oltre che numerosi altri compiti tra cui soprattutto di carattere consultivo e di collaborazione a livello internazionale ed europeo, nonché l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM), istituito con legge 111/1907 al fine di garantire l'evoluzione delle tecnologie nel panorama della sicurezza informatica e delle telecomunicazioni (oltre che collaborare con l'ENISA in una serie di esercitazioni mirate ad aumentare la collaborazione tra settore pubblico e privato contro gli attacchi informatici).

Sempre nel 2003 viene emanato il Codice in materia di tutela dei dati personali ed il primo Codice delle comunicazioni elettroniche che si pone nel solco di non porre limiti alla libera iniziativa economica che non siano quelli derivanti da esigenze di natura pubblica quali tutela della *privacy*, dell'ambiente, della sicurezza e della difesa pubblica.

Attraverso quest'ultimo codice vengono anche recepite le indicazioni di una direttiva europea del 2002, dando vita ad una Autorità Nazionale di Regolamentazione (ANR) e ad un CERT domestico.

Gli anni successivi vedono un momento di fibrillazione tra la pubblicazione di studi dedicati al potenziamento dei sistemi di prevenzione, passando per l'emanazione del Codice dell'amministrazione digitale nel 2005 – che ha permesso, tra le altre cose, la comunicazione digitale tra PA e cittadini – e, non per ultima, la legge Pisanu[27] in materia di contrasto al terrorismo che per prima attribuisce al Ministero dell'Interno e alla Polizia Postale compiti di contrasto alla commissione di simili fattispecie di reato a mezzo internet.

Si dovrà però attendere il decreto legislativo n. 61 del 2011 per vedere finalmente recepita in Italia la direttiva 2008\114\CE e con esso il delineamento delle infrastrutture critiche definite come gli enti "in uno stato membro dell'Unione europea, che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della

[27] Legge 31 luglio 2005, n.155, Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n.144, recante misure urgenti per il contrasto del terrorismo internazionale.

popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello stato, a causa dell'impossibilità di mantenere tali funzioni"[28].

Eppure, il passo più importante del nostro Stato in materia di *Cybercrime* resta ancora oggi la ratifica della Convenzione di Budapest[29] avvenuta nel 2008 e che ancora oggi resta la stella polare per tutti i reati informatici, continuamente aggiornati tramite l'opera di numerose fondazioni, istituti o commissioni (quali il CoPS ed il NISP).

La grande attenzione che in questi ultimi anni scosse il nostro Paese, unito all'insieme di ricerche ed analisi svolte e sopra accennate, portò all'istituzione di un Comitato Interministeriale presso la Presidenza del Consiglio adibito alla progettazione di una strategia nazionale per la sicurezza informatica e il recepimento di direttive europee in materia di protezione dei dati tra il 2011 ed il 2012, oltre che alla nascita proprio nel 2012 dell'Agenzia per l'Italia Digitale (AgID) con l'unico obiettivo comune di diffondere la cultura digitale e l'innovazione tecnologica in tutto il territorio nazionale, promuovere la collaborazione tra gli amministratori statali, regionali e locali guidandone la coordinazione, elaborare linee guida e diffondere *standard* operativi rivolti alla riduzione dei costi nel garantire l'uniformità e l'efficienza dei servizi informatici offerti.

Questi sforzi comuni hanno portato, alla fine, alla maturazione e alla promulgazione del DPCM[30] recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, con il compito di definire i concetti di *cybersecurity*[31], *cyber space*[32], *cyber*[33] e *cyber threat*[34].

---

[28] Come si può leggere in D.lgs. 11 aprile 2011, n. 61 in attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione.

[29] Convenzione di Budapest del 23 novembre 2001 del Consiglio d'Europa sulla criminalità informatica.

[30] Decreto del Presidente del Consiglio dei ministri 24 gennaio 2013 che adotta la Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

[31] "Ramo dell'informatica che si occupa di tutelare i sistemi di elaborazione, siano essi reti complesse o singoli computer, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti. Tali tentativi di violazione possono essere contrastati sia mediante programmi sia mediante specifici strumenti hardware". Vedi "*Cyber security*", in *Enc. onl. Treccani*, su www.treccani.it/enciclopedia/sicurezza-informatica/.

[32] "Lo spazio virtuale nel quale utenti (e programmi) connessi fra loro attraverso una rete telematica (v., per es., internet) possono muoversi e interagire per gli scopi più diversi, come, per

In generale tale provvedimento contiene indicazioni riguardo ai soggetti predisposti e alle modalità con cui delineare le strutture critiche a livello nazionale ed i futuri quadri strategici per la sicurezza dello spazio cibernetico.

Proprio questi quadri acquistano un'importanza non secondaria, divisibili al loro interno in due diversi aspetti: la prima parte si limita a sottolineare le minacce a livello tecnologico e i rischi connessi a determinate attività con l'indicazione di vulnerabilità che potrebbero mettere a rischio i sistemi telematici o informatici; nella seconda parte, invece, il documento procede ad indicare come risolvere queste criticità e quali debbano essere gli operatori incaricati di aumentare la capacità nazionale di garantire una sicurezza cibernetica ed informatica, non solo per minimizzare i rischi ma anche per diminuire eventuali danni attraverso la concreta attuazione e potenziamento di un CERT a livello nazionale.

Nel 2014 la Relazione sulla politica dell'informazione per la sicurezza dal Sistema di informazione per la sicurezza della Repubblica mette in luce l'aumento dei reati informatici (connessi, probabilmente, ad un maggior numero di reati informatici denunciati oltre che ad un'incrementata capacità da parte di singoli ed aziende di rendersi conto della loro eventuali effettuazione) e l'impatto positivo che la collaborazione tra pubblico e privato in questo campo stava apportando alla materia con la conferma dell'istituzione di un Tavolo tecnico di valutazione dell'esecuzione delle linee strategiche e di una Unità di allerta in situazioni critiche.

Tutto questo ha spianato la strada al nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, pubblicato in Gazzetta Ufficiale il 31 maggio 2017 e conosciuto come DPCM del 17 febbraio 2017[35]. Quest'ultimo non si pone come mero aggiornamento del precedente piano ma si inserisce nell'ambito nazionale come evoluzione e allo stesso tempo continuazione sotto la s*pin*ta di una nuova revisione fatta dal Presidente del Consiglio dei ministri,

---

es., la consultazione di archivî e banche dati o lo scambio di posta elettronica". Vedi "*Cyber space*", in *Enc. onl. Treccani*, su www.treccani.it/vocabolario/ciberspazio/.

[33] "Primo elemento di parole composte della terminologia informatica angloamer., tratta dall'agg. cybernetic «cibernetico», che alla cibernetica appunto fa riferimento". Vedi "*Cyber*", in *Enc. onl. Treccani*, su www.treccani.it/vocabolario/cyber/.

[34] L'insieme dei mezzi e delle tecnologie rivolti alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici.

[35] Anche conosciuto come "decreto Gentiloni", rappresenta una direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali.

coadiuvato da diversi esperti del settore e delle organizzazioni nate nel corso del tempo.

Per far ciò il piano si prefigge la suddivisione della messa in sicurezza su tre distinti livelli: quello nazionale, quello delle infrastrutture critiche e quello dei cittadini e dei servizi. L'obiettivo è non solo quello di semplificare la disciplina ma anche renderla più rispondente alla realtà fattuale, potenziando contemporaneamente la velocità di risposta ad eventuali crisi da parte degli istituti preposti con una maggiore collaborazione sia a livello nazionale che internazionale e, in particolar modo, europeo.

Tutto questo viene perseguito attraverso l'istituzione di diversi "*response and remediation*" studiati in campo accademico e scientifico ma anche dal punto di vista degli organi pubblici che ricoprono funzioni in materia di *cybersecurity*. Basandosi su queste premesse il DPCM Gentiloni prosegue alla esplicazione di undici punti cardine attraverso i quali si ritiene debba continuare il cammino d'evoluzione nazionale in ambito informatico e telematico. In questa sede, interessano specificatamente il settimo e l'ottavo indirizzo che riguardano, rispettivamente, "*Compliance* a *standard* e protocolli di sicurezza" (soprattutto per il perfezionamento dei metodi certificativi e di valutazione dei procedimenti di messa in sicurezza dei sistemi oltre che per la periodica e *standard*izzata realizzazione di test di verifica basati su parametri applicati in modo comune ed imparziale) e "Supporto allo sviluppo industriale e tecnologico" (mirante all'implementazione di sempre nuove tecnologie in campo ICT[36], sia per promuovere la ricerca già esistente che per la creazione di nuovi sistemi).

Questo piano, in conclusione, mostra il crescente interesse che sia sul piano nazionale sia internazionale si presta alla prevenzione degli incidenti che al "*response and remediation*"[37].

Il tempo, ci mostrerà i nuovi equilibri che si andranno a creare nel nostro ordinamento a seguito dell'introduzione del Regolamento "*Cybersecurity act*" emanato nel 2019[38].

---

[36] "Sigla dell'ingl. *Information and comunication technology* ("Tecnologia dell'informazione e della comunicazione"), usata per indicare il settore dell'informatica e delle telecomunicazioni." Voce "ICT", in Enc. onl. Treccani, su http://www.treccani.it/enciclopedia/ict/.

[37] Meccanismi per la reazione ad un attacco informatico ed il contenimento degli eventuali danni cagionati dallo stesso.

1.5 Condotte lesive e *focus* introduttivo sul tema

Nell'ambito di un mondo digitale inteso, come si è visto, in maniera sempre più importante e come spazio fondamentale per la realizzazione e l'esplicazione della personalità degli individui, oltre che per le attività economiche di enti e persone fisiche, è comprensibile come le condotte lesive che possono osservarsi sono delle più variegate e lo sono in particolar comodo quelle connesse all'utilizzo di programmi informatici che diventano più complessi man mano che si evolve la tecnologia.

In origine, le fattispecie che utilizzavano questi programmi informatici erano soprattutto annoverate tra quelle di truffa o di "violazione di domicilio" inteso in senso virtuale, tuttavia ad oggi si assiste alla proliferazione di *malware* e *software* che si inseriscono come strumenti all'interno di condotte sempre più variegate a sostegno dei più disparati disegni criminali normalmente legati al raggiungimento di un guadagno personale, spesso rappresentato dal danneggiamento di un *hardware* o dall'acquisizione di dati ed informazioni personali connessi a crimini di matrice sessuale.

Durante questa trattazione verranno considerati e sviluppati in particolar modo solo gli aspetti più strettamente connessi all'uso dei "*dual use software*"[39] che vanno a ricadere soprattutto nella disciplina legata all'accesso abusivo e al danneggiamento informatico.

Prima di concentrarsi su tali fattispecie, si ritiene opportuno soffermarsi preliminarmente sul concetto di "accesso abusivo" e di "danneggiamento informatico" così da avere una visione generale di alcuni temi ricorrenti nella presente trattazione.

1.5.1 Cos'è un accesso abusivo

[38] Vedi "*supra*", capitolo I, paragrafo 1.4.1, per una maggiore spiegazione sul contenuto del Regolamento citato.

[39] Per definizione vedere *infra*, capitolo III, § 3.1.

Il disvalore contenuto negli articoli 615-*ter* e successivi del Codice penale era, nella prospettiva del legislatore del 1993[40], quello di accedere abusivamente ad un sistema informatico o telematico a cui protezione fossero state poste delle misure di sicurezza (*password, firewall* ecc.) la cui violazione sarebbe coincisa con quella del comune delitto di violazione di domicilio (articolo 614 c.p.).

Con il concetto di accesso abusivo, però, non si deve ricadere nella trappola presentata dallo stesso legislatore che nella non corretta rappresentazione del delitto si accostò eccessivamente alla fattispecie della violazione di domicilio[41]: "introdursi" in una villa è ben differente rispetto ad "accedere" ad un *personal computer*. Con l'ultima azione non si ritiene di dover incriminare qualsiasi condotta che vede un soggetto avvicinarsi ad un *hardware* e poggiare le mani sulla sua tastiera quanto quello di impartire degli ordini ad un sistema informatico altrui così da fargli svolgere determinate operazioni che lo mettono in condizione di conoscere quanto in esso contenuto o di poter operare attraverso lo stesso anche da remoto. Come tale è assolutamente irrilevante ai fini dell'accesso abusivo l'effettiva conoscibilità delle informazioni memorizzate nel sistema violato. È sufficiente che il soggetto attivo abbia instaurato un dialogo logico che gli permetta di utilizzare, totalmente o meno, le risorse del computer altrui o di potersi muovere all'interno di determinati spazi in esso contenuti (il fallimento di tale azione comporta il mero tentativo) e ciò può essere fatto sia manualmente (come gli *hacker* di un tempo) sia attraverso l'uso di appositi *spyware* (tali come il *Trojan horse* o il *Keylogger*) in modo da "infestare" – impossibile trovare termine migliore – la macchina altrui[42].

La condotta di accesso abusivo serba nel suo cuore, però, un pericolo ben maggiore ed un disvalore che nessuna violazione di domicilio potrà mai equiparare: la possibilità che il proprietario del sistema non venga mai a

[40] Legge 23 dicembre 1993, n. 547 recante modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

[41] Sulla questione si pronunciò già ai tempi PAZIENZA F., *In tema di criminalità informatica: l'art. 4 della legge 23.12.1993, n. 547*, in *Riv. it. dir. e proc. pen*., 1995, 750 ss., 755. Tale scelta del termine "introdursi", però, non deve lasciare stupiti poiché sebbene non completamente corretto appariva ai legislatori del tempo come il modo più sicuro di accostare la disciplina a quella del delitto di violazione di domicilio (e che viene ritrovata anche, per esempio, nelle leggi di molti Stati americani).

[42] Cfr. Cass. pen., sez. V, sent. 8.7.2008, n. 37322; Cass. pen., sez. I, 27.9.2013, n. 40303.

conoscenza di questa intrusione tanto da permettere al soggetto attivo l'illecita permanenza all'interno del computer contro la "*voluntas domini*".

Inoltre, ad essere punito non è solamente l'accesso ma anche la semplice "sosta" abusiva, quando colui che si sia introdotto non stia più operando direttamente sul sistema andando a ricomprendere anche la condotta del tecnico informatico che una volta ricevuta l'autorizzazione ad inserirsi in un sistema informatico (come durante un "*penetration test*") successivamente non esca ma ci permanga consapevolmente con tutti i rischi che potrebbero derivare da una simile condotta[43]. Chiaramente, ancora una volta, il rimanere all'interno del sistema non deve essere inteso in chiave fisica bensì come il mantenimento della connessione logica con l'elaboratore, indipendentemente dal proprio ‹‹continuare ad accedere alla conoscenza dei dati, nonostante l'intervenuto divieto del soggetto»[44], come vorrebbe parte minoritaria della dottrina.

È interessante notare come nel nostro ordinamento questa fattispecie sia punita più gravemente, abbracciando anche un novero più ampio di condotte, rispetto a quelle di altri ordinamenti europei come quello tedesco o austriaco: obiettivo principale di queste forme di tutela resta, come si è detto all'inizio dell'esposizione, garantire la possibilità di esprimere sé stessi all'interno di un sistema informatico o telematico e ciò passa direttamente attraverso la certezza che un utente ha riguardo la sicurezza del proprio apparecchio elettronico.

Come accesso abusivo, non si intende dunque l'accesso e l'effettiva apprensione del contenuto di un sistema, quanto la mera instaurazione o permanenza non autorizzata di una connessione logica. Ciò può avvenire secondo diverse modalità compreso anche l'utilizzo di un *dual use software* la cui funzione, anzi, è spesso quella di effettuare "*penetration test"* il cui obiettivo è proprio quello di cercare di introdursi forzosamente all'interno di un sistema[45].

---

[43] Tra i molti si sono espressi a sostegno di questa visione PECORELLA C., *Il diritto penale dell'informatica*, cit., 351 e PICA G., *Diritto penale*, cit., 42

[44] Cfr. MANTOVANI F., *Diritto penale, PS*, I, cit., 576; ma si può leggere negli stessi termini anche in BORRUSO R., *La tutela del documento e dei dati*, ed in BUONOMO G.-CORASANITI G.-D'AIETTI G. (a cura di), *Profili penali dell'informatica*, cit., 32 ed anche in MAZZACUVA N., *Delitti contro la persona*, cit., 659. La stessa giurisprudenza si è espressa più volte a sostegno come in Cass. pen., sez. V, 7.11.2000, in *Cass. pen*., 2002, 1015 nonché in Cass. pen., sez. V, 31.10.2014, in CED, n. 263454.

[45] Nell'ultimo capitolo si affronterà l'argomento e si chiarirà perché una simile condotta rientri all'interno della fattispecie appena descritta.

1.5.2 Cos'è un danneggiamento informatico

Il concetto di danneggiamento informatico è contenuto, invece, all'interno dell'articolo 635-*bis* c.p. e va a punire la condotta di chi causa la "distruzione, deterioramento, cancellazione, alterazione o soppressione" di un *hardware*, dei *software* in esso contenuti o delle informazioni conservate.

Ci troviamo dunque dinnanzi ad una fattispecie che non solo vede diverse modalità di condotta piuttosto variegate ma che si estende a diversi oggetti che possono essere la scocca esterna del computer nonché la sua natura fisica (il c.d. "*hardware*") ma anche "l'anima" che permette ad un sistema informatico o telematico di funzionare, quindi tutto quell'insieme di programmi (chiamati "*software*") che guidano l'agire del computer. All'interno di questi aspetti si inseriscono anche le informazioni o i dati che possono essere conservati all'interno del computer stesso.

Le condotte descritte sono tutte rivolte a rendere illecita la condotta di chi con il proprio agire, diretto o indiretto, impedisce l'utilizzo di un sistema informatico o telematico. Il grande quantitativo di azioni elencate vuole proprio essere esemplificativo ed il più ampio possibile in modo da abbracciare tutto un insieme di fattispecie considerate più gravi: il concetto di danneggiamento informatico, infatti, è non solo ripreso come circostanza aggravante nell'articolo 615-*ter* ma anche come autonoma fattispecie di reato negli articoli 615-*quinquies* e 617-*quater* del Codice penale.

In questo caso l'agire del soggetto attivo è considerato più grave perché non solo si sta turbando il normale utilizzo del *computer* da parte del suo proprietario ma ci si sta intromettendo in maniera diretta (con la penetrazione all'interno del sistema o approfittando nel trovarlo incustodito per cancellare dei documenti) o indirettamente (tramite l'inoculazione di un malware, cosa sempre più facile e frequente) per danneggiarne anche il sistema o parti di esso Esattamente, come si era in precedenza visto per l'accesso abusivo, l'oggetto giuridico del reato è l'inviolabilità del possesso e della disponibilità delle cose oggetto materiale della condotta, quindi ci si riferisce all'integrità fisica delle apparecchiature e delle

istruzioni di funzionamento incise su taluni dei loro componenti. Non è, dunque, necessario che si verifichi un danno economico o patrimoniale, bensì è sufficiente che la propria azione abbia sortito un effetto negativo o deteriore.

Non viene operata alcuna distinzione tra un'azione effettuata sull'*hardware* (prendere una mazza da baseball e colpire ripetutamente un computer portatile), un *software* (il *trojan virus* contratto in rete impedisce l'utilizzo di strumenti *microsoft*) o dati ed informazioni (per sbaglio un collega ha cancellato importanti testi di lavoro o, volontariamente, un *hacker* infiltratosi nella sua posta gli ha sottratto e poi cancellato determinate *e-mail* commerciali o personali).

Il particolare carattere di questa fattispecie di reato è stato sottolineato da una sentenza della Corte di Cassazione[46] che ha considerato il delitto esistente anche se sia stato poi possibile recuperare il materiale precedentemente danneggiato (in questo caso alcuni *files*), perché ancora una volta la tutela non va a colpire il danno materiale subito dal sistema vero e proprio, quanto la più gravosa condizione in cui si viene a trovare l'interessato che quel sistema informatico o telematico lo utilizza non solo per lavorare ma anche per esprimere le proprie passioni o veicolare la propria personalità.

L'unica differenza voluta dal legislatore , sulla quale si tornerà comunque in seguito, riguarda la modalità con cui il danneggiamento viene procurato: se mediante la diretta esecuzione delle condotte contenute nell'articolo 635-*bis* c.p. ovvero se gli stessi risultati vengono perseguiti indirettamente attraverso l'introduzione o la trasmissione di dati, informazioni o programmi con i quali distrugge, danneggia, rende, in tutto in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento (come indicato negli articoli 635-*quater* e 635-*quinquies* del Codice penale)[47].

Ovviamente nell'illegittimità della condotta bisogna considerare l'altruità dei dati danneggiati così come dell'*hardware* o del *software*.

Per quanto riguarda i primi si fa riferimento alla figura dell'"interessato" che viene espressamente presentato quale "titolare" o "responsabile del trattamento"[48].

---

[46] Vedi Cass. pen., sez. V. 5.4.2012 n. 8555.

[47] A seguito della riforma del D.lgs. 15 gennaio 2016, n.7.

[48] Precisamente nell'4 del D.lgs. 196/2003.

Nel caso di danneggiamenti di programmi o *hardware*, invece, le persone offese possono essere il concessionario, il legittimo utilizzatore, il concedente, i partner, il proprietario e così via.

Il danneggiamento, allo stesso tempo, può essere totale o parziale senza che ciò possa in un qualche modo escludere l'eventuale applicazione dell'articolo 635-*bis* e successivi.

Andando al cuore della presente trattazione, viene in rilievo il "*dual use software*" il quale consiste spesso in un programma che può essere utilizzato anche per commettere un danneggiamento informatico ma, come per l'accesso abusivo, si analizzeranno le ragioni che portano a escludere il suo utilizzo dal novero delle fattispecie che integrano questa tipologia di reato[49].

1.6 Forme di tutela

Per concludere questo capitolo si deve tornare al punto da cui è tutto cominciato, dunque denotando la quantità di beni giuridici che possono essere lesi tramite l'utilizzo di internet al giorno d'oggi: si va dai beni tradizionali quali possono essere il patrimonio, l'onore, la propria identità sessuale ecc., fino ad arrivare a nuovi interessi comunque meritevoli di tutela quali la riservatezza informatica, l'integrità e la disponibilità di uno spazio in cui poter coltivare la propria personalità[50].

Non c'è da stupirsi se, quindi, nel corso degli ultimi anni le diverse normative hanno ampliato il novero dei reati informatici che vanno da quelli che possono essere commessi da chiunque abbia una benché minima conoscenza e l'accesso ad un sistema informatico o telematico (quali la pubblicazione di un messaggio

[49] E per le quali si rimanda anche alla trattazione di SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "*dual-use software*"*, in *Rivista italiana di diritto e procedura penale*, ISSN 0557-1391, Vol. 60, N. 2, 2017, pag. 747-788.

[50] Leggasi al riguardo ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, 12 s. Invece, per quanto riguarda la sempre maggiore importanza di queste tematiche nella società di oggi si rimanda già PICOTTI L, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 ss., 70 ss.; più di recente SALVADORI I., *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 125 ss., 149 ss.

offensivo o diffamatorio su una determinata persona nella propria pagina *Facebook* fino all'adescamento di minorenni in chat pubbliche o private passando per l'estorsione di denaro in cambio della non pubblicazione di determinate foto pornografiche) fino ad arrivare a una serie di delitti che richiedono, invece, una conoscenza maggiorata e specialistica (tipica degli *hacker* e dei cracker). È chiaro, infatti, come le fattispecie di accesso abusivo e quella di danneggiamento informatico si basino solitamente sulla volontà – e le capacità – di poter penetrare in un determinato sistema protetto da difese e, anzi, l'articolo 615-*ter* del Codice penale espressamente richiede che il sistema informatico o telematico sia protetto da "misure di sicurezza" che possono variare da una *password* fino ad un sistema di chiavi d'accesso e così via.

Tutto ciò apre la strada a quella categoria di reati informatici in "senso stretto" che si manifestano come la fraudolenta intercettazione di informazioni a mezzo internet (*data-espionage*), la commissione di truffe mediante *e-mail* (*scam*), tecniche di ingegneria sociale (insieme molto ampio ricomprendente il *phishing* ma anche lo *smishing* o il *pharming* ecc.), l'attacco ai *server* di imprese o di istituzioni pubbliche attraverso la creazioni di reti *Botnet* (DoS o DDS *attack* ecc.).

Questi reati informatici non solo, però, richiedono più elevate conoscenze sul campo, ma anche l'accesso ad una serie di *software* (che possono essere creati dallo stesso *hacker* o comprati nel *Deep-web*) che rendano possibile superare le misure di sicurezza che sono state imposte a protezione di sistemi informatici o telematici: tali *software* prendono solitamente il nome di "*malware*"[51].

Negli anfratti più scuri di internet, il *Dark-web*, è spesso molto facile acquisire *malware* per ogni possibile necessità criminosa o illecita ed anzi questo è un mercato assolutamente fiorente: un *hacker* capace di creare un determinato *software* malevolo facilmente lo metterà in vendita e lo consegnerà al miglior offerente, anche solo temporaneamente[52]. Comportamento comune, infatti, è quello di dare in affitto tali programmi che vengono utilizzati solitamente per

[51] La definizione qui utilizzata è particolarmente ampia ed in generale ricomprende tutti i software che possono essere utilizzati con fini illeciti.

[52] Al riguardo si è costretti a rimandare soprattutto a dottrina straniera quale LACSON W.-JONES B., *The 21st Century DarkNet Market: Les-sons from the Fall of Silk Road*, in *IJCC*, vol. 10, Issue 1, 2016, 40 ss.

poche ore ma che, a seconda della loro funzione e complessità, possono anche causare numerosi danni come accade con gli "*spam-toolkits*" che sono capaci di inviare migliaia e migliaia di *e-mail* in pochi minuti.

Alcune volte sono gli stessi Stati che si armano di vere e proprie compagnie di *hacker* all'alba di una guerra in cui l'acquisizione di informazioni secretate diventa spesso più importante dei rapporti diplomatici (*cyber warfare* e *cyber-espionage*)[53].

Logica legge di mercato dice che più la domanda è alta più l'offerta tenderà a soddisfarla ed anche questa parte di commercio non può sottrarsi a questa massima sempre vera: ad oggi i *cybercrime* si stanno diffondendo anche a causa del sempre crescente numero di persone che acquistano o creano *malware* capaci di commettere reati informatici tendenti agli scopi più variegati. È a questo punto che, come in qualsiasi guerra, le imprese e gli Stati si sono armati a propria volta proprio per contrastare questi continui e crescenti attacchi.

Nella disciplina sopra indicata, infatti, è ormai appurato come una corretta attività d'impresa debba passare anche attraverso la valutazione del rischio di successo di un attacco informatico così da poter comprendere quali siano i settori a rischio e proteggerli con la creazione di "*fire-wall*" o percorsi differenti. Ma come si scoprono queste "debolezze" di sistema?

Nella stragrande maggioranza dei casi attraverso l'esecuzione di *penetration test* il cui obiettivo è l'innalzamento delle capacità difensive di un sistema. Per effettuare questi *penetration test* è necessario, però, utilizzare proprio uno di quei *software* malevoli (di solito, oltretutto, di ultima generazione) così da testare le capacità di un sistema di rilevare e sconfiggere una minaccia. Fu nella paura generale scaturita dalla diffusione dei *cyber criminals* che gli organismi internazionali hanno suggerito agli Stati di adottare una disciplina sanzionatoria ad ampio spettro che andasse a colpire indistintamente tutti coloro che fabbricassero *malware* indipendentemente dall'elemento soggettivo. Così facendo si sono andati a danneggiare, però, sia coloro che producevano *malware* a scopo illecito che le

[53] Anche in questo caso la dottrina che finora si è occupata della materia è soprattutto di matrice straniera e ad essa si rimanda per maggiori informazioni, v. ROSCINI M., *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; ed in specie SCHMITT M.N., (ed.), *Tallinn Manual on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, 2017.

stesse aziende che, invece, lo facevano per vendere poi il prodotto alle imprese per lo svolgimento dei *penetration test*.

Il problema è che una simile legislazione va a ripercuotersi gravemente sui creatori di *malware*, benevoli, che agiscono alla luce del sole ma non possono invece colpire le persone che operano all'ombra del Deep-web e che, per definizione, sfuggono alle maglie della legge.

Le ragioni motrici di una simile decisione sono da rinvenirsi nel fatto che, comunque, il *software* resti malevolo e che possa essere usato anche per scopi illeciti se entrasse in possesso della persona sbagliata, tuttavia ciò può accadere rispetto a qualsiasi "arma", ravvicinando in un certo senso la casa produttrice di un *malware* ad un'azienda che produce pistole.

Vista l'originaria vastità di queste fattispecie la dottrina tedesca andò a coniare un apposito termine (*software-Delikte*[54]) che per sua stessa natura è troppo vasto e troppo impreciso.

Nel corso degli anni, quindi, la necessità di una tutela si è unita anche ad una più intelligente capacità definitoria che ha smussato sempre più gli angoli di una disciplina in origine quasi controproducente. Sono così apparsi, nel nostro ordinamento, riferimenti al "diritto penale dei *software*" sia nella parte speciale del Codice penale che nella legislazione complementare: come le discipline che puniscono l'utilizzo di *software* malevoli destinati ad accedere abusivamente ad un sistema informatico o telematico che sia stato protetto da misure di sicurezza o ad intercettare o ostacolare illecitamente comunicazioni elettroniche o a violare le misure di protezione disposte a tutela di opere sotto *copyright* ecc.

Obiettivo di qualsiasi difesa fin dai tempi degli *offendicula* posti a tutela di una proprietà privata è quella di impedire o rendere più complesso l'accesso o il danneggiamento di un proprio avere ed anche tale normativa non fa esclusione: si

[54] Utilizzata per la prima volta nella dottrina germanica da POPP A., *§ 202c StGB und der neue Typus des europäischen "Software-Delikts"*, in *GA*, 2008, 375 ss., come commento della norma introdotta all'interno del codice penale tedesco con il 41. StrÄndG del 7 agosto 2007, che sanziona gli atti preparatori all'accesso e all'intercettazione di dati informatici (*«Vorbereiten des Ausspähens und Abfangens von Daten»*) di cui al *§ 202c D-StGB*

cerca, così, di punire la commissione di comportamenti prodromici o preparatori alla commissione di più gravi reati a danno dei beni giuridici tutelati[55].

Data la difficoltà non solo di rilevare ma anche di punire i reati informatici una volta commessi, si è adottata la strategia inversa, quella di cercare di impedire o prevenire la commissione di quegli stessi reati informatici socialmente dannosi o offensivi di determinati interessi giuridici.

Il legislatore, però, si trova davanti a numerose nuove sfide di non facile risoluzione: una disciplina sanzionatoria troppo ampia, infatti, va a colpire anche tutto quell'insieme di aziende che creano *malware* a scopo di rivenderli alle imprese per ragioni positive, ma allo stesso tempo il frazionamento dell'*iter criminis* in questo specifico ambito penale rende estremamente complessa la repressione di tali fattispecie delittuose. Da una parte, infatti, abbiamo colui o coloro che fanno uso del *malware* e dall'altra – di ancor più difficile rilevamento – vi sono coloro che tale *malware* lo creano e che poi lo mettono a disposizione in un ambiente (il *Dark-web*) dove mantenere l'anonimato è molto facile se non alcune volte richiesto[56].

Per cercare di reprimere i *cybercrime* e fornire protezione alle persone che si muovono nello spazio virtuale di internet, dunque, il legislatore ha rinunciato al tradizionale paradigma del reato d'evento ma ha anche superato i normali limiti imposti solitamente al tentativo e al concorso di persone nel reato per cercare di punire tutte quelle condotte illecite che vengono solitamente commesse in rete.

Se l'obiettivo è positivo, però, diverse critiche possono essere sollevate proprio sulle modalità con cui si prova a perseguirlo: solitamente incuneate nella scarsa capacità del legislatore di distinguere tra *software* creati e messi a disposizione per scopi illeciti e, magari, gli stessi identici *software* ma senza il loro scopo malevolo. Certo, questa distinzione è facile quando si vanno a guardare tutti quei *malware* (*trojan horse*, virus, *spyware*, *hacking tools*, ecc.) che colpiscono direttamente beni giuridici classicamente tutelati come i già citati patrimonio,

---

[55] Vedi PICOTTI L., *Sicurezza, informatica e diritto penale*, in DONINI M.-PAVARINI M. (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, 217 ss., 221 ss.

[56] Si cominciano a vedere i primi risultati delle indagini criminologiche anche sui soggetti che operano all'interno del web come si può osservare nello studio di BROADHURST R.-GRABOSKY P.-ALAZAB M.- CHON S., *Organizations and Cyber Crime: An Analysis of The Nature of Groups engaged in Cyber Crime*, in *IJCC*, vol. 8, Issue 1, 2014, 1 ss

riservatezza informatica, onore e così via ma che diventa decisamente più complessa quando ci si rende conto della mole sempre maggiore di *malware* che vengono quotidianamente creati e che obbligano il legislatore ad adottare una definizione maggiormente "elastica" che rischia, per ricollegarsi al discorso precedente, di ricomprendere anche i *software* che non sono realmente pericolosi.
Si considerino ad esempio quei *software* usati nella quotidianità per criptare determinati *file* o documenti sul proprio computer personale così da rendere l'accesso più difficile alle persone prive di autorizzazione e che vengono ad oggi utilizzati dai criminali informatici anche per criptare e rendere inaccessibili documenti presi in "ostaggio" su un computer e per liberare i quali viene richiesto un riscatto (i c.d. *ransomware*): ci troviamo davanti ad un *software* con una doppia anima che, a seconda dei casi, può essere utilizzato per scopi leciti o illeciti.
Alla luce di quanto sin qui illustrato, in conclusione alla presente trattazione si cercherà proprio di spiegare la natura di questi "*dual use software*" ed indicare nuovi modi per approcciarsi ad una materia così complessa. Dar adito, infatti, ad una incriminazione troppo restrittiva – andando a colpire solo i *software* esclusivamente creati per scopi illeciti – risulterebbe spesso in una disciplina inapplicabile perché assai raramente un *software* possiede una sola possibilità di utilizzo[57]. D'altra parte, però, se si cedesse ad una incriminazione eccessivamente ampia si andrebbero a ricomprendere anche quei *software* che di per sé non hanno un carattere offensivo o che non sono stati creati originariamente per scopi illeciti: si finirebbe per colpire il settore dell'*Information Technology* (anche detta semplicemente: IT) impedendo l'evoluzione e la crescita di quel settore necessario allo sviluppo di *antivirus*, *firewall* e di tutti quei programmi pensati per elevare il livello di sicurezza informatica di un sistema. Si otterrebbe, dunque, l'effetto inverso a quello che si vorrebbe ottenere: un "*chilling effect*" con le aziende non invogliate a creare quegli stessi *software* atti a difendere la rete ed i sistemi contro quei *malware* che, invece, continuerebbero facilmente a proliferare indisturbati[58].

[57] Vedesi al riguardo CLOUGH J., *Principles of Cybercrime*, 2nd ed., Cambridge, 2015, 135.
[58] Anche in questo caso si rimanda alla lettura degli ordinamenti esteri per comprendere le scelte fatte sulla questione, in particolar modo a quello tedesco in *§ 202c D-StGB*, BORGES S.-STUCKENBERG C.F.-WEGENER C., *Bekämpfung der Computerkriminalität. Zum Entwurf*

CAPITOLO II

PROFILI DI TUTELA A LIVELLO NAZIONALE

A questo punto della trattazione, risulterà utile analizzare nel dettaglio gli articoli riguardanti l'accesso abusivo ad un sistema informatico o telematico (articoli 615-*ter* e successivi c.p.) e quelli riguardanti il danneggiamento informatico (635-*bis* e successivi c.p.); peraltro, in connessione con il primo gruppo di disposizioni richiamate si tratterà anche la disciplina delle intercettazioni di comunicazioni "relative ad un sistema informatico o telematico o intercorrenti tra più sistemi" contenuta negli articoli 617-*quater*, 617-*quinquies* e 617-*sexies* c.p., le quali possono essere attuate anche attraverso l'utilizzo di un *dual use software* e che si inseriscono nella più vasta fattispecie di quelle condotte atte a tutelare la propria attività svolta a mezzo internet, in questo caso quella comunicativa.

1.0 I reati contro la riservatezza informatica

All'interno di questo paragrafo saranno esaminate due diverse categorie di reati, quella dell'accesso abusivo ad un sistema informatico o telematico (articoli 615-*ter* e successivi del Codice penale) e quella delle intercettazioni di comunicazioni "informatiche" (articoli 617-*quater* e successivi del Codice penale) poiché si ritiene che entrambe ricadano su un bene giuridico molto simile, quale un generico diritto alla riservatezza informatica intesa come libertà individuale all'espressione della propria personalità, sia per quel che riguarda quanto viene

Strafrechts-änderungsgesetzes zur Bekämpfung der Computerkriminalität, in *DuD*, 2007, 275 ss., 277.

contenuto o svolto in un elaboratore elettronico sia nel caso in cui quest'ultimo venga usato per comunicare a distanza con altri. Sia concesso di iniziare questo cammino dal reato che per primo ha visto la luce ed ha aperto la strada a tutti gli altri che sono poi seguiti.

1.1 L'articolo 615-*ter* c.p.

Tale fattispecie sanziona chi ‹‹abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo››[59]. Nella prospettiva del legislatore del 1993[60] questa condotta coincideva con quella contenuta nell'articolo 614 c.p. (violazione di domicilio) tanto da meritare un identico trattamento sanzionatorio: reclusione fino a tre anni nell'ipotesi base, da uno a cinque anni nelle ipotesi aggravate previste al comma 2 e sulle quali avremo modo di tornare in futuro. Eppure, le similitudini con l'articolo 614 non sono esaurite perché la stessa struttura del reato di cui all'articolo 615-*ter* ricalca quella del suo predecessore tanto da essere distinto al suo interno tra due diverse ipotesi alternative: quella di chi si introduce "abusivamente" in un sistema informatico o telematico (attiva) e quella di chi illecitamente vi si mantiene contro la volontà di chi avrebbe il diritto di escluderlo (passiva). Questo debito dovuto alla fattispecie della violazione di domicilio non solo rivela la *forma mentis* del legislatore che tale norma plasmò nel lontano 1993 – che cercava di far rientrare le nuove fattispecie di reati informatici all'interno di ipotesi già conosciute nel nostro codice penale, alcune volte accostandole sulla base dello stesso ipotetico bene giuridico tutelato – ma disvela anche i diversi errori che furono commessi durante la stesura di tale articolo, a partire proprio dalla condotta punita: si parla non di "accesso" come sarebbe stato più corretto fare – anche solo per restare fedeli alla stessa rubrica del delitto – ma di "introduzione"[61]. Chiaramente questo verbo è più utile a descrivere la fattispecie di una persona che fisicamente si "introduca" in un luogo delimitato, che vada a varcare un confine immaginario o non.

[59] Art. 615-*ter*, primo comma, c.p.
[60] Legge 23 dicembre 1993, n. 547.
[61] Si rimanda "*supra*", nota numero 40, capitolo I, §1.5.1 per maggiori dettagli.

Come spesso accade, la giurisprudenza ha approfittato di questa somiglianza non del tutto corretta per semplificare e andare ad applicare i precedenti schemi che erano già stati creati per l'articolo 614 del Codice penale. Cosa ha significato tutto questo? Prima di tutto nel dover capire quali siano i confini applicativi della fattispecie, poiché se si applicasse pedissequamente l'ipotesi più "fisica" del significato del verbo si dovrebbe punire chiunque entri anche solo in contatto con il computer senza per questo accedervi. Messa da parte questa ipotesi illogica bisogna però fare un passo in avanti, entrare maggiormente nello specifico: "introdursi" deve essere inteso come l'atto d'andare ad intessere un dialogo logico o automatico con il *software* di un sistema informatico, dunque impartirgli una serie di comandi che lo strumento computerà e ai quali successivamente risponderà per svolgere un'operazione che dia così accesso e permetta la disponibilità del computer alla persona che quei comandi li abbia inseriti. Da notare come è punita la semplice instaurazione di questo dialogo, non è importante né tantomeno pare avere rilevanza il fatto che poi l'agente, una volta entrato, abbia appreso determinate informazioni o modificato determinati documenti e così via[62]. Certo, è ovvio, al giorno d'oggi che gli accessi abusivi siano effettuati proprio con tale obiettivo e non sono rari i soggetti criminali che utilizzino *spyware* (come i *trojan horse* o i *keylogger*) per intrufolarsi all'interno di un sistema e captare così, all'insaputa del suo utilizzatore, eventuali dati e informazioni che passano attraverso quella specifica piattaforma o piattaforme connesse. Tuttavia, come già accennato, il pensiero del legislatore non era rivolto alla protezione delle informazioni contenute all'interno di un computer, bensì alla salvaguardia dello spazio personale di un individuo anche attraverso l'utilizzazione di apparecchi elettronici.

Altrettanto degna di biasimo è la condotta di chi si "mantenga" all'interno di un sistema informatico o telematico contro la volontà di chi abbia il diritto di escluderlo (espressamente o tacitamente). Così facendo è possibile punire anche l'intrusione di chi abbia avuto erroneamente accesso ad un sistema o ci sia potuto entrare perché autorizzato (ma poi ci sia rimasto contro la volontà o all'insaputa della stessa persona che tale permesso gli aveva concesso).

[62] Tema già precedentemente trattato, v. *supra*, capitolo I, §1.5.1.

Il tipico esempio è quello del tecnico informatico entrato all'interno di un sistema per svolgere dei controlli ma che poi ci si mantenga per visionare determinati documenti o spiare l'attività di dipendenti e dirigenti. Anche in questo caso, come nell'ipotesi di condotta attiva, con "mantenimento" si intende semplicemente la continuazione della connessione logica o automatica previamente instaurata e non bisogna leggere il verbo in senso "fisico".

Secondo parte della dottrina per aversi tale condotta sarebbe necessario il ‹‹continuare ad accedere alla conoscenza dei dati, nonostante l'intervenuto divieto del soggetto››[63], tuttavia ciò si porrebbe in contrapposizione non solo con il dato normativo, ma anche con la previa valutazione della condotta attiva che sanziona la mera introduzione in un sistema informatico o telematico.

Rispetto ad altri ordinamenti (quali quello austriaco o tedesco) l'articolo 615-*ter* punisce il mero accesso o la mera permanenza: non è necessario quindi che il soggetto apprenda il contenuto di qualche dato o prenda possesso di un qualsivoglia programma, ma è sufficiente che la connessione logica instaurata con quello specifico elaboratore elettronico continui a permanere contrariamente alla volontà del suo titolare[64].

1.1.1 L'abusività della condotta

Il delitto di cui si è appena delineata la condotta richiede, però, anche un altro elemento che si è più volte implicitamente affermato e cioè la sua abusività: si richiede che sia l'accesso sia la permanenza avvengano all'oscuro del titolare del sistema informatico o telematico o, addirittura, contro la sua volontà.

Qualcuno potrebbe far notare, però, come nella condotta "attiva" si richieda solamente l'abusività mentre nella condotta "passiva" il mantenersi debba avvenire ‹‹contro la volontà espressa o tacita›› di chi avrebbe il diritto di escludere, tuttavia, la differenza si risolve soltanto in una clausola di stile voluta dal legislatore, senza che ciò comporti una reale differenza tra le due fattispecie;

[63] Anche qui si rimanda *supra* alla nota 43, capitolo I, §1.5.1.

[64] La giurisprudenza si divide solo riguardo alla situazione in cui un soggetto, precedentemente autorizzato ad accedere ad un sistema informatico o telematico, vi si mantenga per svolgere attività diverse o contrarie alle ragioni che avevano in origine giustificato il ricevuto permesso d'accesso. Si tornerà sull'argomento in maniera più estesa *infra*.

pertanto, si può leggere e riassumere tutto, semplicemente, nel termine ‹‹abusivamente››.

Secondo alcuni non sarebbe altro se non una clausola di illiceità espressa[65] e dunque il giudice, al momento della valutazione, dovrebbe verificare che al momento della commissione del reato non vi fosse il consenso dell'avente diritto a quell'accesso; tuttavia una simile lettura non è del tutto convincente[66]. Così considerando, infatti, l'avverbio utilizzato sembrerebbe più che altro integrare un elemento costitutivo del reato o, meglio, un "elemento positivo costruito negativamente" funzionale a una più precisa delimitazione dell'ambito d'applicazione del fatto tipico ("Tatbestandseinschränkung")[67]. Se si facesse a meno di tale requisito la previsione legale perderebbe di valore dato che di per sé le semplici condotte di introduzione o mantenimento all'interno di un sistema informatico o telematico non sono capaci di possedere un'autonoma offensività. Come già detto, infatti, non si tutelano i documenti, le informazioni, i dati ecc. presenti in un computer, quanto la sfera privata dell'individuo che utilizza tale strumento ed è quindi proprio l'abusività ad esprimere l'illiceità di tale comportamento: se la persona che utilizza il sistema prestasse il suo consenso espresso o tacito (tipo fornendo ad altri le chiavi d'accesso o la *password*) allora la condotta di introduzione o mantenimento perderebbe di offensività mancando il conflitto intersoggettivo tra l'agente e il titolare del diritto di esclusione.

---

[65] A sostegno di questa tesi si sono schierati, nel tempo, BORRUSO R., *La tutela del documento e dei dati*, cit., 32; PAZIENZA F., *In tema di criminalità informatica*, cit., 756; PICA G., *Diritto penale*, cit., 38 ss.; PECORELLA C., *Sub art. 615-ter c.p.*, in *Codice penale commentato*, cit., 596 ss.; GATTA G.L., *Delitti contro l'inviolabilità del domicilio*, in VIGANÒ F.-PIERGALLINI C. (a cura di), *Reati contro la persona e contro il patrimonio*, in *Trattato teorico/pratico di diritto penale*, diretto da PALAZZO F.-PALIERO C.E., 2ª ed., Torino, 2015, 317 ss., 353 s.; PIERGALLINI C., *I delitti contro la riservatezza informatica (artt. 615*-ter. *615*-quater, *615*-quinquies*)*, in AA. VV., *I delitti contro la persona, Trattato di Diritto penale*, PS, diretto da MARINUCCI G.-DOLCINI E., Milano, 2015, 769 ss., 780.

[66] Contrari sono stati, ad esempio, DELITALIA G., *Il "fatto" nella teoria generale del reato*, Milano, 1930, 15 ss.; ma anche PULITANÒ D., *Illiceità espressa e illiceità speciale*, in *Riv. it. dir. e proc. pen*., 1967, 65 ss., 72 ss. Meno risalente nel tempo è l'analisi di MORGANTE G., *L'illiceità speciale nella teoria del reato*, Torino, 2002, 27 ss., 30 ss., 61 ss. dove viene ripreso il tema che l'‹‹antigiuridicità espressa›› non può essere elemento costitutivo di reato quando vengono utilizzate locuzioni quali ‹‹abusivamente›› *et similia*.

[67] Per una più approfondita analisi riguardante il disvalore che ruota intorno alla mancanza di autorizzazione leggasi MAZZACUVA N., *Le autorizzazioni amministrative e la loro rilevanza in sede penale*, in *Riv. it. dir. e proc. pen*., 1976, 774 ss.; a riguardo delle fattispecie trattate questa configurazione è stata ripresa anche da SALVADORI I., *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, Napoli, 2016, 118 ss., 146 ss.

Può dunque concludersi che il reato in esame punisce colui che si introduce o si mantiene in un sistema informatico ‹‹in assenza di autorizzazione o eccedendo i limiti della stessa››[68].

Chiaramente tale abusività deve essere valutata in modo oggettivo facendo riferimento al momento in cui l'introduzione o la permanenza avvengono e non in relazione a quanto possa avvenire successivamente (danneggiamento del sistema, copia di *files,* alterazione del funzionamento ecc.)[69]: il comportamento di introduzione o permanenza risulterà punibile solo nel momento in cui sia avvenuto con la volontà contraria del titolare del diritto d'esclusione o senza una dovuta autorizzazione (come nel caso in cui un soggetto utilizzi un captatore elettronico fuori dai casi specificatamente indicati dalla legge[70])[71].

Nell'ambito dell'articolo 615-*ter* ma anche nella nostra successiva analisi riguardante il *dual use software* acquista, quindi, un'importanza centrale l'interpretazione estensiva o restrittiva di questo elemento costitutivo[72]. Quand'è che si opera in maniera abusiva accedendo o mantenendosi in un sistema e fino a quali risultati si può portare l'autorizzazione espressa o tacita dell'avente diritto? Come al solito per dare una risposta non si sbaglia se ci si mantiene quanto più possibile fedeli al dato normativo senza andare a trascendere i possibili significati. Non esiste una definizione normativa espressa del concetto di "abusività" ma si può porre un rimedio andando ad interpretare questo termine secondo il significato che gli viene attribuito in ambito europeo[73]. In questo modo si

---

[68] La questione, in realtà, è tutt'altro che risolta sia in giurisprudenza che in dottrina. Personalmente ho deciso di adottare la visione che viene espressa da SALVADORI I., *Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-*ter *c.p.,* in *Riv. trim. dir. pen. economia*, 2012, 369 ss. ma estremamente forte è ancora la dottrina che sostiene che l'‹‹abusività›› corrisponda solo all'‹‹assenza di autorizzazione›› originale e tra i molti si può citare, per esempio, FLOR R., *Verso una rivalutazione dell'art. 615-*ter *c.p.?,* in *Dir. pen. cont.-Riv. trim*., 2011, 126 ss.

[69] Cfr. Cass. pen., sez. VI, sent. 8.10.2008, Peparaio, n. 39290.

[70] Qui si è espresso direttamente il legislatore con il D.lgs. 29.12.2017, n. 216, recante ‹‹Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23.6.2017, n. 103››.

[71] Cfr. Cass. pen., SS. UU., sent. 27.10.2011, n. 4694.

[72] La materia è particolarmente complessa ed il dibattito giurisprudenziale ancora vivo. Avendo optato per sostenere la visione più estensiva si rimanda, anche per i riferimenti bibliografici, a SALVADORI I., *Quando un insider accede abusivamente*, cit., 369 ss.

[73] Cass. pen., sez. V, 29.5.2008, n. 26797 si è espressa così al riguardo dicendo che ‹‹la formula "abusivamente si introduce" recata dalla disposizione in esame [art. 615-*ter* c.p.] appare la incerta traduzione di quella "accesso non autorizzato" (o accesso illegale) già utilizzata nella lista minima

dovrebbe tenere in considerazione soprattutto il concetto di ‹‹senza diritto›› che costituisce il punto focale della materia dell'accesso illecito ad un sistema informatico come contenuto dall'articolo 3 della Direttiva 2013/40/UE.

Secondo quanto indicato dall'articolo 2, lettera d) della stessa direttiva la definizione della locuzione "senza diritto" si potrebbe riscontrare nell'eccesso di una persona che ‹‹non sia stata autorizzata dal proprietario del sistema o da colui che è titolare di diritti sul sistema ovvero non sia consentita a norma del diritto nazionale››[74]. Il preambolo della direttiva, però, ci tiene a specificare che non deve essere punita la condotta di chi si limita a una "mera violazione di accordi contrattuali" così da escludere la punibilità di chi compia una semplice disubbidienza.

In giurisprudenza e in dottrina, partendo proprio da queste basi, è prevalso il modo di vedere di chi marca soprattutto la manifestazione di contrarietà, espressa o tacita, da parte del titolare dell'*ius excludendi*. Questa situazione è ancora una volta dovuta all'originale matrice del reato e cioè l'articolo 614 c.p., per il quale l'ipotesi di violazione di domicilio si manifesta solo nel caso in cui sussista una volontà contraria del titolare dello *ius excludendi alios* (e dunque un disvalore sociale punibile). Come tale non si può desumere l'abusività della condotta dal semplice contrasto con altre norme dell'ordinamento (ad esclusione di qualche eccezione su cui si tornerà in seguito)[75].

Solitamente la giurisprudenza si divide in due tronchi interpretativi riguardo ai criteri ermeneutici da utilizzare per stabilire quando un soggetto svolga la condotta in modo "abusivo": il primo pone la propria stella polare nella contrarietà delle finalità perseguite a quelle per cui l'autorizzazione fu originariamente concessa; la seconda invece si basa sull'oggettiva violazione delle disposizioni e delle prescrizioni che ordinano e disciplinano un accesso o la permanenza in un sistema informatico o telematico.

---

del Consiglio d'Europa che accompagnava la Raccomandazione (89) 9, cui si è adeguato il legislatore nazionale con la legge n. 547 del 1993 e, quindi, della locuzione accesso "senza diritto" (*access… without right*) impiegata nell'articolo 2 della Convenzione sul cybercrime››.

[74] Cfr. Dir. 2013/40/UE, *Consideranda* n. 17.

[75] In contrario leggasi MARINI G., *Delitti contro la persona*, Torino, 1996, 386, che sposa la linea secondo cui, invece, la condotta illecita di accesso abusivo possa essere determinata dall'agire dell'agente contro il consenso di colui che gli aveva in origine conferito l'autorizzazione e, dunque, anche quando agisca fuori dall'ambito delle facoltà che gli furono concesse o delle ipotesi stabilite dalla legge.

Il primo orientamento, in considerazione della pericolosità dei comportamenti adottati dalle persone autorizzate ad accedere a un determinato sistema informatico o telematico (i così detti "*insider*"), ha inteso proporre una visione più ampia del concetto di abusività. Si è quindi ritenuta punibile la condotta di colui che impieghi il suo titolo di legittimazione al fine di perseguire una propria finalità illecita o, comunque, diversa rispetto a quella per cui si è ricevuta l'autorizzazione: una ricostruzione, dunque, della clausola di illiceità speciale dell'abusività intesa maggiormente in senso "soggettivo". Alla luce di quanto sopra esposto il semplice commettere azioni che si allontanano dalle originali finalità dell'autorizzazione porrebbe l'*insider* in contrasto con la "*voluntas domini*" e tutte le attività da lui realizzate sarebbero implicitamente contrarie alle ragioni di colui che potrebbe escluderlo dall'uso del sistema. A tale visione, però, si oppongono una pluralità di ragioni che si possono desumere dallo stesso contenuto dell'articolo e dal suo dato letterale: per prima cosa la fattispecie richiede la volontà contraria, implicita o esplicita, del titolare dello *ius excludendi* o comunque la mancanza del titolo autorizzativo (originaria o derivata che sia)[76]. Certo, è ovvio, tale illiceità può essere desunta anche dal comportamento dell'utilizzatore del sistema che compia atti incompatibili con la volontà del responsabile del sistema o, comunque, in contrasto con le regole di gestione del sistema informatico[77]. L'abusività, come è stato più volte ricordato in passato, si manifesta quando il soggetto si introduce o si mantiene in un sistema informatico o telematico senza l'autorizzazione o contravvenendo ai termini in precedenza indicati dalle norme contrattuali o nelle disposizioni organizzative o dalle regole che disciplinano l'attività di quello specifico ufficio.

Contrariamente, invece, se si seguisse l'interpretazione sopra indicata si andrebbe a ricavare l'abusività esclusivamente dai fatti commessi dopo l'accesso e che quindi andrebbero a richiedere la presenza di ulteriori atti di volizione rispetto a

[76] Si è assistito alla nascita di tale orientamento a partire da Cass. pen., sez. V, 7.11.2000, n. 1675 ed è poi stata ripresa più volte in Cass. pen., sez. V, 8.7.2008, n. 37322; Cass. pen., sez. V, 30.9.2008, n.1727; Cass. pen., sez. V, 3.2.2009, n. 18006; Cass. pen., sez. V, 10.12.2009, n. 2987; Cass. pen., sez. V, 12.2.2010, n. 19463; Cass. pen., sez. V, 22.9.2010, n. 39620; Cass. pen., sez. V, 18.1.2011, n. 24583; fino a Cass. pen., sez. V, 29.11.2017, n. 1021.

[77] Al riguardo Cass. pen., sez. V, 8.7.2008, n. 37322. Aderisce a questa interpretazione DE FLAMMINEIS S., *Art. 615-ter c.p.: accesso legittimo ma per finalità estranee ad un sistema informatico*, in *Cass. pen*., 2011, n.6, 2209 ss.

quello originario di accesso al sistema ponendosi in contrasto con il concetto di "abusività" finora esposto (e che tutela la riservatezza informatica in quanto tale, non il contenuto di un computer). Seguendo tale via si andrebbe fuori dal tracciato dall'articolo 615-*ter* c.p. causando un ampliamento dell'ambito di applicazione di tale fattispecie anche oltre il suo contenuto letterale in violazione non solo del principio di tassatività ma anche del divieto di analogia. Si finirebbe facilmente per dare valore offensivo a qualsiasi azione compiuta dal soggetto autorizzato che si discosti dall'originale ragione di concessione, anche quelle che comunemente non possono essere pericolose o sono prive di un intento malevolo (come controllare il proprio account *Facebook* in un momento di pausa usando lo stesso computer sul quale fino a poco prima si stava lavorando e che appartiene ad altra persona[78]).

Peraltro, sarebbe estremamente difficile dimostrare, in sede processuale, la natura della finalità soggettiva che il soggetto agente avrebbe perseguito con la sua condotta e che dilaterebbe eccessivamente l'ambito applicativo di questo articolo, lasciando alla giurisprudenza l'arduo compito di sopperire a un parametro normativo che, letto in questo modo, risulterebbe troppo poco oggettivamente valutabile. D'altronde, nel 2011, sono state proprio le Sezioni Unite della Corte di Cassazione[79] a sancire in modo espresso l'irrilevanza delle finalità, che siano lecite o illecite, motivanti l'accesso non autorizzato ad un sistema informatico o telematico (ponendo in questo modo fine a questa interpretazione dottrinale).

La seconda interpretazione dottrinale, invece, pone l'accento sulla violazione delle disposizioni che disciplinano l'accesso o il mantenimento all'interno di un sistema informatico o telematico. Anticipando che la consumazione del reato avvenga nel momento in cui l'introduzione prende atto (iniziando il dialogo logico o automatico con il sistema informatico) o nel momento in cui si entra in contrasto con l'originaria ragione giustificatrice della nostra presenza (mantenendo il dialogo precedentemente instaurato con la macchina in modo illecito) non vengono in risalto, almeno in questo senso, tutte le azioni successivamente svolte

[78] Cass. pen., sez. V, 24.4.2013, n. 22024.

[79] Cass. Pen., SS. UU., 27.10.2011, n. 4694 come in *Dir. pen. cont.-Riv. Trim*., n. 1, 2012, 123 ss. con nota di BARTOLI R., *L'accesso abusivo a un sistema informatico (art. 615-ter c.p.) a un bivio ermeneutico teleologicamente orientato*.

che possono al più integrare autonomi fatti illeciti. L'abusività delle condotte tenute va dunque ricostruita guardando i regolamenti nonché le disposizioni organizzative interne o i regolamenti di condotta che delineano l'ambito spaziale e temporale d'accesso nonché di mantenimento o la mancanza del titolo di legittimazione[80].

Così facendo non solo si rispetterebbe la portata della lettura normativa dando adito alla punibilità dell'accesso abusivo in un sistema informatico o telematico ma si andrebbe anche a dare il giusto risalto alla condotta di chi si mantenga in esso "contro la volontà espressa o tacita di chi ha diritto di escluderlo". Come tale l'avente diritto non solo può cercare di proteggersi dagli "*outsiders*" adottando misure di sicurezza, ma può anche delimitare l'ambito di movimento degli "*insiders*" sia attraverso la propria esplicita volontà sia attraverso norme o regolamenti interni che devono essere conosciuti e rispettati. Allo stesso tempo, così facendo, si conferisce anche maggiore sicurezza allo stesso sistema normativo dato che ci si appoggia su regole scritte o precedentemente rese esplicite come parametro di valutazione per una possibile violazione. Si deve comunque evitare di cadere nel precedente errore, quello di ampliare eccessivamente la fattispecie applicativa andando a prevedere specifici regolamenti o norme interne che dicano chiaramente cosa si possa o non si possa fare[81].

Così facendo la clausola di illiceità speciale viene maggiormente delineata nei termini di "violazione di prescrizioni" e non si espone alla scorretta quanto pericolosa inclusione di meri principi o norme generiche quali possono essere l'imparzialità o la buona fede ecc. L'abusività, in conclusione, si manifesta attraverso caratteri previamente determinabili nella loro portata applicativa che non lasciano spazio a interpretazioni eccessivamente dilatate nell'ambito della rilevanza penale della condotta[82].

---

[80] Si fa riferimento a Cass. pen., SS. UU., 27.10.2011, n. 4694; Cass. pen., sez. V, 8.5.2012, n. 42021; Cass. pen., sez. II, 6.3.2013, n. 13475; Cass. pen., sez. V, 28.7.2016, n. 33311. Per quanto riguarda la dottrina, invece, si veda SALVADORI I., *Quando un insider accede abusivamente*, cit., 388; FLOR R., *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'*extraneus, in Cass. pen., fasc. 4, 2009, 1509 ss.

[81] V. SALVADORI I., *Quando un insider accede abusivamente*, cit., 389.

[82] Si notino i rilievi al riguardo di TESAURO A., *Violazione di legge ed abuso d'ufficio. Tra diritto penale e diritto amministrativo*, Torino, 2002, 11-13.

1.1.2 La definizione di misure di sicurezza

Bisogna notare come il legislatore ha ritenuto di dover tutelare, però, solo gli accessi abusivi che fossero messi in atto su sistemi informatici o telematici "protetti da misure di sicurezza". Quel che subito salta all'occhio, dunque, è che non abbia richiesto il loro effettivo aggiramento come accade invece nell'ordinamento austriaco, tedesco o spagnolo[83] e, allo stesso tempo, che non abbia specificato cosa sia una "misura di sicurezza".

Nella relazione ministeriale che ha accompagnato l'emanazione di questo articolo si spiega la risposta al primo quesito, ove si afferma che ‹‹dovendosi tutelare il diritto di uno specifico soggetto, è necessario che quest'ultimo abbia dimostrato, con la predisposizione di mezzi di protezione sia logica che fisica (materiale o personale), di voler espressamente riservare l'accesso e la permanenza nel sistema alle sole persone da lui autorizzate››[84]. La semplice presenza di una misura di sicurezza serve, dunque, ad esprimere la volontà del legittimo titolare del sistema (non sempre coincidente con l'utilizzatore o con il proprietario di dati e informazioni all'interno del computer[85]) di escludere gli altri e quindi prospettarsi come contrario a eventuali tentativi d'accesso non autorizzati. Si richiede implicitamente, in questo modo, una responsabilizzazione del titolare del sistema informatico che dovrà dotarsi di misure di sicurezza atte a manifestare espressamente la sua volontà al fine di rendere molto più semplice, in sede processuale, la dimostrazione dell'abusività della condotta dell'agente[86].

Quel che resta, a questo punto, è la seconda domanda: quale tipo di misura di sicurezza?

---

[83] Cfr. Cass. pen., sez. V, 7.11.2000, n. 12732 che sottolinea come l'articolo 615-*ter* c.p. non sia legato all'effrazione delle misure di sicurezza.

[84] Contenuto nella relazione di presentazione del progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penale in materia di criminalità informatica, in *Doc. giust*., 1991, n. 9, 142 ss.

[85] Tesi sposata in giurisprudenza da Trib. Rovereto 9.1.2004, n. 343, in *Dir. pen. e processo*, n. 1, 2005, 81 ss., con nota di adesione di FLOR R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo* ius excludendi alios. In dottrina, invece, vedasi MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica del diritto*, n.4, 1999, 12 ss., 19 ss.

[86] Cfr. PICOTTI L., *Reati informatici*, cit., 22; MANTOVANI M., *Brevi note*, cit., 20 ss.; PECORELLA C., *Il diritto penale dell'informatica*, cit., 324 ss.

La vaghezza dello stesso dato normativo parrebbe suggerire essa stessa la risposta: qualsiasi tipologia. Non è importante il livello di complessità o la sua reale efficacia ma è sufficiente che essa sia presente e che sia in grado di ostacolare il libero accesso a quell'elaboratore elettronico al fine di far godere il suo titolare della tutela penale nei confronti di possibili intrusioni o permanenze non autorizzate[87]. Non ha alcun tipo di importanza, quindi, che il computer fosse protetto da una semplicissima *password* o che fosse stato semplicemente nascosto all'interno di un cassetto chiuso da un banale lucchetto.

Come tale si deve ricomprendere, almeno stando alla dottrina, nel novero delle misure di sicurezza qualsiasi mezzo assunto per sottolineare la volontà contraria ad un qualsivoglia accesso altrui: può essere un mezzo fisico, come nel citato esempio del lucchetto, o uno organizzativo come dispositivi tecnici di riconoscimento maggiormente avanzati (riconoscimento facciale, *scanner* dell'impronta digitale, chiave vocale ecc.) o di natura "logica" (come la più tipica *password* d'accesso). L'importante è che sia una misura – minimamente – idonea a ostacolare persone senza autorizzazione dall'introduzione in quel determinato sistema informatico o telematico di nostra specifica titolarità[88].

1.1.3 Altri elementi della fattispecie

Il reato è punito a titolo di dolo generico, è sufficiente quindi che il soggetto agente si sia introdotto o si sia mantenuto all'interno del sistema informatico o telematico con la "volontà consapevole" di farlo senza il permesso di colui che avrebbe il diritto di escluderlo o privo di un titolo di legittimazione che possa giustificare la violazione delle misure di sicurezza.

Come tale non è importante la motivazione per cui ci si introduce nel sistema quanto la consapevolezza della violazione di un elaboratore elettronico altrui[89]. Il

[87] In dottrina si legga D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, in BORRUSO R.-BUONOMO G.-CORASANITI G.-D'AIETTI G. (a cura di), *Profili penali dell'informatica*, Milano, 1994, 39 ss., 71 ss.; PARODI C., *Accesso abusivo, frode informatica, rivelazione di documenti informatici segreti: rapporti da interpretare*, in *Dir. pen. e processo*, 1998, 1038 ss. In giurisprudenza, invece, si faccia riferimento a Trib. Torino 4.12.1997, in *Giur. it.*, 1998, 1923 ss.
[88] Cfr. Cass. pen., sez. V, 8.7.2008, n. 37322; Cass. Pen., sez. II, 19.12.2014, n. 52680.
[89] Cfr. PICA G., *Diritto penale*, cit., 69; PECORELLA C., Sub *art. 615*-ter c.p., cit., 606.

problema che ne deriva è che non sempre chi agisce può rendersi conto di star penetrando nelle misure di sicurezza di un'altra persona, come accade per esempio nel caso in cui ci si ritrovi a connettersi a un computer trovato in una rete Wi-Fi pubblica; allo stesso tempo, nel caso in cui l'accesso sia stato fortuito, non sempre sarà così facile rendersi conto del mantenimento che si sta protraendo a danno di un altro all'interno del sistema. In questo specifico caso, dunque, anche se in realtà la condotta ha tutti gli estremi per essere offensiva, difficilmente verrà sussunta all'interno della fattispecie di cui all'articolo 615-*ter*, mancandone alcuni elementi caratterizzanti dell'elemento soggettivo.

La centralità concessa all'aggiramento delle misure di sicurezza torna in tutta la sua importanza anche riguardo al momento consumativo del reato. Quest'ultimo coincide, infatti, con la penetrazione nel sistema informatico o telematico protetto e con l'effettiva instaurazione di un dialogo logico con l'elaboratore elettronico senza autorizzazione o in aperto contrasto con la volontà del legittimo titolare dell'*ius excludendi*[90]. Secondo questa lettura, quindi, il semplice provare ad accedere a un computer non coinciderebbe con la consumazione del reato né tantomeno configurerebbe il tentativo *ex* articolo 56 del Codice penale.

Se si accettasse una simile disposizione si andrebbe ad arretrare – forse eccessivamente – la tutela penale quando l'articolo 615-*ter* già di suo configura un delitto di pericolo astratto che come tale pone la consumazione del reato in modo anticipato (è sufficiente l'instaurazione della connessione logica con il sistema senza la necessità che, da questo legame, si evinca una qualche forma d'informazione o dato[91]).

---

[90] In giurisprudenza Cass. pen., sez. V, 7.11.2000, in *Guida dir*., 2001, 78 ss., con nota di GALDIERI P., *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*; ma anche Cass. pen., SS. UU., 24.4.2015, n. 17325, in *Dir. pen. e processo*, 2015, 1296 ss., con nota di FLOR R., *I limiti del principio di territorialità nel "*cyberspace*". Rilievi critici alla luce del recente orientamento delle sezioni unite*. Ma in dottrina la tesi è stata avvallata anche da PECORELLA C., *Il diritto penale dell'informatica*, cit., 334. *Contra*, Cass. pen. sez. V, 4.12.2006, n. 6459, per la quale ai fini della consumazione del reato è necessario che il soggetto attivo abbia violato le misure di sicurezza poste a protezione del sistema informatico o telematico.

[91] Si sono schierati contro tale tesi NUNZIATA M., *La prima applicazione giurisprudenziale del delitto di "accesso abusivo ad un sistema informatico" ex art. 615-*ter *c.p.*, in *Giur. di Merito*, 1998, II, 711 ss., 715; ma anche PAZIENZA F., *In tema di criminalità informatica*, cit., 1092, per il quale il reato si perfezionerebbe solo al momento dell'apprensione dei contenuti.

Bisogna, però, sottolineare che il tentativo è ammesso da parte di coloro che configurano il delitto come un reato di danno tutelante il bene giuridico del così detto "domicilio informatico" o della "riservatezza informatica".

Per quanto riguarda, invece, il mantenimento all'interno del sistema informatico o telematico il reato si consuma con la scadenza del termine entro il quale si sarebbe dovuto interrompere il dialogo logico con l'elaboratore e, quindi, abbandonarlo[92]. Anche in questo caso il termine entro il quale si sarebbe dovuto adempiere a tale obbligo è da individuare nella volontà espressa o implicita del titolare dell'*ius excludendi* o estrapolabile dalle norme extrapenali a cui si è già fatto riferimento[93] e che disciplinano l'attività del soggetto agente.

La giurisprudenza di legittimità afferma che il luogo di consumazione del reato *ex* articolo 615-*ter* del Codice penale è quello in cui il soggetto agente si introduce o si mantiene attuando la condotta di accesso abusivo[94]. Il problema è che questa tesi, forse eccessivamente risalente nel tempo, non tiene conto del fatto che questo reato ad oggi viene messo in pratica soprattutto da persone che utilizzano VPN (*Virtual Private Network*) o ISP (*Internet Service Provider*) che si trovano in luoghi diversi da quello in cui si trova il criminale o che volutamente permettono di camuffare la propria posizione. Per semplicità, quindi, sarebbe più corretto ritenere che il *locus commissi delicti* venga rappresentato da quello in cui si trova il sistema violato (o il suo *server*)[95].

L'articolo 615-*ter* contempla al proprio interno anche delle circostanze aggravanti ad effetto speciale che sono indicate ai commi 2 e 3 e per le quali è prevista la reclusione da 1 a 5 anni. Nel caso in cui l'aggravante di cui al comma 2 (‹‹accesso abusivo commesso da un funzionario pubblico con abuso di poteri o violazione dei doveri o da un investigatore privato o con abuso della qualità di operatore di sistema; commissione del fatto tramite l'utilizzo di violenza sulle cose o sulle persone o se palesemente armati; distruzione o danneggiamento del sistema o

---

[92] Al riguardo PICA G., *Diritto penale*, cit., 56 ss.; MUCCIARELLI F., *Commento agli art. 1, 2, 4 e 10 l. 1993 n. 547*, cit., 101.

[93] Cfr. *supra*, § 2.0.1.1.

[94] Così Cass. pen., SS. UU., 26.3.2015, n. 17325, 2015, 1296 ss.

[95] Cass. pen., sez. I, 27.5.2013, n. 1921 ss. Esisterebbe anche una terza via avvallata dalla giurisprudenza della Corte di Giustizia europea che sostiene la tesi secondo cui il *locus commissi delicti* corrisponderebbe al luogo in cui si è concretizzato il danno. Viene naturale, però, rendersi conto come questo luogo corrisponderebbe, nella grande maggioranza dei casi, a quello in cui si trova il server.

interruzione totale o parziale del suo funzionamento, ovvero distruzione o danneggiamento dei dati, delle informazioni o dei programmi››) venga commessa in concorso con quella di cui al comma 3 (‹‹delitto commesso contro sistemi informatici o telematici di interesse militari o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico››) la pena è ulteriormente aggravata con la reclusione da 3 a 8 anni; in entrambi i casi il delitto diventa punibile d'ufficio e non più a querela di parte.

1.1.4 Il bene giuridico tutelato

Si è più e più volte tornati sull'argomento nel corso delle pagine precedenti perché è proprio su questo punto che si articola e si espande l'interezza della discussione riguardante l'articolo 615-*ter* e, in generale, tutti quelli connessi all'accesso abusivo ad un sistema informatico o telematico. Si è già detto, anche, che questa norma fu una delle primissime ad essere inserite a partire proprio dalla prima riforma del 1993 e che conserva ancora le tracce di un'impostazione che scontava il modo di vedere dell'epoca. La tutela che si voleva apprestare con questa fattispecie andava a ricadere sul "domicilio virtuale" e quindi rientrava in una forma di tutela tipica quale poteva essere quella dell'articolo 614 c.p. e che aveva, dunque, molti punti di contatto con tale fattispecie[96]. Questa tesi risultava palese dalla stessa relazione ministeriale allegata alla legge 547/1993 in cui si dichiarava che i sistemi informatici e telematici costituiscono ‹‹un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14

[96] *Ex multis*, in giurisprudenza, si prenda ad esempio Cass. pen., sez. V, 16.6.2000, n. 9002; Cass. pen., sez. II, 14.9.2006, n. 30663; Cass. pen., sez. V, 8.7.2008, n. 37322; Cass. pen., sez. V, 26.10.2012, n. 42021; Cass. pen., sez. V, 19.11.2014, n. 47938. In dottrina, invece, si veda ALMA M.M.-PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. e processo*, n.4, 1997, 504 ss., 505; GALDIERI P., *La tutela penale del domicilio informatico*, in ID. (a cura di), *Problemi giuridici dell'informatica nel MEC*, Milano, 1996, 189 ss.; ID, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, 138 ss.; BORRUSO R., *La tutela del documento e dei dati*, cit., 28 ss.; ROSSI VANNINI A., *La criminalità informatica: le tipologie dei computer crimes di cui alla l. 547/1993 dirette alla tutela della riservatezza e del segreto*, in *Riv. trim. dir. pen. economia*, 1994, 427 ss., 431; CUOMO L., *La tutela penale del sistema informatico*, in Cass. pen., 2000, 2998 ss.; PLANTAMURA V., *Domicilio e diritto penale nella società post-industriale*, cit., 186 ss.

della Costituzione e penalmente tutelata nei suoi aspetti più essenziali agli articoli 614 e 615 del Codice penale››[97].

A maggior ragione questa tesi era suffragata anche dal fatto che si richiedesse una misura di sicurezza apposta a protezione del sistema informatico o telematico così da delineare ancora meglio la linea separatorio di un "luogo chiuso" virtuale simile, per analogia, alla delimitazione spaziale del domicilio tradizionale[98]. Secondo questa visione ne deriverebbe che il legislatore abbia voluto tutelare questo luogo in capo al titolare dello *ius excludendi* in quanto "*spatium vitae et cogitationis*" che assurgerebbe a diritto fondamentale tutelato dall'articolo 2 della Costituzione[99]. Così facendo si dovrebbe leggere il delitto come un reato d'evento in cui non solo si punisce il tentativo di introduzione e mantenimento ma qualsiasi condotta che possa penetrare all'interno del sistema informatico o telematico indipendentemente dalle azioni o dall'effettiva captazione di dati, informazioni o programmi andando così a salvaguardare più che la sicurezza del contenuto, l'integrità e la riservatezza offerta dal contenitore in quanto tale[100].

Una parte della dottrina, però, ha sottolineato quanto questa tesi escluderebbe dall'ambito della tutela penale molti sistemi informatici o telematici che, in generale, non vengano utilizzati per contenere un qualsivoglia dato personale o individuale (come potrebbe essere un elaboratore elettronico usato esclusivamente a fini commerciali, industriali o scientifico/culturali)[101].

A questo punto si è andata ad affermare una tesi assolutamente opposta, secondo cui si tratterebbe di una tutela che ricadrebbe non sul sistema in quanto tale quanto sull'integrità delle informazioni o dei contenuti in esso conservati[102]. Si avrebbe così un reato di pericolo astratto che anticipa la tutela cercando di impedire

---

[97] Cfr. CAMERA DEI DEPUTATI, *XI Legislatura*, cit.

[98] Al riguardo ROSSI VANNINI A., *La criminalità informatica*, cit., 744; PLANTAMURA V., *Domicilio e diritto penale*, cit., 187.

[99] Come fatto notare da PICA G., *Diritto penale*, cit., 68.

[100] PICA G., *Diritto penale*, cit., 69; DESTITO V., *Reati informatici*, cit., 744; PLANTAMURA V., *Domicilio e diritto penale*, cit., 187. Si cita BORRUSO R., *La tutela del documento e dei dati*, cit., 28 ss., per cui la consumazione si avrebbe ‹‹anche se l'intromettitore non ha preso conoscenza di alcuna informazione, né ha altrimenti turbato il funzionamento del computer, così come commette violazione di domicilio chi voglia trovarvi una persona che ivi abita anche se poi non lo trova››.

[101] PECORELLA C., *Il diritto penale dell'informatica*, cit. 316; PAZIENZA F., *In tema di criminalità informatica*, cit., 750 ss.; PICOTTI L., *Sistematica dei reati informatici*, cit., 80; MANTOVANI F., *Diritto penale*, PS, I, cit., 577.

[102] Come in MANTOVANI M., *Brevi note*, cit., 12 ss.

l'accesso abusivo per evitare che possano essere messi a rischio tutti i contenuti di un determinato elaboratore elettronico. Questa seconda tesi, però, causerebbe non pochi problemi ad avviso di alcuni commentatori perché non solo escluderebbe la configurabilità del tentativo ma, allo stesso tempo, si andrebbe anche a scontrare ideologicamente con altre fattispecie penali che si occupano specificatamente dell'integrità dei sistemi ma anche dei loro contenuti (come gli articoli 635-*bis* e successivi del Codice penale)[103].

Da notare, oltretutto, l'illogicità di una simile decisione del legislatore che andrebbe a tutelare solo le informazioni o i dati conservati in sistemi informatici o telematici protetti da misure di sicurezza (discriminando, in maniera non ben chiara, tutti gli altri simili beni contenuti in ambienti non protetti)[104].

Una terza tesi ha cercato, invece, una via di mezzo tra le due appena esposte: tenendo in considerazione che il bene giuridico tutelato continua ad essere l'integrità e la riservatezza informatica si è andati a porre l'attenzione sulla finalità di tale tutela che sarebbe quella di proteggere le informazioni ed i dati contenuti nell'elaboratore[105]. Si avrebbe comunque un reato di pericolo astratto ma che si rivolgerebbe maggiormente ad una tutela del mezzo informatico in quanto tale[106].

Anche questa tesi, però, espone il fianco a delle critiche. Se, infatti, il computer dovesse essere vuoto e dunque privo di qualsivoglia informazione personale o individuale, non si andrebbe a violare alcuna riservatezza andandolo a penetrare in maniera abusiva.

Questa terza tesi, così come la seconda, ha il difetto di porre troppa attenzione su un fattore (quello dei contenuti del sistema informatico o telematico) che nella norma non viene mai citato.

In conclusione, pare quindi assolutamente corretto quello di ritenere che l'articolo 615-*ter* vada a tutelare l'interesse giuridico della riservatezza informatica tuttavia

---

[103] Cass. pen., sez. V, sent. 29.7.2016, n. 33311 il cui tema è stato ampliato in dottrina da SALVADORI I., *Il microsistema normativo*, cit., 204 ss.

[104] PECORELLA C., *Il diritto penale dell'informatica*, cit., 321; MANTOVANI F., *Diritto penale*, PS, I, cit., 577.

[105] PECORELLA C., *Il diritto penale dell'informatica*, cit., 322 ss.; PIERGALLINI C., *I delitti contro la riservatezza informatica (artt. 615*-ter, *615*-quater, *615*-quinquies*)*, cit., 769 ss., 772 s.

[106] PECORELLA C., *Il diritto penale dell'informatica*, cit., 323. Per MANTOVANI F., *Diritto penale*, PS, I, cit., 577, si tratterebbe invece di un reato di danno visto che l'accesso abusivo ad un sistema informatico o telematico andrebbe a ledere il diritto alla riservatezza, quindi dei dati e dei programmi contenuti in un elaboratore elettronico.

intesa quale spazio o ambito "virtuale" in cui sia possibile esprimere la propria individualità liberi da interferenze altrui senza ricadere eccessivamente sulla presenza e sulla natura dei contenuti in esso presenti.
Alla luce di quanto si è appena detto si può comprendere perché il reato si configuri, comunque, come un delitto di pericolo astratto.

1.2 L'articolo 615-*quater* c.p.

L'articolo 615-*quater* del Codice penale è stato introdotto per la prima volta dall'articolo 4 della legge 547 del 1993 per sanzionare la diffusione e la detenzione abusiva di codici di accesso a sistemi informatici o telematici.
La lettera della norma recita: ‹‹chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei d'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino ad euro 5164››[107].
Questo articolo è uno dei tanti che nell'ordinamento italiano anticiparono forme di tutela che solo successivamente sarebbero state recepite e introdotte a livello europeo (con l'articolo 6 della Convenzione *Cybercrime* ad opera del Consiglio d'Europa e poi con l'articolo 7 della Direttiva 2013/40/UE).
La ragione ispiratrice di questa norma consisteva nella tutela anticipata del bene giuridico della riservatezza informatica e, in via mediata, della sicurezza informatica, andando a incriminare fatti prodromici alla commissione di reati informatici più gravi (come l'accesso abusivo ad un sistema informatico o telematico, il danneggiamento informatico ecc.)[108]. Tale obiettivo era perseguito attraverso la repressione della circolazione di mezzi idonei a facilitare intrusioni in sistemi informatici altrui. È giusto, quindi, aver inserito questa norma subito dopo l'articolo 615-*ter* anche se solleva maggiori perplessità l'inserimento all'interno

[107] Contenuto dell'articolo 615-*quater* c.p.
[108] Contra PLANTAMURA V., *Domicilio e diritto penale*, cit., 217, per il quale questa fattispecie sarebbe posta a tutela del bene giuridico del domicilio informatico in forma anticipata.

della sezione IV del titolo XII del libro II del Codice penale che riguarda i delitti contro l'inviolabilità del domicilio.

1.2.1 Condotta e abusività

Si è già anticipato come l'articolo in questione preveda la punibilità di condotte che sono prodromiche alla commissione di altri reati informatici considerati come "più gravi". La fattispecie si divide in due forme di condotta principali: la prima sanziona la condotta di chiunque entri in possesso o agisca per far entrare nella sua sfera di possesso "*password*", "chiavi informatiche", "codici" o strumenti che possano essere in generale successivamente utilizzati per accedere o danneggiare un sistema informatico o telematico protetto da misure di sicurezza ("si procura" o "riproduce"), mentre la seconda punisce coloro che "mettono a disposizione" i mezzi materiali che potrebbero essere utilizzati per mettere in pratica la prima condotta ("procura ad altri", "comunica" o "consegna")[109].
Nonostante la semplificazione, le condotte sono molteplici ed è opportuno analizzarle nel dettaglio di ognuna così da comprendere anche le modalità con cui il legislatore decise di intervenire sulla questione.
Si inizia con il "procurarsi" che manifesta chiaramente l'azione di colui che riesce a entrare in possesso di qualcosa, in questo caso di un determinato oggetto materiale che possa aiutarlo a mettere in pratica un più grave reato informatico e ciò può avvenire sia tramite l'autoproduzione sia tramite l'acquisto. Questo fa rientrare nella fattispecie non solo i programmi specificatamente creati per compiere una penetrazione o un danneggiamento, ma anche tutti quei tentativi che poi si sostanziano nella riuscita della successiva condotta (come un *hacker* che dopo diversi tentativi di inserimento manuale riesca a trovare la chiave d'accesso per entrare in un computer).
La condotta di "riproduzione" si riferisce semplicemente all'attività di clonazione o copiatura di *password* o chiavi d'accesso che vengano così tenute per essere successivamente utilizzate o rivendute.

[109] Leggasi SALVADORI I., *I reati di possesso*, cit., 7 s.

Molto legata a questa seconda fattispecie è, infatti, la condotta della "diffusione" che si sostanzia nel rendere pubblico uno di questi oggetti materiali mettendolo a disposizione di uno o più persone (in numero indeterminato) attraverso qualsiasi mezzo (un tipico esempio è la pubblicazione dell'informazione in un forum pubblico)[110].

A sua volta affine a quest'ultima è la "comunicazione" che si diversifica solo per il fatto che la diffusione avviene solo tra un numero ristretto e specifico di persone (anche in questo caso, per esempio, con la pubblicazione in un forum ma questa volta a numero chiuso).

La "consegna" specifica una condotta anche più ristretta perché in questo caso la messa a conoscenza avviene attraverso un passaggio ad un determinato destinatario: normalmente la consegna sottintende quasi la presenza di un trasferimento di persona che, però, in questa specifica materia non è richiesta (molto spesso, anzi, la consegna avviene tra due persone che non si sono mai neanche viste di persona come accade nello scambio tra in *hacker* che mette a disposizione un determinato *malware* ed il suo acquirente).

Per finire il legislatore ha, giustamente, ritenuto di dover inserire una "clausola di chiusura" andando a sanzionare la condotta di chi "fornisce" informazioni o comunque indicazioni idonee ad agevolare o a rendere possibile a terzi il conseguimento di mezzi o programmi per poter accedere abusivamente ad un sistema informatico: punita è, quindi, anche la condotta di chi abbia solo scritto i passaggi logici su come arrivare da soli a produrre un determinato oggetto materiale con lo scopo di commettere reati informatici.

Nonostante quanto indicato nella rubrica, tale articolo non punisce la semplice detenzione dei codici o di chiavi per poter perpetrare l'accesso[111]. Una parte della dottrina ha cercato di ricomprendere comunque tale modalità della condotta in

---

[110] Così la intende il nuovo articolo 2-ter, comma 4, lett. b), D.Lgs. n. 196/2003 (modificato dal D.Lgs. n. 101/2018).

[111] Di diverso parere è MANTOVANI F., *Dir. pen*., PS, I, cit., 580, nota 93, che invece richiama la detenzione come presupposto per tutte le condotte richiamate nella fattispecie; di uguale idea è CANNATA S.-COSTALUNGHI D., *Detenzione e diffusione di codici d'accesso a sistemi informatici o telematici (art. 615*-quater*)*, in *I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti*, *Trattato di diritto penale*, PS, IX, diretto da CADOPPI A.-CANESTRARI S.-MANNA A.-PAPA M., Torino, 2011, 553 ss., 555, per i quali l'articolo in questione punirebbe il semplice possesso delle informazioni necessarie per accedere; idem per TIGANO S., *Delitti contro l'inviolabilità del domicilio*, cit., 264.

quella del "procurarsi" ma già dall'analisi etimologica del termine la cosa suona sbagliata[112]. Il "procurarsi", infatti, indica una condotta che è certamente prodromica al possesso: se uno fosse in possesso di un oggetto non dovrebbe certamente procurarselo[113].

Per quanto potrebbe essere possibile che questa sia stata una svista del legislatore si deve applicare il principio di tassatività e quindi ritenere che nella norma non si volesse condannare la condotta di chi si ritrovi in possesso di determinati codici o strumenti per poter compiere un accesso abusivo (non li abbia prodotti né, quindi, abbia fatto in modo di ottenerli) e non voglia utilizzarli per commettere reati informatici. Di per sé questi comportamenti non sono "offensivi" ma rappresentano condotte neutre che vengono sanzionate solo nella misura in cui rientrano nell'ambito di altri elementi costitutivi di determinati reati informatici.

Tali condotte sono preparatorie e comunque successive alla commissione di altri reati, come tale l'articolo 615-*quater* del Codice penale è stato posto a tutela dei beni della riservatezza informatica e indirettamente della sicurezza informatica nel momento in cui si cerca di contrastare la fattispecie di persone che sempre più facilmente possono creare e scambiarsi gli strumenti per compiere attività criminali su internet. Il problema è che queste condotte, probabilmente sulla falsariga dell'articolo 615-*ter* c.p., richiedono una loro "abusività"[114].

Una parte della dottrina ha sottolineato come il legislatore, con questo riferimento, avrebbe voluto suggerire al giudice il dovere di controllare pedissequamente la presenza o meno di cause di giustificazione che potessero dare una spiegazione legittima a queste condotte illecite[115]. Però a una prima lettura ciò sarebbe stato inutilmente ripetitivo poiché la fattispecie già contiene al proprio interno i dovuti elementi per distinguere i fatti penalmente rilevanti da quelli non punibili: uno di questi elementi sarebbe proprio il dolo specifico che richiede che tali condotte

---

[112] A sostegno si è espresso, tra gli altri, D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, cit., 81.

[113] Sempre in riferimento a SALVADORI I., *I reati di possesso*, cit., 7.

[114] FIANDACA G.-MUSCO E., *Dir. pen.*, PS, *I delitti contro la persona*, vol. II, t. 1, 4ª ed., 2019, 297. Si fa riferimento allo stesso elemento già previsto nel delitto di accesso abusivo ad un sistema informatico o telematico.

[115] Così MARINI G., *Delitti contro la persona*, Torino, 2ª ed., 1996, 390-391; MANTOVANI F., *Dir. pen.*, PS, I, cit., 575, per quanto l'accettazione di questa tesi si attesti sulla condivisione della menzione espressa in quanto mette in luce l'illegittimità della condotta; PECORELLA C., *Sub art. 615*-quater *c.p.*, in *Codice penale commentato*, cit., 614 ss., 618; ma anche MAZZACUVA N., *Delitti contro la persona*, cit., 660 s.

siano messe in atto con l'intento di procurarsi un profitto o cagionare un danno, elemento che da solo però non è sufficiente a delineare l'ambito del penalmente rilevante.

Proprio il riferimento a questo aspetto consente di affrontare, seppur brevemente, l'argomento principale della presenta trattazione, ovverosia l'utilizzo dei *dual use software* e la loro possibile incriminazione.

Accade infatti continuamente che i tecnici del settore IT creino loro stessi o paghino altri soggetti per entrare in possesso di *software* che gli consentano di eseguire i così detti "*penetration test*" e aumentare in questo modo il livello di sicurezza dell'azienda presso cui operano. Ci si rende rapidamente conto di come questa condotta rientri perfettamente all'interno della fattispecie di cui all'articolo 615-*quater* del Codice penale ed è proprio per evitarlo (non turbando così quel processo di condotta virtuosa atta proprio ad elevare il proprio *standard* di sicurezza) che bisogna far affidamento e sottolineare l'abusività della condotta.

Certo, è ovvio che sarà offensivo il comportamento di colui che produca o fornisca un determinato programma per compiere intrusioni informatiche a una persona che abbia intenti malevoli (*hacker* ecc.) mentre sarà legittima l'attività di questi stessi soggetti nel momento in cui a richiedere la sua assistenza sia un "*system administrator*" così da poter entrare in possesso di un *malware* e simulare un attacco informatico al proprio sistema. Il discrimine si trova proprio nell'abusività della condotta dove il primo agisce senza autorizzazione e il secondo, invece, lecitamente pur ponendosi entrambi con l'intenzione di "cagionare un danno".

L'avverbio così posto ha arricchito la previsione chiarendo il fatto tipico e ponendo il discrimine a partire da termini oggettivi più che rientrare nei sempre vaghi elementi soggettivi[116]. Il giudice non dovrà limitarsi solo a constatare l'assenza o la presenza di cause di giustificazione ma con questa specifica clausola di antigiuridicità speciale il legislatore gli richiede di compiere un passo

[116] Come tale l'agente dovrà essere certamente conscio dell'abusività della condotta dato che nell'oggetto del dolo rientrano elementi di legge che aiutano a dare corpo al precetto normativo. Al riguardo si veda ROMANO M., *Pre-Art. 39/63-64*, in ID (a cura di), *Commentario sistematico del codice penale*, 3ª ed. rinn. e ampl., Milano, 2004, 299 ss., 324.

in più rinviando la punibilità a regole extrapenali o in ogni caso desumibili dal contesto nel quale il soggetto agente ha operato[117].

La domanda che sorgerebbe spontanea, a questo punto, sarebbe come riuscire a distinguere i casi in cui una società produttrice di *software* si metta a produrre un *malware* a "fin di bene" o per scopi illeciti; tuttavia a tale interrogativo si risponderà nella terza e ultima parte di questa trattazione.

1.2.3 Altri elementi della fattispecie

L'oggetto materiale del reato è indicato nella stessa fattispecie dell'articolo ed è costituito da ‹‹codici, parole chiave o altri mezzi idonei›› ad accedere ad un sistema informatico o telematico o da ‹‹indicazioni o istruzioni›› che possano comunque portare a tale finalità.

Occorre però chiarire l'esatto significato di tali espressioni.

I termini "codice" o "parola chiave" si riferiscono a quelle sequenze alfanumeriche (da noi tutti solitamente chiamate "*password*") atte a permettere l'accesso a un sistema informatico o telematico protetto da misure di sicurezza a chiunque ne sia in possesso[118]. Con "altri mezzi idonei", invece, ci si riferisce a una clausola di chiusura molto elastica con cui si vogliono ricomprendere tutti quegli strumenti tecnologici anche non ancora inventati.

In questo modo il legislatore ha tentato di apprestare una tutela contro quella variegata e sempre in evoluzione branca dell'*hacking* che si occupa di innovare continuamente i *software* multifunzionali o multiscopo che permettono di aggirare le misure di sicurezza e consentire l'accesso ad un sistema informatico o telematico (solitamente chiamati "*hacking tool*") così come ad altri supporti anche fisici che possano essere utilizzati con la stessa finalità (come eventuali tessere magnetiche)[119].

---

[117] PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, n. 2, 2005, 189 ss., 197.

[118] Leggasi PECORELLA C., *Diritto penale dell'informatica*, cit., 365.

[119] Cfr. SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei* dual-use software, in *Riv. it. dir. e proc. pen*., 2017, 747 ss.

In questa ampia definizione finiscono anche le schede informatiche (*smart-cards, pic-cards* ecc.) che permettono l'accesso a un determinato abbonamento attraverso il loro inserimento in un determinato *hardware* ricevitore e che solitamente vengono "crackate" per permettere l'utilizzo gratuito di un servizio altrimenti a pagamento. Vi ricadono anche i codici alfanumerici con cui solitamente si proteggono i dispositivi elettronici mobili (comunemente chiamati "*pin*") sia da eventuali accessi che da penetrazioni all'interno della propria *sim*: insomma, se c'è un mezzo di sicurezza apposto a un determinato sistema elettronico qualsiasi modo illecito utilizzato per aggirarlo rientrerà in questa fattispecie.

Nel termine conclusivo di ‹‹indicazioni o istruzioni idonee al predetto scopo›› rientrano tutte le informazioni che vengono condivise e che permetterebbero anche ad soggetti non esperti di poter mettere in pratica quelle azioni che facilitano o permettono di aggirare o eludere misure di sicurezza: vi rientra quell'insieme di condotte che sempre di più sono fiorite negli ultimi anni su molti *social network* (primo fra tutti *Reddit* seguito da *4chan*) e che vedono veri e propri *tutorial* su come fare o racconti riguardanti determinate "imprese" compiute da altri utenti e che vengono spiegati nei minimi dettagli e resi disponibili a chi sia interessato.

Chiaramente, per evitare di andare a punire qualsiasi "istruzione" fornita, il legislatore ha richiesto che la descrizione dell'oggetto materiale del reato contenga anche l'"idoneità" di questa condotta a suggerire come penetrare all'interno di un sistema informatico o telematico[120].

In precedenza, si è già anticipato come questo delitto sia punibile a titolo di dolo specifico: è necessario quindi che chi lo realizza agisca con la finalità di procurarsi un profitto o per cagionare un danno.

Il profitto che si vuole conseguire deve essere per sé o per altri ma ci si potrebbe giustamente domandare cosa possa essere considerato "profitto". Di solito consiste in somme di denaro ma non necessariamente, potendo anche avere natura non patrimoniale: si pensi ad esempio a colui che attua sul *Dark-web* uno scambio

[120] Per una più ampia trattazione della materia sia permesso rimandare *infra* al capitolo III di questo stesso scritto e a SALVADORI I., *Il diritto penale dei* software *"a duplice uso"*, in WENIN R.-FORNASARI G. (a cura di), *Diritto penale e modernità*, Napoli, 2017, 361 ss., 399.

di *malware* tra due *software* house al fine di far entrare entrambe in possesso di un *malware* di cui hanno bisogno per commettere un determinato crimine informatico.

Si è già detto come la previsione del dolo specifico, almeno per parte della giurisprudenza, avrebbe la funzione di delimitare quei comportamenti che sono legittimi da quelli che sono invece illeciti. Un esempio spesso riportato a favore di questa tesi è quello del tecnico a cui si consegna il computer con i codici di accesso per permettergli di eseguire una diagnostica di sistema: finché il tecnico si limita a svolgere il lavoro, *nulla quaestio*, ma nel momento in cui dovesse cominciare ad agire per suo profitto o in mio danno usando il computer per commettere reati informatici allora rientrerebbe in questa fattispecie di reato.

Tale formulazione è corretta anche se non del tutto centrata perché tiene conto del dolo specifico ma non del vero elemento sotteso e caratterizzante, l'abusività: si era dato il proprio permesso al tecnico di utilizzare il computer personale per compiere una diagnostica, qualsiasi sua attività che si discosti dall'accordo che lo aveva visto autorizzato ad agire risulterà essere illecito.

Ancora prima dell'elemento soggettivo, dunque, l'illegittimità è da rintracciarsi in un elemento oggettivo: la mancanza di autorizzazione. Il riferimento al dolo specifico ha qui, quindi, un altro significato che è da ritrovarsi nel fatto che la condotta del soggetto agente debba essere offensiva, poiché non solo si va contro la volontà del titolare dell'*ius excludendi* ma si agisce, volontariamente, per ottenere un profitto o cagionare un danno[121].

Il reato si consuma nel momento in cui il soggetto agente entra in possesso dei mezzi capaci di fargli eludere le misure di sicurezza o nel momento in cui le mette a disposizione o dà suggerimenti su come fare ad aggirarle. È una condotta prodromica alla commissione di molti altri reati informatici che ha l'obiettivo di anticipare non poco la tutela del bene giuridico della riservatezza informatica e, indirettamente, della sicurezza informatica[122].

---

[121] Così facendo non si sostiene la tesi di PLANTAMURA V., *Domicilio e diritto penale*, cit., 217, per il quale l'articolo 615-*quater* c.p, con il dolo specifico, avrebbe finito per far rientrare la norma nell'ambito della tutela anticipata del patrimonio.

[122] PECORELLA C., *Diritto penale dell'informatica*, cit., 371 s. ha affrontato la materia e trattato il dubbio riguardante l'illegittimità costituzionale di questa fattispecie per l'eccessiva anticipazione della tutela penale

In quanto reato di pericolo indiretto è, quindi, da escludere l'ammissibilità del tentativo (perché sarebbe un tentativo di tentativo)[123].

Così come il delitto precedente anche l'articolo 615-*quater* c.p. al secondo comma prevede delle circostanze aggravanti. In questo caso sono due e si rifanno al comma quarto dell'articolo 617-*quater* del Codice penale.

La prima contempla l'aumento della reclusione (da 1 a 5 anni di carcere) nel considerare l'evento prodromico più grave a causa del tipo di strumenti o mezzi di cui si sia entrati in possesso o che si siano messi a disposizione o che siano stati suggeriti nel momento in cui questi permetta l'accesso a sistemi informatici usati dallo Stato o da un'impresa esercente un servizio pubblico o pubblica utilità (tale accesso mette a rischio e danneggia l'intera comunità e la sua preparazione è, dunque, considerata più grave).

Identico aumento di pena è previsto per la seconda fattispecie aggravata andando, questa volta, a porre il discrimine sul soggetto agente che è rappresentato da un "agente pubblico" (da intendersi come pubblico ufficiale o incaricato di pubblico servizio) "con abuso dei suoi poteri o con violazione dei suoi doveri ovvero con abuso della qualità di operatore di sistema". Tale aggravante si giustifica, anche in questo caso, con la maggiore gravità che si attribuisce al comportamento di soggetti che svolgono un servizio per la collettività e che, per loro qualifiche, si ritrovano spesso in possesso di informazioni e dati particolarmente sensibili compresi di taluni utilizzabili per penetrare all'interno di sistemi informatici o telematici (spesso anche questi pubblici).

1.2.4 Struttura del reato e bene giuridico

Si è già detto che il delitto di cui all'articolo 615-*quater* c.p. si configura come un reato di pericolo indiretto[124] poiché punisce semplicemente, per esempio, la

[123] Pacifico al riguardo MANTOVANI F., *Dir. pen*., PS, I, cit., 581. Contrario, invece, FLOR R., *Sub art. 615*-quater *c.p.*, in FORTI G.-SEMINARA S.-ZUCCALÀ G. (a cura di), *Commentario breve al codice penale*, 6ª ed., Milano, 2017, 2133 ss., 2134, per il quale il tentativo è configurabile nel momento in cui il soggetto attivo esegua atti idonei e diretti a copiare *password* e codici d'ingresso.

[124] Al riguardo PECORELLA C., *Sub art. 615*-quater *c.p*., cit., 615, per il quale non si potrebbe parlare assolutamente se non di "pericolo indiretto"; idem CANNATA S.-COSTALUNGHI D., *Detenzione e diffusione di codici d'accesso*, cit., 555; TIGANO S., *Delitti contro l'inviolabilità del*

condotta di una persona che si procuri un *malware* con l'intenzione di utilizzarlo per intercettare delle informazioni al fine di rivenderle per profitto personale. Chiaramente, però, per far sì che il profitto venga realmente percepito sarà necessaria una condotta in più, quella di utilizzare il *malware* per spiare davvero il contenuto di informazioni che vengano scambiate da altri due soggetti tramite internet e poi trovare un acquirente a cui interessi davvero acquistare ciò che è stato sottratto così che si possa ricevere il tanto sperato denaro che ha mosso la propria originale condotta. Tra il fatto di procurarsi un *malware* capace, però, di permettere una simile azione e l'offesa al bene giuridico che vuole essere tutelato è necessario che si compia anche altre condotte. Dunque, la situazione che vede un soggetto in possesso di un simile *malware* rappresenta semplicemente il pericolo del pericolo dell'offesa al bene giuridico della riservatezza informatica (ed indirettamente della sicurezza informatica in generale).

È presente anche un'altra tesi che vede il bene giuridico tutelato rappresentato dalla stessa riservatezza di una *password* d'accesso scambiata o nel possesso del *software* malevolo ma tale ipotesi non pare particolarmente convincente[125]. È vero, infatti, che nel primo esempio la *password* può giustamente essere equiparata ad un dato personale così come indicato dall'articolo 4 del Regolamento (UE) 2016/679[126] ma allo stesso tempo ben più facilmente e correttamente, in questo caso, potrebbe essere applicata la tutela in materia di dati personali nel caso in cui venisse utilizzata in modo illecito. Allo stesso tempo questo tipo di garanzia si andrebbe a mal conciliare con la condotta costituita dal fornire ‹‹indicazioni o istruzioni idonee›› che non per forza hanno come oggetto dati o informazioni riguardanti la sfera personale. Ancor meno potrebbe sposarsi questa tesi se il *malware* ottenuto fosse utilizzato per intercettare delle informazioni personali tra due altri sistemi visto che un *software* non è certamente un'informazione personale.

---

domicilio, cit., 263 s. Per MANTOVANI F., *Dir. pen.*, PS, I, cit., 580, si tratterebbe invece di un "reato di sospetto"; allo stesso modo la pensa FUMO M., *La condotta nei reati informatici*, in *Arch. Pen*., 2013, 771 ss., 781 s., per quanto quest'ultimo equipara l'articolo 615-*quater* c.p. al reato di sospetto all'articolo 707 c.p. basandosi sull'erroneo pensiero che la fattispecie punisca anche il "mero possesso" come presupposto del reato. Per Trib. Milano 10.10.2000, in Foro Ambr., 2000, 474, si tratterebbe invece di un reato di pericolo astratto.

[125] La tesi è sostenuta da PICA G., *Diritto penale*, cit., 81.

[126] Il già nominato in precedenza "GDPR", riguardante la materia dei dati personali. Vedasi *supra*, capitolo I.

La volontà del legislatore, per concludere, non era altro che quella di tutelare in modo molto anticipato il bene giuridico della riservatezza informatica e, dunque, in maniera mediata anche quella della sicurezza informatica cercando di rendere più difficile il procurarsi strumenti con cui ledere questi aspetti.

1.3 L'articolo 615-*quinquies* c.p.

Tale articolo punisce con la reclusione fino a due anni e con la multa fino a euro 10.329 ‹‹chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici››.
Il posizionamento di questo articolo nei delitti contro l'inviolabilità del domicilio è stato un errore dovuto alla presenza dell'articolo 615-*quater* c.p. di cui questa norma costituisce quasi una continuazione e un'espansione a livello di contenuto. Al pari dell'articolo precedente, infatti, questa fattispecie ha rappresentato un'innovazione in campo europeo andando a coprire e trattare la materia dei reati informatici in senso stretto nel 1993, quando a livello sovranazionale i primi riferimenti sono da ricercarsi solo a partire dalla Convenzione *Cybercrime* e nella Direttiva 2013/40/UE, quando si richiese agli Stati membri di andare a reprimere il così detto "abuso di dispositivi" (*misure of device*) ed in particolare di tutti quei programmi che veniva utilizzati per compiere danneggiamenti di dati o di sistemi informatici.
Se l'articolo 615-*quater* c.p. era stato pensato per reprimere soprattutto condotte preparatorie alla commissione dei reati d'accesso abusivo (articolo 615-*ter* c.p.), invece, l'articolo 615-*quinquies* c.p. cerca di sanzionare tutte quelle azioni preparatorie al danneggiamento di dati, informazioni o programmi informatici (articoli 635-*bis* e 635-*ter* del Codice penale) o a sistemi informatici o telematici (635-*quater* e 635-*quinquies*).

Nella versione del 1993 l'articolo 615-*quinquies* puniva le condotte di diffusione, comunicazione o consegna di un programma informatico "avente scopo o per effetto" il danneggiare dati o sistemi informatici. Già ad una prima lettura si può vedere un'ulteriore differenza abbastanza marcata con l'articolo immediatamente precedente e cioè il fatto che vengano punite solamente le condotte di creazione e diffusione, non anche quelle che indichino semplicemente come procurarsi o creare da sé quei programmi malevoli capaci di danneggiare un computer (e probabilmente la ragione sarebbe da ricercare semplicemente in una svista del legislatore stesso)[127]. Dopo la riforma attuata con la legge 48/2008 (la legge di ratifica della Convenzione *Cybercrime*) si è posto rimedio a questa situazione, riavvicinandosi all'elevato *standard* di tutela contenuta nell'articolo 615-*quater* c.p. (ad oggi il *malware*, in maniera decisamente più variegata, può essere "procurato", "prodotto", "riprodotto" o "importato").

Sempre nella sua formulazione originaria l'oggetto materiale del reato era riassunto nei programmi "aventi scopo o per effetto" il danneggiamento di dati o sistemi informatici altrui (che però era anche l'evento indipendentemente punito nell'articolo 635-*bis* c.p. anteriforma della legge 48/2008)[128].

Quanto ai *dual use software* si rimanda allo specifico capitolo conclusivo l'analisi delle modalità attraverso cui è stato possibile escludere tali programmi dalle maglie di questa fattispecie, tuttavia già da un primo sguardo si può comprendere quanto, soprattutto prima della riforma del 2008, la condotta non era chiara sul punto: prima di tutto, "avente lo scopo" non è una definizione limpida perché comporta che il *software* sia stato creato con questa finalità[129]; ancor peggio se ci si sofferma sul successivo richiamo "all'effetto" che ricomprende al suo interno, indistintamente, tutti i programmi che possono essere la causa di un danneggiamento informatico a prescindere dalla ragione per cui sono stati pensati e per cui li si voglia utilizzare.

---

[127] PICOTTI L., *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, 6, 700 ss., 708, evidenzia giustamente che la mancata incriminazione di queste azioni vada contro la stessa natura di reato d'ostacolo punito dall'articolo 615-*quinquies* c.p.

[128] PECORELLA C., *Diritto penale dell'informatica*, cit., 245 ss.

[129] SALVADORI I., *Criminalità informatica*, cit., 758 ss.

Si è già detto come la legge 48/2008 abbia modificato l'articolo in analisi per adattarlo alla matrice europea della Convenzione *Cybercrime* a partire dall'oggetto del reato che ora è costituito da "apparecchiature, dispositivi o programmi informatici" anche se, ancora una volta, non è ben chiaro se questi debbano essere stati creati con il principale intento di danneggiare dati o programmi informatici altrui per rientrare nel novero della punibilità del reato in questione.

Leggendo questo articolo non si scorge l'offensività e non si individua immediatamente né nell'oggetto materiale né tantomeno nelle condotte che sono neutre da un punto di vista oggettivo, mentre assumono rilievo unicamente in base alla specifica finalità che deve sorreggere il fatto base. Senza un'offensività oggettiva[130] tutto dipenderebbe dalla volontà di colui che, per esempio, fornisce il programma, tuttavia, così facendo rientrerebbe nel novero delle persone punibili anche quello stesso tecnico che consegna un *malware* ad un'azienda per permetterle di fare un *penetration test*, poiché il soggetto agente sarebbe a conoscenza che tale *software* verrebbe utilizzato per eseguire un "lecito" danneggiamento (sebbene controllato e voluto).

Si è cercato di porre rimedio a questa situazione concentrandosi sull'elemento soggettivo del reato richiedendo un dolo specifico: nel consegnare o rendere disponibile un *software* che potrebbe avere un "doppio uso" il disvalore deriva dal fine specifico di voler danneggiare un sistema informatico o telematico in modo illecito[131]. Ancora una volta questa illiceità deve essere letta – ma il discorso verrà ampliato nel capitolo conclusivo come già annunciato – dall'abusività che anche in questo caso viene chiamata a risolvere ipotesi non propriamente semplici da risolvere.

Il reato, come i precedenti, si consuma quando il soggetto agente entra in possesso di questa tipologia di apparecchiature, dispositivi o programmi informatici oppure li mette a disposizione di terzi. Esattamente come nell'articolo 615-*quater* c.p. anche questo delitto rappresenta un reato di pericolo indiretto anticipando di

[130] SALVADORI I., *Criminalità informatica*, cit., 764.

[131] Si noti come si stia trattando di "reati composti" dove l'oggetto del dolo specifico sorregge anche il fatto-base. Al riguardo si faccia riferimento a MORGANTE G., *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Torino, 2013, in particolare 10 ss., 58 ss.

molto la tutela del bene giuridico della riservatezza informatica (e indirettamente della sicurezza informatica). Per questa ragione il tentativo non è contemplato.

2.0 Le intercettazioni informatiche e telematiche

Sulla falsariga degli articoli precedenti, il legislatore ha continuato a inserire reati informatici affiancandoli a delitti già precedentemente contemplati. L'articolo 6 della legge 547/1993, in particolare, ha avvicinato ai "delitti contro l'inviolabilità dei segreti" tre nuove fattispecie tese a punire "l'intercettazione, l'impedimento o l'interruzione di comunicazioni informatiche o telematiche" (articolo 617-*quater* c.p.), l'installazione di apparecchiature atte a compiere le precedenti ipotesi di condotta (articolo 617-*quinquies* c.p.) così come la "falsificazione, l'alterazione o la soppressione del loro contenuto (articolo 617-*sexies* c.p.).

A ben vedere, questa classificazione e il contenuto degli articoli ricalca da vicino la legge 98/1974 e le disposizioni introdotte a tutela della riservatezza delle comunicazioni e delle conversazioni telefoniche o telegrafiche "tra persone" e che si credeva non potessero essere applicati alle comunicazioni "tra sistemi". Così facendo il legislatore riteneva di rimuovere qualsiasi eventuale dubbio ermeneutico senza però andare ad aggiornare il contenuto di articoli del 1974 alle nuove tecnologie della comunicazione.

Con una simile considerazione si possono anticipare tutti i problemi interpretativi e di applicazione che si sono susseguiti nel corso del tempo man mano che le modalità di comunicazione a distanza si facevano sempre più complesse e diversificate. Il problema più grande si è manifestato a livello interpretativo riguardo agli elementi costitutivi dei reati informatici che non è sempre così facile applicare ai "mezzi materiali" di nuova invenzione.

La complessa formulazione della fattispecie è, oltretutto, spesso causa di conflitto interno con altre norme, soprattutto con quelle del danneggiamento informatico *ex* articolo 635-*bis* e successivi del Codice penale, la cui ampiezza applicativa è spesso discussa e varia a seconda della situazione nonché dell'interpretazione giurisprudenziale della norma. In particolare, il problema precedente, già presente in relazione all'accesso abusivo ad un sistema informatico o telematico (articolo

615-*ter* c.p.), diventa ancora più grave proprio nel caso dei reati posti a tutela della "corrispondenza" informatica o telematica contenuti negli articoli 617-*quater* e successivi del Codice penale e la cui nozione è stata ad oggi equiparata dall'estensione dell'articolo 616 cpv., c.p., a quella di corrispondenza epistolare, telegrafica e telefonica.

Tali articoli erano stati posti a tutela delle informazioni che venivano scambiate tra due apparecchiature elettroniche e dunque "in fase di trasmissione", come poteva essere l'invio di un documento[132]: l'obiettivo non era tanto quello di tutelare la riservatezza dell'informazione inviata, quanto la sicurezza generale del collegamento creato tra i due computer per scambiare quel determinato dato[133]. L'oggetto materiale, invece, degli articoli 616 e 619 del Codice penale è quello di salvaguardare la segretezza del contenuto della comunicazione che può essere scambiata in modo cartolare o a mezzo internet, dunque i veri e propri "messaggi" che sono personali e riservati e che rappresentano il rapporto comunicativo tra due o più persone[134].

Come si spiega, dunque, la differenza di pena tra queste norme con una maggiore gravità di quelle previste agli articoli 617-*quater* c.p. e seguenti? La risposta si trova nel fatto che una lettera cartacea è un mero supporto, un foglio di carta che viene affidato alla segretezza di una busta posta e spedita nella speranza che il servizio postale rechi al destinatario la lettera a lui specificatamente inviata. Una "comunicazione" tra "sistemi informatici o telematici", invece, è delineata da una semplicità e una velocità di conversazione dovute al fatto che il contenuto di una *e-mail*, per esempio, viene criptato e trasformato in un linguaggio informatico che poi il computer ricevente decripterà per riportarlo ad un linguaggio intellegibile all'essere umano. In altri termini, un computer conserva nella sua memoria quanto viene in lui inserito sotto forma di linguaggio digitale, per questo si è ritenuta più grave la condotta di chi si intrometta all'interno di questa complessa operazione

---

[132] PECORELLA C., *Diritto penale dell'informatica*, cit., 303.

[133] In contrasto c'è PECORELLA C., *Reati informatici*, in *Enc. Dir*., Annali, X, Milano, 2017, 707 ss., cit., 717 per il quale tutte le norme elencate, tenendo presente della loro collocazione all'interno del nostro ordinamento, dovrebbero comunque riguardare trasmissioni contenenti qualcosa di interpersonale.

[134] PICOTTI L., *Commento art. 5 l. n. 547/1993*, in *Legislazione pen*., n. ½, 1996, 109 ss., 115, si era già espresso riguardo alla possibilità di separare le fattispecie con oggetto la "corrispondenza" informatica da quelle che, invece, riguardano il più ampio concetto di "comunicazioni informatiche o telematiche)

nella quale è possibile, con le giuste conoscenze, sottrarre facilmente informazioni in modo non autorizzato per gli scopi più vari (con la necessità di tutelare, come al solito, l'interesse super-individuale alla riservatezza e alla sicurezza delle telecomunicazioni).

2.1 L'articolo 617-*quater* c.p.

L'articolo 617-*quater* c.p. punisce, con la reclusione da sei mesi a quattro anni, ‹‹chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe››. Allo stesso modo viene punito anche ‹‹chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma››. Per completezza la disciplina è stata ampliata ed estesa anche a ‹‹qualunque altra trasmissione a distanza di suoni, immagini o altri dati›› da parte dell'articolo 623-*bis* del Codice penale così da ricomprendere qualsiasi scambio di informazioni.

2.1.1 La condotta tipica e la fraudolenza

L'obiettivo di questo articolo è quello di punire la condotta di chi intercetta in maniera fraudolenta delle comunicazioni informatiche o telematiche o che, comunque, opera per impedirle o interromperle in qualche modo. Per definire cosa si intenda per "intercettare" possiamo rivolgerci direttamente ad un ampio settore dottrinale per il quale tale azione coincide con quella di prendere conoscenza di cosa contengano comunicazioni informatiche o telematiche[135]. Ciò avviene nel momento in cui tale trasmissione viene realizzata, intromettendosi fraudolentemente.

[135] Così si esprime RINALDI R., *Commento art. 6 l. 23/12/1993 (Criminalità informatica)*, in *Legislazione pen*., n. 1/2, 1996, 118 s.; PICA G., *Diritto penale*, cit., 176; PECORELLA C., *Sub art. 617*-quater *c.p*., cit., 672; LOTTINI R., *I delitti contro l'inviolabilità dei segreti, in I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti*, *Trattato di diritto penale*, PS, IX, diretto da CADOPPI A.-CANESTRARI S.-MANNA A.-PAPA M., Torino, 2011, 573 ss., 643.

Bisogna, in questo caso, anche considerare la valenza di quanto detto dalla dottrina minoritaria maggiormente ligia all'interpretazione letterale del testo della legge e dell'oggetto della condotta: non si esige che si venga a conoscenza del contenuto della comunicazione intercettata come, invece, viene espressamente richiesto per l'articolo 617 c.p. per quanto riguarda le comunicazioni e conversazioni telegrafiche o telefoniche ma si ritiene sufficiente la semplice intercettazione fraudolenta[136]. Anche in questo caso il legislatore si è posto in modo tale da non porre al centro la tutela del contenuto quanto, piuttosto, della comunicazione in quanto tale.

Per considerare la condotta come offensiva e rientrante in questa fattispecie di reato è bastevole che il soggetto agente sia riuscito a entrare in possesso di informazioni, dati o *files* che rappresentano l'oggetto attuale della comunicazione tra due "sistemi informatici" e che, normalmente, per tornare comprensibili all'uomo hanno bisogno d'essere decriptati da un elaboratore elettronico con un *software*[137]. Se, infatti, il legislatore avesse voluto tutelare il contenuto dei pacchetti informativi e non questi ultimi in quanto tali, avrebbe espressamente previsto, come avviene nel comma 2 dell'articolo 617-*quater* del Codice penale, un chiaro riferimento al "contenuto delle comunicazioni"[138].

La volontà, si potrebbe notare, di mettere in atto questa specifica forma di tutela pone le sue radici nella necessità di arretrare la punibilità nel tempo così come ricomprendere all'interno della fattispecie determinate condotte che, in caso contrario, sfuggirebbero alle maglie della norma (come, per esempio, il caso di sequestro di pacchetti di dati con l'intenzione di chiudere un riscatto in cambio della restituzione o per rivenderli senza saperne il contenuto).

L'intercettazione, come azione, è una condotta a forma libera che può avvenire nei modi più disparati a patto che si utilizzi un sistema informatico o telematico e che ciò non vada a confliggere con la ricezione di tali informazioni da parte del

---

[136] Vedasi MANTOVANI F., *Dir. pen*., PS, I, cit., 647, che sottolinea come il testo dell'articolo 617-*quater* c.p. punisca espressamente l'intercettazione e non la conoscenza del contenuto come, invece, richiesto dall'articolo 617 c.p.

[137] RELLA R., *Art. 617-617-quater c.p.*, in MANNA A. (a cura di), *Reati contro la persona*, Torino, 2007, 870 ss., 874; allo stesso modo PICOTTI L., *I reati informatici*, cit., 23.

[138] PICOTTI L., *Commento art. 5 l. n. 547/1993*, cit., 109 ss., che per tutti ha trattato esaustivamente la questione della ‹‹corrispondenza›› come intesa dall'articolo 616, comma 4, c.p. e che il legislatore ha applicato anche a quella informatica e telematica.

suo destinatario. In caso contrario, infatti, non vi sarebbe intercettazione ma le condotte comunque previste ed alternative dell'"impedimento" e dell'"interruzione"[139]. Per l'esattezza, "impedire" significa andare a ostacolare l'invio o l'inizio della trasmissione di dati tra due sistemi informatici mentre l'interruzione si posiziona nel caso opposto, cioè quando il processo di trasferimento sia iniziato ma la fraudolenta intromissione impedisca il corretto ricevimento dei dati inviati (entrambe le condotte restano, comunque, a forma libera).

Si è già toccata la questione del comma secondo dell'articolo 617-*quater* c.p. quando si è trattato della conoscenza del contenuto delle comunicazioni informatiche o telematiche. In questo specifico caso si ritiene offensiva la condotta di colui che, entrato a conoscenza di determinate comunicazioni avvenute a mezzo internet (dunque non necessariamente frutto di una precedente intercettazione, eventualmente essendone entrato in possesso anche in modo casuale[140]) ne riveli la natura o il contenuto al pubblico: tale ipotesi, più che tutelare la sicurezza delle comunicazioni, si pone l'obiettivo di impedire o punire l'azione di coloro che rendono pubbliche informazioni pensate per essere private.

In ogni caso, per quanto riguarda la condotta di "intercettazione" contenuta nel comma 1 dell'articolo in questione, questa richiede il carattere della "fraudolenza" per vedere perfezionata la fattispecie criminale. Con questo termine il legislatore ha voluto punire la condotta di chi, a distanza e con strumenti capaci di nascondere la sua presenza, riesca a inserirsi insidiosamente all'interno del processo di comunicazione tra due sistemi informatici o telematici in modo da carpire lo scambio di informazioni[141].

Altra parte della dottrina, questa volta seguita maggiormente anche dalla giurisprudenza, ha adottato un'altra interpretazione al fine di ampliare la sfera di offensività di questa fattispecie: il concetto di "fraudolenza" non dovrebbe

---

[139] Così sia PICA G., *Diritto penale*, cit., 176; che PICOTTI L., *I reati informatici*, cit., 23.

[140] Cfr. Trib. Milano 12.4.2002; in *Giur. di Merito*, 2003, 737 ss.

[141] In dottrina, PICA G., *Diritto penale*, cit., 177. Analogamente in giurisprudenza si faccia riferimento a Cass. pen., sez. V, 30.1.2015, n. 29091; Cass. pen., sez VI, 5.5.2016, n. 18713. Della stessa idea ma ritenendo, in senso più restrittivo, che il soggetto attivo debba agire tramite artifizi o raggiri RINALDI R., *Commento art. 6 l. n. 547/1993*, cit. 120; ma anche PARODI C., *Detenzione abusiva di codici di accesso a sistemi e illecito impedimento di comunicazioni telematiche*, in *Dir. pen. e processo*, 1998, 1149 ss., 1155.

riscontrarsi nella capacità del soggetto agente di nascondere o mascherare la sua identità quanto nella capacità di aggirare i sistemi di sicurezza posti a protezione dei processi di comunicazione[142]. Si ritiene di dover supportare proprio la tesi che non va a dare eccessiva importanza esclusivamente all'intensità del dolo quanto, piuttosto, alla "consapevole volontà" di andare a commettere tale delitto pur essendo a conoscenza dell'insidiosità del mezzo utilizzato (come, per esempio, l'installazione di uno *spyware* di tipo "*keylogger*" che non necessariamente si concentra sull'occultare l'indirizzo del proprio proprietario quanto sull'occultare la sua stessa presenza all'interno del computer su cui si è inserito)[143].

Il carattere della fraudolenza è richiesto soltanto per le "intercettazioni", non invece per le altre due alternative condotte dell'"impedimento" e dell'"interruzione"[144]. Il legislatore ha giustamente ritenuto come offensive queste semplici condotte per quel che sono, senza il riferimento alla fraudolenza, in quanto di per sé stesse capaci di arrecare un grave nocumento alle comunicazioni tra due o più sistemi informatici o telematici. Se si seguisse la tesi minoritaria che, invece, vorrebbe estendere anche a queste condotte il fattore della "fraudolenza" si andrebbero a escludere dal novero delle azioni punibili quelle di impedimento o di interruzione delle comunicazioni informatiche o telematiche attraverso l'utilizzo della violenza "logica" su tutte quelle informazioni interessate dall'azione del soggetto agente[145].

2.1.2 Altri elementi della fattispecie

[142] Cfr. Cass. pen., sez. V, 6.7.2007, n. 31135. Mentre in dottrina si prenda PECORELLA C., *Dirritto penale dell'informatica*, cit., 305, nota 118; PLANTAMURA V., *La tutela penale delle comunicazioni informatiche e telematiche*, in PLANTAMURA V.-MANNA A. (a cura di), *Diritto penale e informatica*, Bari, 2007, 63 ss., 74 s., per il quale l'avverbio sarebbe rivolto solo all'esclusione dei casi in cui l'intercettazione fosse totalmente occasionale.

[143] In giurisprudenza Trib. Milano 12.4.2002, in *Giur. di Merito*, 2003, 737. In dottrina PICA G., *Diritto penale*, cit., 177.

[144] Così PECORELLA C., *Diritto penale dell'informatica*, cit., 305, nota 118. Contra, invece, FONDAROLI D., *La tutela penale dei beni informatici*, in *Dir. informaz. e informatica*, 1996, 291 ss., 316; MARINI G., *Delitti contro la persona*, cit., 419; RINALDI R., *Commento all'art. 6 l. n. 547/1993*, cit., 120; LOTTINI R., *I delitti contro l'inviolabilità dei segreti*, cit., 65; FIANDACA G.-MUSCO E., *Dir. pen*., PS, vol. II, t. I, cit., 307.

[145] PECORELLA C., *Diritto penale dell'informatica*, cit., 305, nota 118.

Come più volte accennato, tutte le condotte devono avere come loro oggetto materiale le ‹‹comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi››. I lavori preparatori alla legge numero 547/1993 rivelano che obiettivo del legislatore, con il riferimento al termine ‹‹comunicazioni relative ad un sistema informatico››, fosse quello di intendere tutti quegli scambi di *files*, dati, informazioni o programmi che provengano o siano diretti ad un elaboratore elettronico[146]. Ad eccezione del comma 2 dell'articolo 617-*quater* c.p. risulta essere irrilevante il contenuto delle informazioni che siano state in questo modo intercettate, interrotte o impedite potendo essere delle più varie: si può andare dal *pin* della carta di credito appreso attraverso l'inserimento in un sito di *phishing* delle proprie credenziali passando per l'apprensione di *password* tramite l'utilizzo di un "*keylogger*" o altri *spyware* della stessa famiglia durante la navigazione in internet. Non è necessario che l'*hacker* o il soggetto attivo in generale sia mosso da un qualche specifico interesse, essendo bastevole il dolo a titolo generico inteso come semplice volontà di carpire fraudolentemente una comunicazione che sta avvenendo tra due o più sistemi informatici o telematici o comunque impedirla o interromperla.

Per quanto riguarda, invece, il comma 2 il dolo rimane generico ma si deve leggere come la cosciente volontà di rivelare ad altri informazioni ottenute da comunicazioni informatiche che si sa essere destinate a restare private (e che quindi, nelle intenzioni originali degli interlocutori erano state pensate per essere riservate). Nulla di sorprendente per quanto riguarda il momento consumativo del reato sia per quanto riguarda le ipotesi di cui al primo sia al secondo comma che vedono il loro perfezionamento nel momento in cui la condotta viene realizzata (con l'intercettazione, interruzione, impedimento o condivisione della comunicazione informatica o telematica).

Per quanto riguarda la condotta di cui al comma 2, quest'ultima può concorrere con quelle di cui al comma 1 se le informazioni rese pubbliche derivino da un'intercettazione informatica o telematica.

[146] Contenuto della presentazione dello schema di progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penale in tema di criminalità informatica, in *Doc. giust.*, 1991, n. 9, 142 ss.

L'articolo 617-*quater* del Codice penale ammette il tentativo per tutte le ipotesi criminose contenute e previste al suo interno[147].

2.1.3 Circostanze aggravanti, struttura e bene giuridico tutelato

Mentre i casi previsti nei commi precedenti sono procedibili a querela di parte, il comma 4 dell'articolo 617-*quater* c.p. prevede tre circostanze aggravanti che non solo determinano la perseguibilità d'ufficio ma che si distanziano anche dalle fattispecie aggravate già previste nell'articolo 617 c.p. per la particolare natura informatica o telematica delle comunicazioni in questione.

Così come per altre ipotesi aggravate esaminate nell'ambito degli altri reati informatici già trattati, la prima circostanza prevede un aggravamento di pena con la reclusione da uno a cinque anni per chi, attraverso la condotta di intercettazione, impedimento o interruzione di comunicazioni tra due o più sistemi informatici o telematici o attraverso la rivelazione al pubblico del loro contenuto, agisca ‹‹in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità››. Non si rivela del tutto corretto il riferimento al "danno" nei confronti dei sistemi sopra descritti poiché non necessariamente un'intercettazione o la pubblicazione del suo contenuto provocano un nocumento direttamente ai sistemi. Decisamente più appropriato sarebbe stato un riferimento alla punizione di condotte rivolte verso sistemi informatici pubblici essendo comunque l'oggetto materiale del reato la fraudolenta captazione della comunicazione in quanto tale.

Anche in questo caso la maggior gravità della pena è da far ricadere sull'importanza della funzione svolta dai sistemi informatici che sono gestiti per servizi pubblici o di "pubblica necessità"[148], nonché sulla delicatezza delle informazioni che possono essere trasferite nel processo tanto da richiedere la garanzia che ciò avvenga assicurando, per quanto possibile, la regolarità, l'autenticità e l'affidabilità del servizio reso.

---

[147] PIERGALLINI C., *I delitti contro la riservatezza e la libertà delle comunicazioni (artt. 617*-ter. *617*-bis, *617*-ter, *617*-quater, *617*-quinquies, *617*-sexies, *621)*, cit., 822 ss. Cass. pen., sez. II, 4.12.2007, n. 45207.

[148] Vedasi gli artt. 358 e 359 c.p. per la definizione di servizio pubblico e servizio di pubblica necessità.

Le stesse ragioni sono alla base dell'applicazione di identico trattamento sanzionatorio nei confronti del soggetto agente che sia un agente pubblico (da leggersi come pubblico ufficiale o incaricato di pubblico servizio) e che attui la condotta abusando dei suoi poteri o violando i suoi doveri o, ancora, abusando della sua qualità di operatore di sistema. La *ratio* alla base di questa circostanza aggravante, soggettivamente qualificata, è da ricercarsi nella maggior facilità con cui la condotta può essere messa in atto da un soggetto che, oltretutto, sarebbe chiamato a svolgere un pubblico servizio avendo maggiori responsabilità ma anche la fiducia da parte della pubblica amministrazione.

La terza circostanza aggravante è diversa dal solito e va a incriminare come maggiormente offensiva la condotta quando realizzata da un esercente la professione di investigatore privato (anche abusivamente). La ragione è da ricercare nel fatto che tali soggetti sono spesso invogliati, nello svolgimento della loro stessa attività, a violare la riservatezza altrui e nel farlo sono facilitati dal possedere comunemente conoscenze tecniche o mezzi per poter realizzare una simile condotta.

Quanto al bene giuridico tutelato, una parte della dottrina ritiene che lo stesso consista nel garantire la libertà delle comunicazioni attraverso una forte riservatezza del relativo contenuto.[149]. In questo caso, però, ci si ritroverebbe davanti ad un reato di danno nel quale la fattispecie di cui all'articolo 617-*quater* c.p. verrebbe richiamata ogni volta che attraverso una delle condotte in essa contenute si venisse a consumare un danneggiamento dell'interesse tutelato. Si ritiene, però, di dover aderire alla posizione di altra parte della dottrina che ritiene tale ipotesi non particolarmente convincente. Ricordiamo, infatti, che l'oggetto materiale del reato non è la riservatezza del contenuto delle comunicazioni (ad eccezione della condotta di cui al comma 2) quanto la tutela dell'integrità del processo che permette a due o più sistemi informatici o telematici di mettersi in comunicazione tra di loro e scambiarsi informazioni non ancora intellegibili per

[149] PICA G., *Diritto penale*, cit., 180; RINALDI R., *Commento art. 6 l. n. 547/1993*; GALDIERI P., *Teoria e pratica*, cit., 119 ss., per il quale l'articolo 617-*quater* c.p. sarebbe posto a protezione della riservatezza delle comunicazioni interpersonali e, dunque, solo in modo mediato tutelerebbe anche la sicurezza informatica. LOTTINI R., *I delitti contro l'inviolabilità dei segreti*, cit., 643. In giurisprudenza si veda Cass. pen., sez. VI, 5.5.2016, n. 18713.

gli esseri umani ma trasferibili da sistema a sistema[150]. L'interesse tutelato è, dunque, da ricercare a monte nella garanzia di un pacifico e libero svolgimento delle funzioni che permettono la comunicazione tra due o più sistemi informatici o telematici in modo da consentire lo scambio di documenti, *files* o informazioni tra i vari utenti e, dunque, solo indirettamente la loro riservatezza[151].

2.2 L'articolo 617-*quinquies* c.p.

Con l'articolo 6 della legge numero 547/1993 si è introdotto nel Codice penale l'articolo 617-*quinquies* che prevede la pena della reclusione da 1 a 4 anni per chi ‹‹fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad una sistema informatico o telematico ovvero intercorrenti tra più sistemi››.
Essendo un delitto particolarmente vicino e simile al precedente, si è prevista una pena maggiorata (la reclusione da 1 a 5 anni) per le stesse circostanze previste al comma 4 dell'articolo 617-*quater* c.p[152].
Leggendo la fattispecie si comprende fin da subito che essa ricalchi le condotte di cui all'articolo precedente ma ponendosi a tutela di una condotta prodromica rispetto ad esse: quella dell'utilizzo o dell'installazione di apparecchiature o *software* che possano intercettare, impedire o interrompere la comunicazione attuata tramite sistemi informatici o telematici.
La paura del legislatore nei confronti dei mezzi e degli strumenti capaci di realizzare una simile condotta, e ad oggi sempre più facilmente reperibili, si manifesta nella non particolarmente logica previsione di una pena maggiore (anche nel minimo) rispetto a quella prevista dall'articolo 617-*quater* che punisce chi fraudolentemente intercetta, interrompe, impedisce o rivela al pubblico le stesse informazioni.

---

[150] PIERGALLINI C., *I delitti contro la riservatezza e la libertà* delle *comunicazioni (artt. 617*-ter. *617*-bis, *617*-ter, *617*-quater, *617*-quinquies, *617*-sexies, *621)* cit., 838, per il quale il punto focale della disposizione è assicurare l'affidabilità e l'autenticità sia al contenuto che al destinatario delle comunicazioni informatiche o telematiche, così come il regolare funzionamento dei sistemi informatici e telematici.
[151] CORASANITI G., *La tutela della comunicazione informatica*, cit., 120-121; BERGHELLA F.-BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in Cass. pen., 1995, 2329 ss., 2333.
[152] Vedi *supra*, capitolo II, paragrafo 2.0.5.3.

2.2.1 La condotta e l'oggetto materiale del reato

La condotta richiesta, in realtà, è particolarmente semplice e lineare: si realizza con l'installazione di uno strumento o un programma che sia idoneo a permettere successivamente l'intercettazione, l'impedimento o l'interruzione delle comunicazioni tra sistemi informatici o telematici, indipendentemente dal loro successivo utilizzo.

Per fare un esempio, l'installazione su un computer di uno *spyware* che possa captare le comunicazioni inviate tramite *e-mail* anche se, nella realtà fattuale, il proprietario di quell'elaboratore elettronico non possegga alcun indirizzo di posta elettronica. In questo caso il *discrimen* tra un comportamento lecito e uno lecito non è da ritrovarsi nella mancanza di autorizzazione o nella finalità lesiva del fatto base quanto, semplicemente, dalla clausola che prevede automaticamente l'illiceità di qualsiasi condotta di questo tipo posta in essere ‹‹fuori dai casi consentiti dalla legge›› (che il legislatore ha ripreso dalla fattispecie dell'articolo 617-*bis* del Codice penale, norma gemella riguardante le comunicazioni o le conversazioni telegrafiche o telefoniche).

Chiaramente l'originale intento del legislatore era quello di scriminare eventuali intercettazioni attuate dall'autorità giudiziaria e previste dalla legge numero 98/1974, inserendo un uguale strumento anche per quanto riguarda il mondo delle comunicazioni digitali sempre più soggetto all'azione di controllo successivo da parte delle autorità di polizia autorizzate dall'autorità giudiziaria (captatori elettronici come *trojan horse* o *spyware* si usano spesso per tracciare l'attività criminale di soggetti già conosciuti alla legge). Nonostante questo, il pericolo è che, interpretando in modo letterale la legge numero 547/1993 per quanto riguarda l'articolo 617-*quinquies* del Codice penale, si vada ad allargare eccessivamente il novero di condotte che si troverebbero a essere incluse nella fattispecie. Vi rientrerebbero, per esempio, alcune ipotesi prive di disvalore penale come l'installazione di programmi di controllo sui proprio dispositivi di lavoro da parte di un "*system administrator*" per monitorare il corretto funzionamento di un sistema aziendale o *software* utilizzati da parte dei genitori per tenere sotto

controllo l'attività dei figli minorenni su internet. Sarebbe dunque stato più opportuno seguire l'esperienza della Convenzione *Cybercrime*, modificando la norma come accaduto per altre già presenti nel nostro ordinamento penale con l'introduzione dell'avverbio "abusivamente" o "senza autorizzazione".

L'oggetto materiale del reato, come già sottolineato, è rappresentato da tutte quelle "apparecchiature" che possono essere utilizzate per intercettare, impedire o interrompere "comunicazioni informatiche o telematiche". Il novero, però, di tale tipologia di "apparecchiature" è molto vasto e lo diventa sempre di più con il passare degli anni. Vi potrebbero rientrare, infatti, sia gli "apparecchi" in senso stretto (gli *hardware*) sia una vasta gamma di *software* solitamente chiamati "*spyware*" (sniffers, *keylogger*, *spyware*, skimmer, *trojan horse* ecc…) che una volta installati senza autorizzazione nel sistema informatico o telematico dell'utilizzatore rendono possibile l'accesso remoto o la captazione delle informazioni in entrata o in uscita.

Non è necessario che queste "apparecchiature" siano poi utilizzate ma è sufficiente che siano in grado di produrre l'evento lesivo del reato, che siano cioè oggettivamente idonee a tale scopo: il loro essere "atte ad intercettare" dovrà essere valutato di volta in volta dal giudice in concreto.

2.2.2 Gli altri elementi della fattispecie del reato

Passiamo ora a trattare l'elemento soggettivo del reato che è rappresentato da un dolo generico: si richiede, semplicemente, la conoscenza delle capacità dell'apparecchiatura (in grado di compiere le condotte di cui al comma 1 dell'articolo 617-*quater* c.p.) e che volontariamente si vada ad installare la stessa all'interno di un sistema informatico o telematico[153].

Una parte della dottrina, però, sostiene che il dolo sarebbe specifico e non generico: l'installazione dell'apparecchiatura ha la specifica finalità di intercettare, impedire o interrompere le comunicazioni informatiche o telematiche, questo è l'obiettivo che deve perseguire il soggetto agente affinché la sua condotta

[153] Come contenuto nella manualistica di FIANDACA G.- MUSCO E., *Dir. pen.*, PS, vol. II, t. I, cit., 309.

rientri all'interno di questa fattispecie di reato[154]. Questa visione sembrerebbe essere erroneamente suggerita da una lettura parallela della norma gemella di cui all'articolo 617-*bis* c.p. che richiede espressamente che l'installazione venga attuata "al fine di", espressione che manca totalmente nell'articolo 617-*quinquies* del Codice penale. Si deve quindi preferire, per non allontanarsi troppo dalla lettera della norma, un dolo generico.

Considerata l'importanza dell'installazione non stupisce che il momento consumativo del reato si perfezioni proprio con essa.

Trovandoci davanti ad un reato di pericolo indiretto non è ammissibile il tentativo[155].

Anche l'articolo 617-*quinquies* c.p. prevede, al comma 2, delle circostanze aggravanti che sono le stesse di quelle previste al comma 4 dell'articolo 617-*quater* del Codice penale al quale, pertanto, si rimanda.

Per quanto riguarda la struttura e il bene giuridico tutelato si deve tenere in considerazione che l'articolo in questione non faccia altro che punire condotte prodromiche alla commissione del delitto di cui all'articolo 617-*quater* c.p. e come tale condivide con esso la tutela – ulteriormente anticipata – della riservatezza e, dunque, della sicurezza delle comunicazioni che avvengono tra sistemi informatici o telematici. Si può, al massimo, discutere se ci si trovi o meno innanzi a un reato di pericolo indiretto[156] o concreto[157]. Secondo l'orientamento che sposa la seconda opzione il pericolo sarebbe concreto perché il giudice è chiamato *a posteriori* a valutare l'idoneità in concreto dello strumento utilizzato per intercettare, impedire o interrompere le comunicazioni informatiche o telematiche, tuttavia altra parte della dottrina e la giurisprudenza di legittimità preferiscono propendere per un reato di pericolo indiretto che come "pericolo di pericolo" anticipa di molto la punibilità di una condotta offensiva per tutelare un interesse giuridico ritenuto particolarmente importante dal legislatore

[154] PECORELLA C., *Diritto penale dell'informatica*, cit., 305, per il quale il delitto sarebbe di dolo specifico visto che il soggetto attivo agisce per intercettare, interrompere o impedire comunicazioni informatiche; idem anche RELLA R., *Art. 617-617*-quater *c.p.*, cit., 879.

[155] Non concorde Cass. pen., sez. II, 14.10.2011, CED, n. 251544. In dottrina, invece, si veda PIERGALLINI C., *I delitti contro la riservatezza e la libertà delle comunicazioni*, cit., 845.

[156] Per PIERGALLINI C., *I delitti contro la riservatezza e la libertà delle comunicazioni*, cit., 845, si tratterebbe di un reato comune a consumazione anticipata.

[157] PECORELLA C., *Diritto penale dell'informatica*, cit., 305; CUOMO L-RAZZANTE R., *La nuova disciplina dei reati informatici*, Torino, 2009, 201.

(sottolineando in questo modo, però, l'illogicità manifesta di una norma che vada a punire più gravemente un comportamento prodromico rispetto alla commissione dello stesso delitto il cui svolgimento si vorrebbe così tanto ardentemente rendere più difficoltoso)[158].

2.3 L'articolo 617-*sexies* c.p.

Siamo, quindi, giunti all'ultimo articolo riguardante i reati contro la "riservatezza informatica". L'articolo 6 della legge numero 547/1993 ha introdotto anche l'articolo 617-*sexies* del Codice penale prevedendo la sanzione della reclusione da uno a quattro anni per chi ‹‹al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, qualora ne faccia uso o lasci che altri ne facciano uso››. Come vedremo anche in questo caso è previsto l'aggravamento della pena con la reclusione da 1 a 5 anni nel caso in cui si rientri nelle circostanze aggravanti già viste al comma 4 dell'articolo 617-*quater* c.p.

2.3.1 La condotta tipica e l'oggetto materiale del reato

Nel citare la lettera della norma si è potuto intendere che la condotta tipica prevista sia particolarmente complessa, consistendo nell'alterare o sopprimere dati informatici che siano parte del contenuto di comunicazioni tra sistemi informatici o telematici intercettati – volontariamente o anche in modo occasionale – e nell'utilizzo seguente da parte del soggetto agente o di un terzo.
La condotta di "falsa formazione" si manifesta nella produzione di comunicazioni informatiche o telematiche che, in tutto o in parte, si fanno passare come il contenuto di una comunicazione intercettata, anche occasionalmente, attribuendola ad un autore apparente.

[158] BORRUSO R., *La tutela della comunicazione informatica*, cit., 124, per il quale la fattispecie sarebbe posta a tutela generale della sicurezza informatica.

Il termine "alterazione" ha il significato di "modificare, anche solo parzialmente, il contenuto di una comunicazione informatica o telematica attraverso l'aggiunta, la sostituzione o la soppressione di parte di essa ottenuta mediante la sua intercettazione, anche se occasionale".

Il "sopprimere" consiste nella distruzione o nella cancellazione, in tutto o in parte, di ciò che sia contenuto all'interno di una comunicazione informatica o telematica precedentemente intercettata, anche in modo occasionale[159].

Tutte queste condotte appena descritte hanno bisogno, per essere perfezionate, che vi sia stata una previa captazione, anche se involontaria, di quanto compone una conversazione tra due sistemi informatici o telematici (e irrilevante è il modo in cui il soggetto agente abbia ottenuto il materiale così intercettato).

Il momento consumativo del reato si verifica nel momento in cui tali comunicazioni, così modificate, vengono utilizzate dallo stesso soggetto che ha compiuto l'alterazione o da un terzo a cui tali contenuti sono stati trasferiti o concessi[160]. Come tale è necessaria anche un'ulteriore condotta per soddisfare i criteri d'esistenza di questo reato, ponendosi a un livello di maggiore gravità rispetto alla mera intercettazione dell'articolo 617-*quater* c.p., poiché non solo ci si inserisce abusivamente nel corretto funzionamento del processo comunicativo tra due o più sistemi ma si spacciano anche per veri contenuti falsi.

Si deve così escludere dal novero di applicazione dell'articolo 617-*sexies* c.p. la condotta di chi (secondo la pratica del "phishing"[161]) crei una *e-mail ad hoc* spacciandosi, ad esempio, per Poste italiane poiché in questo caso mancherebbe la previa necessaria azione della captazione, anche parziale e occasionale, di una comunicazione informatica o telematica reale. Si richiede, infatti, la presenza di una "fase dinamica" con l'alterazione, la soppressione o la falsa formazione del contenuto di una comunicazione tra sistemi, ancora in corso, per cui questi dati devono essere stati previamente intercettati.

Non rappresenta un'ipotesi di condotta che si inserisce all'interno di questa fattispecie anche quella di chi "contraffà" una comunicazione che si è già ricevuta

---

[159] Cfr. MARINI G., *Delitti contro la persona*, cit., 425; PICA G., *Diritto penale*, cit., 182.

[160] PICOTTI L., *Commento all'art. 6 l. 23/12/1993*, cit., 124, nota 22, sottolinea insieme ad altri come sia bastevole ad integrare l'elemento costitutivo della fattispecie il semplice uso delle comunicazioni anche da parte di una singola persona.

[161] Lo sottolinea Trib. Milano, g.i.p., 10.12.2007, in *Foro ambr*., 2008, 280.

ed in quanto tale non ancora "in corso": se si è già ricevuta l'*e-mail* reale da parte di Poste italiane, la successiva azione di chi spacciandosi per la società invia una seconda *e-mail* separata non rientrerebbe nella modifica di una comunicazione ma, al massimo, in quella di "corrispondenza telematica". Tale differenziazione è giustificata dal fatto che si considera ben più grave, poiché pericolosa, la modifica di una comunicazione attesa e che si attribuisce ad un determinato soggetto (dunque ritenendola vera) piuttosto che il successivo tentativo di convincimento con ulteriori invii, magari non attesi, di altre comunicazioni.

La condotta del soggetto agente ricade, come più volte ripetuto, sul contenuto di informazioni formanti ‹‹comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi››, anche se intercettate occasionalmente[162]. Tale contenuto non deve avere una funzione probatoria o, in questo caso, troverebbe applicazione la più grave fattispecie di falsità prevista all'articolo 491-*bis* c.p. se tale documento informatico sia anche un atto pubblico.

Allo stesso tempo non deve riguardare neanche una mera conversazione tra due persone, uno scambio privato, poiché in questo caso troverebbe applicazione la più restrittiva definizione di "corrispondenza" e con essa l'articolo 616, cpv., c.p. ad oggi ricomprendente anche "quella informatica o telematica ovvero effettuata con ogni altra forma di comunicazione".

Rispetto, dunque, al gemellare articolo 617-*ter* c.p. questa fattispecie trova un'applicazione molto minore poiché non vede un'estensione del suo oggetto materiale ad opera dell'articolo 623-*bis* c.p. come invece accade per questo, applicandosi anche a ‹‹qualunque altra trasmissione a distanza di suoni, immagini od altri dati›› maggiormente indeterminati[163].

2.3.2 Altri elementi della fattispecie

L'elemento soggettivo è rappresentato da un dolo specifico. Infatti, oltre alla coscienza e alla volontà di agire per "formare falsamente", "alterare" o "sopprimere" il contenuto di una comunicazione informatica o telematica che sia

[162] Si rimanda *supra*, capitolo II, paragrafo 2.0.5.2 per quanto riguarda l'oggetto materiale dell'articolo 617-*quater* c.p.

[163] PICOTTI L., *Commento all'art. 6 l. 23/12/1993*, cit., 123.

stata previamente intercettata, anche se in modo occasionale, per farne uso o per permettere ad un terzo di farne uso è necessario che tutto ciò venga fatto "per procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno". Non è necessario, per la consumazione, che tale profitto o danno vengano poi raggiunti ma solo che tali comunicazioni così alterate siano state utilizzate per questo scopo.

Come tale la consumazione si perfezionerà proprio nel momento in cui il contenuto delle comunicazioni informatiche o telematiche intercettate e modificate dal soggetto agente vengano utilizzate da quest'ultimo o anche da un terzo al quale si sono messe a disposizione.

Per quanto estremamente raro una simile disposizione non viete la configurazione del tentativo.

Esattamente come già visto per l'articolo 617-*quinquies* c.p. anche per l'articolo 617-*sexies* c.p. è previsto l'aggravamento della pena con la reclusione da uno a cinque anni per le stesse circostanti aggravanti contenuto nel comma 4 dell'articolo 617-*quater* del Codice penale.

Essendo l'articolo in esame gemello dell'articolo 617-*ter* c.p. ne condivide non solo la struttura ma anche il bene giuridico tutelato rappresentato dall'autenticità, integrità e genuinità di quanto contenuto all'interno delle comunicazioni scambiate attraverso due o più sistemi informatici o telematici[164]. In particolar modo è obiettivo della norma in questione quello di evitare che tali informazioni siano falsificate, alterate o soppresse nel momento in cui sono più esposte: durante il processo di trasferimento da un sistema informatico o telematico all'altro.

2.4 Profilo conclusivo di "corrispondenza" informatica e telematica

Si è più volte toccata, nel corso della precedente trattazione, la definizione di "comunicazione" e quella di "corrispondenza" informatica o telematica. Il problema è alla base dell'applicazione, di volta in volta, degli articoli 617 e successivi del Codice penale o dell'articolo 616 c.p. Quest'ultimo, infatti, al suo

[164] Vedi PICOTTI L., *Commento all'art. 6 l. 23/12/1993*, cit., 121, 124; PECORELLA C., *Sub art. 617-sexies c.p.*, cit., 6050.

capoverso, modificato dall'articolo 5 della legge numero 547/1993, si riferisce alla "corrispondenza" tutelando anche quella "informatica" e "telematica" così come quella ‹‹effettuata con ogni altra forma di comunicazione a distanza››.

Chiaramente questa norma era stata pensata, in origine, per le forme di corrispondenza "classica" come quella ‹‹epistolare, telegrafica o telefonica›› e fu estesa dal legislatore nel 1993 per cercare di coprire una lacuna di tutale all'interno del nostro ordinamento. Così facendo, però, tale garanzia rischia di andare a confondersi e a sovrapporsi con quella che ricomprendere le comunicazioni informatiche o telematiche ulteriormente ampliate dalla clausola estensiva dell'articolo 623-*bis* c.p. (riformulato anch'esso dalla legge numero 547/1993 ma all'articolo 8) in forza del quale tali fattispecie si applicano anche "a qualunque altra trasmissione a distanza di suoni, immagini o ad altri dati".

Questa formulazione è ampia proprio perché non ha dei confini ben definiti, è molto indeterminata ed è normale che la sua estensione finisca per avvicinarsi pericolosamente a quella dell'articolo 616 cpv. del Codice penale[165]. Sul piano meramente oggettivo, infatti, sia la corrispondenza che le comunicazioni si caratterizzano per l'utilizzazione di strumenti tecnici e misure di sicurezza atte a cercare di escludere l'illecita captazione da parte di estranei. Dall'altro lato, sul piano soggettivo, la corrispondenza si caratterizza per un contenuto maggiormente personalistico con uno sfondo di riservatezza mirata a una "esclusività" propria delle informazioni e dei dati comunicati che sono pensati per restare all'interno della cerchia degli individui determinati a partecipare a quello specifico rapporto comunicativo. Ci si trova davanti, quindi, a una differenza legata al fatto che la "corrispondenza" sia scambiata con l'intenzione di mantenere le informazioni in essa contenute maggiormente intime e segrete rispetto alla normale "comunicazione" informatica o telematica[166]: tra le due ipotesi, dunque, intercorre un rapporto di genere a specie.

Il discrimine tra le norme pensate dal legislatore a garanzia della corrispondenza informatica o telematica (come l'articolo 616 ma anche il 618, il 619 ed il 620 c.p.) è rappresentato dall'interesse più "personale" e "individuale" con il contenuto della comunicazione strettamente rivolto a soggetti facenti parte di una

[165] PICOTTI L., *Commento all'art. 5 l. 23/12/1993*, cit., 109 ss., 115.
[166] Vedi MANTOVANI F., *Dir. Pen.*, PS., vol. I, cit., 626 s.

cerchia determinata[167]. Dall'altro lato, le fattispecie che si pongono a tutela contro le intercettazioni delle comunicazioni informatiche o telematiche (contenute negli articoli 617-*quater*, 617-*quinquies* e 617-*sexies* c.p.) garantiscono l'interesse collettivo alla riservatezza ma, soprattutto, alla sicurezza delle telecomunicazioni che può passare solo attraverso un corretto funzionamento dei processi di "conversazione" tra sistemi informatici o telematici non disturbati da azioni abusive di soggetti terzi.

3.0 I reati di danneggiamento informatico

Dopo aver trattato il tema dell'illegittima intromissione all'interno di un sistema informatico o telematico, nonché l'illecita captazione e l'utilizzo delle informazioni ottenute mediante un'abusiva introduzione nel processo di comunicazioni tra due o più sistemi dobbiamo, prima di poter parlare con maggiore cognizione di causa di un *dual use software*, trattare della tutela penale dell'integrità dei dati e dei sistemi informatici ad oggi contenuta all'interno degli articoli 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del Codice penale.
Come per tutti i delitti aggiunti con la riforma della legge 547 del 1993 anche quelli riguardanti i danneggiamenti informatici affondano le loro radici in un passato in cui vi era una lacuna di tutela.
Con l'espandersi del mondo digitale in Italia sul finire degli anni '70 si cominciarono a osservare i primi episodi di criminalità informatica. In assenza di apposita normativa al riguardo, l'unico strumento della giurisprudenza fu quello di praticare un'interpretazione estensiva di norme già esistenti nel tentativo di colmare il vuoto di tutela[168]. Ovviamente per quanto riguarda il danneggiamento informatico la fattispecie più similare e vicina da poter essere utilizzata fu quella del danneggiamento di cose contenuta all'articolo 635 c.p., che non mostrava

[167] Vedi MANTOVANI F., *Dir. Pen.*, PS., vol. I, cit., 627 s.
[168] PICA G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, cit., 420 ss.

particolari problematiche per quanto riguardava la violenza perpetrata sulle parti fisiche e visibili di un elaboratore elettronico (il così detto "*hardware*")[169].

La giurisprudenza riuscì comunque a ricondurre anche il danneggiamento delle parti non "fisiche" del computer alla fattispecie dell'articolo 635 c.p. attraverso il così detto "danneggiamento logico"[170]. Per quanto, infatti, fosse complesso far rientrare un "*software*" all'interno della nozione di "cosa" era molto più facile estendere la tutela dell'articolo sopracitato andando ad affermare che la parte "non fisica" del computer, quella che potremmo definire quasi come la sua "anima", era strettamente collegata al corretto funzionamento dell'"*hardware*" poiché connessi in un "connubio indivisibile tra le apparecchiature fisiche *hardware* ed i programmi che le utilizzano e specializzano".

E' chiaro come questo fosse il massimo della garanzia che si era in grado di applicare all'epoca, quando ancora oltretutto i computer erano particolarmente semplici ma allo stesso tempo è difficile accettare completamente questa interpretazione: se anche si volesse ammettere che ogni singola modifica logica ai dati e ai programmi informatici possa determinare il danneggiamento o compromettere il corretto funzionamento del suo supporto magnetico, i limiti di una simile visione si percepivano riguardo ai danneggiamenti dei dati in fase di trasmissione (attraverso la rete internet o una rete LAN) e che per tale ragione non si trovavano in quel momento a essere incorporate all'interno di un supporto fisico specifico[171].

Proprio per risolvere tale problematica il legislatore italiano introdusse con l'articolo 9 della legge 547/1993 ‹‹modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica››

---

[169] PICOTTI L., *La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione dati*, in *Dir. inf.*, cit., 969 ss.

[170] Così Cass. pen., SS. UU., 13.12.1996, n. 1282, Carpanelli, in *Giur. It.*, 1997, II, cit., 647 ss., che affermava: ‹‹antecedentemente all'entrata in vigore della legge 23 dicembre 1993 n. 547 (in tema di criminalità informatica), che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione dei dati dalla memoria di un computer, in modo tale da renderne necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento ai sensi dell'art. 635 c.p. in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore››.

[171] Lo stesso caso risolto dalla Corte di Cassazione e citato nella nota immediatamente precedente aveva trovato difficoltà nel fatto che l'hardware, nonostante la perdita di dati, non avesse avuto bisogno di correzioni o aggiustamenti per poter tornare a funzionare perfettamente ed in maniera autonoma.

con la creazione dell'apposita fattispecie di ‹‹danneggiamento di sistemi informatici e telematici››. Tale apparato di tutela è stato ulteriormente modificato con la legge numero 48 del 2008 riguardante la ‹‹ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno›› che, tra le altre cose, ha anche aggiornato l'articolo 635-*quinquies* del codice penale.

Il primo aspetto che salta all'occhio è che il legislatore italiano abbia deciso di adottare la stessa bipartizione suggerita in ambito europeo tra danneggiamento di "dati informatici" e di "sistemi informatici"[172]: i primi trovano tutela negli articoli 635-*bis* e 635-*ter* del codice penale mentre i secondi all'interno delle fattispecie di cui all'articolo 635-*quater* e 635-*quinquies*. Tali quattro articoli formano, insieme all'articolo 640-*bis* c.p. (frode informatica) e all'articolo 615-*quinquies* c.p. (diffusione di programmi diretti a danneggiare un sistema informatico) un microsistema normativo il cui obiettivo è quello di garantire la tutela penale dell'integrità dei dati e dei sistemi informatici.

Procedendo all'illustrazione dei singoli articoli si andrà ad analizzare anche l'ambito di tutela ad oggi garantito dalla normativa attuale e che ci servirà come base per la successiva trattazione della materia riguardante i *dual use software* e il loro utilizzo.

3.1 L'articolo 635-*bis* c.p.

Introdotta con la legge 547/1993, la norma recita: ‹‹salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni››.

Il testo vigente è stato così modificato dalla legge numero 48 del 2008 che ha inciso soprattutto sulle condotte considerate illecite in modo da integrare quelle

[172] Cfr. CORRIAS LUCENTE G., in CORASANITI G.-CORRIAS LUCENTE G. (a cura di), *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Padova, 2009, cit., 132; PICOTTI L., *Profili di diritto penale sostanziale*, cit., 700 ss.; nella manualistica, invece, FIANDACA G.-MUSCO E., *I delitti contro il patrimonio*, cit., 2015, 145 ss.

già esistenti della "distruzione, deterioramento o rendere inservibile" con quelle della "cancellazione, alterazione e soppressione", eliminando quella della "provocata inservibilità"[173]. Oltre a ciò, il legislatore della riforma ha scorporato dall'oggetto materiale del reato i "sistemi informatici e telematici" che oggi costituiscono l'oggetto dei reati di cui agli articoli 635-*quater* e 635-*quinquies* c.p. Non bisogna, però, confondere questa fattispecie con una delle circostanze aggravanti previste nel comma 2 dell'articolo 615-*ter* del Codice penale che riguarda il danneggiamento avvenuto per realizzare o a causa dell'accesso abusivo ad un sistema informatico o telematico: il discrimine è da trovarsi nella volontarietà della condotta.

Il danneggiamento seguito all'accesso abusivo in un sistema informatico o telematico, infatti, non dovrà essere voluto dal soggetto agente, presentandosi questa ipotesi come un reato aggravato dall'evento[174] (per altra dottrina, invece, ci si troverebbe davanti ad un reato circostanziato[175]). Se, invece, il danneggiamento fosse stato lo scopo originale della condotta fin dalla sua origine troveranno direttamente applicazione i delitti di cui agli articoli 635-*bis* c.p. e seguenti che trattano specificatamente la materia in questione[176].

3.1.1 La condotta tipica e l'oggetto materiale del reato

L'articolo 635-*bis* c.p. nella sua formulazione originaria era stato plasmato sulla struttura del già esistente articolo 635 c.p., precedentemente applicato con interpretazione estensiva anche alle fattispecie di danneggiamento informatico.

---

[173] Prima della riforma il testo dell'articolo 635-*bis* 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. Se ricorre una o più delle circostanze di cui al secondo comma dell'art. 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni››.

[174] Cfr. MANTOVANI F., *Diritto penale*, PS, I, cit., 579.

[175] BONDI A., *I reati aggravati dall'evento tra ieri e domani*, Napoli, 1999, 60, nota 34, per il quale l'evento ulteriore del "danneggiamento" costituirebbe un'aggravante causalmente legata alla condotta di accesso abusivo. Se così fosse si riscontrerebbero diversi problemi dato che le circostanze aggravanti sottostanno alla disciplina del bilanciamento secondo quanto contenuto nell'art. 69 c.p.

[176] MUCCIARELLI F., *Commento agli artt. 1, 2, 4 e 10 l. 1993 n. 547*, cit., 102; idem PECORELLA C., *Il diritto penale dell'informatica*, cit., 354.

Per quanto la nuova formulazione dell'articolo abbia aggiunto diverse nuove condotte ha comunque mantenuto quelle del "distruggere" e del "deteriorare": la prima condotta va intesa come l'eliminazione definitiva – totale o parziale – delle informazioni mediante il vero e proprio annientamento del supporto fisico sul quale si trovavano incorporate (dunque si prende una chiave inglese cominciando a colpire un *personal computer* finché non si è sbriciolato l'*hardware* e quello che conteneva) mentre la seconda condotta si riferisce alla diminuzione – che deve essere apprezzabile – della funzione strumentale dei dati con annessa riduzione del loro valore o utilizzabilità.

Con la legge di ratifica della Convenzione di Budapest si sono introdotte anche le condotte di "cancellazione", "alterazione" e "soppressione" dei dati che prima non erano previste: con il "cancellare" – tra l'altro l'ipotesi più frequente nella pratica – si intende la distruzione anche in questo caso totale o parziale dei dati o dei programmi contenuti mediante non tanto l'annientamento fisico del supporto materiale ma con la smagnetizzazione del supporto (come potrebbe avvenire usando una calamita di sufficiente potenza) o la sostituzione dei precedenti dati con nuovi e diversi o mediante l'imposizione di un comando o l'inoculazione di un virus in grado di provocare la cancellazione dei dati stessi; l'"alterazione" deve essere letta come la modificazione dell'essenza stessa del dato o del programma attuabile attraverso la manipolazione, totale o parziale, delle istruzioni che li compongono (per esempio con l'aggiunta, il taglio o la modifica del codice interno) e con il quale si procede alla perdita, anche qui totale o parziale, della loro originaria funzionalità tanto che è difficile tracciare una linea di demarcazione specifica rispetto alla condotta del "deterioramento"; la "soppressione" crea ancora maggiori problemi poiché non ha una definizione propria ma appare sovrapponibile con le condotte di "distruzione" e di "cancellazione" dei dati e dei programmi[177].

Questa forse eccessiva elencazione da parte del legislatore, mostra però quanto sia complesso coprire l'interezza delle possibili condotte illecite realizzate in questa nuova materia (e dunque "*melius abundare quam deficere*"). Proprio questa ampia

[177] MANTOVANI F., *Diritto penale, parte speciale*, cit., 2014, 141; ATTILI G., in *Reati contro la persona e contro il patrimonio*, cit., 2015, 618; CRACA A., in *Codice dei reati contro il patrimonio*, cit., 196 ss.

formulazione ha indotto il legislatore a ritenere d'aver già offerto una tutela più che adeguata, portandolo ad eliminare, quindi, la condotta di "rendere inservibile" e che andava a coprire tutto quell'insieme di attività aggressive le quali, senza poter essere ricondotte all'ipotesi della "distruzione" o della "cancellazione" definitiva, determinavano semplicemente l'inidoneità, in tutto o in parte, degli elaboratori elettronici a svolgere la loro funzione strumentale per un tempo apprezzabile (come potrebbe accadere con l'occultamento dei dati, la cancellazione soltanto apparento o un mezzo di blocco temporaneo sull'accesso). Tale ipotesi, ad oggi, trovano difficoltà ad essere ricomprese o nella condotta di "alterazione" di cui all'articolo 635-*bis* c.p. o a quella della "resa inservibilità parziale" dell'articolo 635 c.p.

Tutte queste condotte, comunque, vanno a ricadere su un comune oggetto materiale rappresentato dalle relazioni di proprietà o di godimento delle entità materiali (sistemi informatici o telematici e relativi supporti) in cui i dati, le informazioni e i programmi sono incorporati.

Il reato è comune essendo concretizzabile da "chiunque" mentre il soggetto passivo è costituito dal proprietario o da chi ha il diritto di godimento sui sopradetti sistemi e supporti.

Bisogna però considerare come, rispetto al precedente articolo 635-*bis* c.p., oggi la modifica legislativa ha optato per una bipartizione dei delitti di danneggiamento informatico. In particolare, sia l'articolo 635-*bis* c.p. che l'articolo 635-*ter* c.p. hanno uno specifico oggetto materiale costituito dai "programmi, informazioni e dati informatici di privata utilità", ovverosia i "*software*" in quanto i "dati informatici" non sarebbero altro che le generiche rappresentazioni di informazioni codificate in una forma non percepibile alla vista (elettronica, magnetica, ottica e così via).

L'articolo 635-*bis* c.p. fornisce tutela, in particolar modo, a quelli di "privata utilità", come si evince implicitamente dalla distinzione rispetto all'articolo 635-*ter* c.p. Oltretutto questi "programmi, informazioni o dati" devono anche trovarsi incorporati in sistemi o supporti "altrui", dunque di proprietà o di godimento di altri. Nel mondo informatico, però, l'altruità non è un concetto di facile definizione. I "programmi informatici", infatti, si caratterizzano soprattutto per la

loro natura immateriale o comunque incorporea che rende molto difficile l'apprensione esclusiva da parte di un solo soggetto specifico. Allo stesso tempo la nozione civilistica di "altruità" deve essere estesa visto che non ricomprende solo il proprietario ed il concedente quanto anche il concessionario, l'utente che abbia un legittimo interesse a che le informazioni, i dati o i programmi funzionino nel modo più corretto e regolare possibile.

3.1.2 Altri elementi della fattispecie

Non c'è molto da discutere sulla natura del reato trattandosi, esattamente come per l'articolo 635 c.p., di un reato d'evento in quanto a forma libera (causalmente orientato) che non si articola, dunque, in mezzi specifici o determinate modalità quanto piuttosto concentrandosi sulla sola azione causale dell'evento.
Le condotte di "distruzione", "cancellazione", "deterioramento", "alterazione" e "soppressione" altro non costituiscono che eventi naturalistici diversi e distinti dalla condotta, cagionanti modificazioni del mondo esteriore[178].
Il delitto è solitamente commesso mediante un'azione ma ciò non significa che non possa realizzarsi anche tramite un'omissione da parte del destinatario di un obbligo giuridico di garanzia in quanto, stando al comma 2 dell'articolo 40 c.p., "non impedire" l'evento equivale a "cagionarlo".
Il D.lgs numero 7 del 2016 ha riformulato il comma 2 che contiene una circostanza aggravante "se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore di sistema". La modifica legislativa ha deciso, così, di differenziare le circostanze aggravanti dell'articolo 635-*bis* c.p. rispetto a quelle dell'articolo 635 c.p. che erano state previste prima del 2008.
La prima circostanza aggravante risulta essere, *ictu oculi*, un'ipotesi più che altro giurisprudenziale – tenendo da conto la rarità con cui può essere posta in essere una condotta di danneggiamento di un computer con "minaccia alla persona" – mentre la ragione alla base della seconda circostanza è la maggiore gravità della condotta quando questa è attuata da soggetti che occupano posizioni privilegiate

[178] Cass. pen., sez. V, 18.11.2011, n. 8555, in Ced Cass., rv. 251731.

in quanto "operatori di sistema". Con tale definizione è controverso se si debba intendere soltanto il "tecnico informatico", dunque colui che all'interno di un'azienda ha il controllo delle diverse fasi del processo di elaborazione dei dati, o in generale "tutti i tecnici dell'informatica", riferendosi quindi a tutti i soggetti che si trovano legittimati ad operare sul sistema.
La clausola di riserva esclude l'applicazione del delitto quando la condotta costituisca più grave reato. Si deve, quindi, escludere l'articolo 420, comma 2 e 3 c.p. dal novero poiché abrogato dalla stessa riforma del 2008 e che ad oggi è stato sostituito dai delitti di cui agli articoli 635-*quater* e 635-*quinquies* del codice penale. Più gravi sono, dunque, da considerarsi l'articolo 635-*ter* c.p. e gli articoli 490 e 491 c.p.
Quando aggravato il delitto diventa perseguibile d'ufficio e la pena aumenta prevedendo la reclusione da 1 a 4 anni.

3.2 L'articolo 635.*ter* c.p.

Quando il legislatore italiano ha accolto la bipartizione tra il danneggiamento dei dati informatici e il danneggiamento dei sistemi informatici ha deciso di optare anche per l'introduzione di altri due delitti che si differenziano esclusivamente per il fatto che la condotta ricada su "sistemi di pubblica utilità"[179]. Si è scelto, dunque, di effettuare un passo ulteriore rispetto a quanto previsto nella Convenzione di Budapest andando a prevedere delle vere e proprie ipotesi aggravate nel momento in cui il danneggiamento ricada su ‹‹informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità›› (articolo 635-*ter* c.p.) e su ‹‹sistemi informatici o telematici di pubblica utilità›› (articolo 635-*quinquies*).
Parte della dottrina si è ritrovata, però, a criticare una simile scelta di matrice politico-criminale in quanto la mancata perfetta equiparazione nei termini può condurre a una differenziazione nell'ambito dei soggetti passivi[180]. In ciò il

[179] MANTOVANI F., *Delitti contro il patrimonio*, cit., 146; COCCO G., in *reati contro i beni economici*, cit., 161.
[180] Cfr. PICOTTI L., *Ratifica alla convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, 2008.

legislatore avrebbe fatto meglio a limitarsi alla sola utilizzazione della locuzione di "pubblica utilità" che sarebbe stata più che esaustiva.

I due articoli nascono in sostituzione del parzialmente abrogato articolo 420 c.p.[181] e si sono modellati proprio su questa ipotesi piuttosto che, forse più correttamente, su quelle contenute negli articoli 635-*bis* e 635-*quater* del codice penale. Dall'abrogato comma 2 dell'articolo 420 c.p. si sono ripresi non solo il trattamento sanzionatorio ma anche la stessa tecnica di formulazione che differenziano queste ipotesi dai precedenti delitti di danneggiamento, in quanto questi ultimi hanno la forma di "reati di evento" mentre quelli in esame si caratterizzano per la peculiare struttura di "delitti di attentato" e, quindi, per l'anticipazione del momento consumativo previsto per tali condotte.

3.2.1 Elementi della fattispecie

La lettera dell'articolo 635-*ter* c.p. recita: ‹‹salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni››.

In questo caso l'elemento oggettivo è sempre costituito dalle informazioni, dati o programmi informatici" ma con la differenza che, rispetto all'articolo 635-*bis* c.p., questi vengano utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o, comunque, di pubblica utilità.

[181] Prima della modifica legislativa il testo dell'art. 420 c.p. così recitava: ‹‹Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni. La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti. Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni.››

A differenza dell'articolo 635-*quinquies* c.p. oltre alla "pubblica utilità" si fa riferimento anche alle informazioni, dati e programmi che vengano utilizzati dallo Stato o da altro ente pubblico, da intendersi come ricomprendenti anche quelli appartenenti a privati ma utilizzati dai soggetti sopra scritti. In questo caso la "pubblica utilità" va intesa in senso ampio, abbracciando anche tutti quei dati, informazioni o programmi che pur essendo privati sono destinati a soddisfare degli interessi pubblici o collettivi a causa dell'indeterminatezza del numero dei fruitori e, in quanto tale, l'ulteriore locuzione "ad essi pertinenti" appare oggi superflua.

La gravità della condotta è sottolineata anche dal fatto che non si richieda "l'altruità" dei dati che quindi comporta l'illiceità del comportamento anche quando ricadente su beni informatici di proprietà dello stesso soggetto agente.

Come si è precedentemente sottolineato la particolarità di questo articolo, come dell'articolo 635-*quinquies* c.p. che ne è il gemello, è il fatto che la struttura del reato – a differenza dei soliti delitti di danneggiamento – è a "consumazione anticipata" per quanto sia più corretto dire che sia un "reato di attentato" dato che lo stesso tentativo costituirebbe fatto integrante del reato. Il delitto sarebbe, dunque, già da considerarsi perfezionato e quindi consumato in tutte le ipotesi normalmente giustificanti l'ipotesi di tentativo per i reati agli articoli 635-*bis* e 635-*quater* c.p. Come tali tutti gli atti che, *ex post*, si riveleranno oggettivamente idonei e diretti in modo inequivoco a creare un concreto pericolo per il bene giuridico tutelato rientreranno nella fattispecie di cui al comma 1.

Se poi l'evento di danneggiamento dovesse verificarsi veramente ci si troverebbe davanti all'ipotesi di cui al comma 2 dello stesso articolo che prevede una pena maggiore[182]. Come per il delitto precedente anche qui ‹‹se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore di sistema›› il delitto è aggravato e la pena aumentata.

[182] MEZZETTI E., *Reati contro il patrimonio*, cit., 2013, 350; COCCO G., in *I reati contro i beni economici*, cit., 161; PICOTTI L., *Profili di diritto sostanziale*, cit., 715, che rappresentano parte di quella dottrina maggioritaria che riterrebbe il secondo comma dell'articolo 635-*ter* non un'ipotesi aggravante quanto un'autonoma figura di reato aggravato dall'evento e, per tanto, non opererebbe in questo caso il bilanciamento di circostanze ex art. 69 c.p.

3.3 L'articolo 635-*quater* c.p.

In ottemperanza alla Convenzione di Budapest l'articolo 5, comma 2, della legge numero 48 del 2008 ha aggiunto l'articolo 635-*quater* c.p. che così recita: ‹‹salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni››.
Tale articolo rappresenta la scelta legislativa, a livello europeo, di dividere le ipotesi di danneggiamento informatico a seconda dell'oggetto materiale che in questo specifico caso è il così detto "*hardware*".
Il testo attualmente vigente rappresenta altresì il frutto delle modifiche di cui all'articolo 2 del D.lgs numero 7 del 2016.

3.3.1 Condotta tipica e oggetto materiale del reato

La norma in esame non si distanzia eccessivamente dall'articolo 635-*bis* c.p., riprendendo spesso forme e stilemi. Anch'esso è un reato a forma vincolata dato che l'evento deve essere prodotto dalle condotte già elencate all'interno dell'articolo 635-*bis* del codice penale ("distruggere", "deteriorare", "cancellare", "alterare" o "sopprimere") o "attraverso l'introduzione o la trasmissione di dati, informazioni e programmi". Si presenta tuttavia come un'ipotesi maggiormente aggravata rispetto alla "compagna" perché ricade sui sistemi informatici[183] o telematici[184] in generale, potendo ottenere il loro danneggiamento o l'ostacolo al loro funzionamento anche meditante l'introduzione di "*software*".
Quest'ultima ipotesi è stata resa necessaria per contrastare il così detto "danneggiamento logico", cioè quelle condotte neutre che si rivelano però

[183] Secondo Cass. pen., sez. II, 14.12.2012, n. 9870, in Foro it. 2012, II, 576, ‹‹l'oggetto materiale del delitto di danneggiamento di sistema informatico è costituito dal complesso di apparecchiature, interconnesse o collegate tra loro, in cui una o più di esse effettui il trattamento automatico di dati mediante un programma››.
[184] Solitamente consistente in tutte quelle forme di telecomunicazione gestite informaticamente, come presente in COCCO G., *I reati contro i beni economici*, cit, 2015, 163.

dannose (quali l'inoculazione di un programma che poi si rivela essere un "*malware*").
È un reato comune potendo compierlo "chiunque" e il soggetto passivo è sempre il proprietario o chi ha il godimento dei sistemi sopra elencati.
Per il resto, la disposizione ripropone in gran parte quanto già visto nell'articolo 635-bis c.p. alla quale, prima della riforma del 2008, questa fattispecie era accorpata. Ciò che ha invogliato il legislatore a compire un distinguo fu proprio l'attenzione che nella Convenzione di Budapest si pose sull'elemento oggettivo del reato: l'oggetto materiale, infatti, è costituito dai sistemi informatici e telematici (di privata utilità) con l'articolo 635-*bis* c.p. posto a tutela del "*software*" mentre l'articolo 635-*quater* c.p. sanziona le condotte di danneggiamento rivolte nei confronti dell'"*hardware*".
Attraverso le condotte sopra elencate si deve conseguire uno specifico evento che può essere il "danneggiamento" (dunque la diminuzione della funzionalità strumentale del sistema), l'"inservibilità totale o parziale" (dunque l'impossibilità per il sistema di funzionare correttamente, senza la sua materiale distruzione) o il "grave ostacolo al funzionamento" (che rispetto all'ipotesi di "inservibilità" prevede un ostacolo al funzionamento soltanto temporanea).
Il problema risiede nella capacità di distinguere quando il danneggiamento, magari rivolto solamente a un *software* e dunque rientrante nella fattispecie di cui all'articolo 635-*bis* c.p., possa sortire anche un effetto nei confronti dell'*hardware* e quindi giustificare l'applicazione della più grave fattispecie di cui all'articolo 635-*quater* c.p.

3.3.2 Altri elementi della fattispecie

Trattato l'argomento differenziante rispetto all'articolo 635-*bis* c.p. (l'elemento oggettivo) non risultano altre particolarità rispetto alla normativa già affrontata.
L'elemento soggettivo è un dolo generico. La norma richiede solamente la coscienza e la volontà delle condotte che vengono messe in atto per causare quegli specifici eventi elencati nella fattispecie.

Si ha la consumazione del reato con la verificazione dell'evento finale che perfeziona le condotte di "distruzione", "danneggiamento", "inservibilità" o "grave ostacolo" dei sistemi informatici o telematici che si è desiderato colpire. Ciò implica, ovviamente, anche la configurabilità del tentativo.
Il D.lgs numero 7 del 2016 ha aggiunto una circostanza aggravante quando "il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema".
Anche in questo caso la clausola di riserva iniziale serve ad escludere l'applicazione di questo delitto nel momento in cui la fattispecie ricada in quella più grave prevista all'articolo 635-*quinquies* c.p., sebbene alcuni abbiano fatto notare anche la possibile sovrapposizione di questo articolo con quello di "interruzione del funzionamento di sistemi informatici" di cui all'articolo 617-*quater* c.p. che già solo dalla rubrica sembrerebbe descrivere una condotta simile.

3.4 L'articolo 635-*quinquies* c.p.

Come l'articolo 635-*quater* c.p. costituisce il gemello dell'articolo 635-*bis* c.p anche l'articolo 635-*quinquies* c.p. si rivela essere similare all'articolo 635-*ter* c.p. con sole poche differenze.
La norma è così scritta: "se il fatto di cui all'articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni".
Le principali differenze già preannunciate con l'articolo 635-*ter* c.p. sono da ritrovarsi nell'oggetto materiale del reato che è lo stesso dell'articolo 635-*quater* c.p., quindi è rappresentato dai sistemi informatici o telematici ma non di uso "privato" quanto quelli di "pubblica utilità". Anche in questo caso si deve considerare la locuzione "di pubblica utilità" in senso estensivo e, per quanto la dizione manchi del riferimento all'utilizzazione da parte dello Stato o di altro ente

pubblico proprio dell'articolo 635-*ter* c.p., non vi è ragione di considerare che i due articoli abbiamo una vera e propria differenziazione in ambito di elemento oggettivo.

Come l'articolo 635-*ter* c.p. e a differenza dell'articolo 635-*quater* c.p. anche questa norma è un reato di attentato e pertanto si rimanda alla trattazione già espressa al riguardo nel precedente paragrafo dedicato all'articolo 635-*ter* c.p.

Come già accaduto in precedenza si pone, però, la questione di delimitare i rispettivi ambiti di operatività delle fattispecie di cui all'articolo 635-*ter* e 635-*quinquies* c.p. in quanto entrambi prevedono delle condotte che consistono nella "distruzione", "deterioramento", "cancellazione", "alterazione" o "soppressione" di informazioni, dati o programmi di pubblica utilità, con l'unica differenziazione che l'articolo 635-*quinquies* del codice penale prevede un passo ulteriore, in quanto tale danneggiamento deve ricadere non tanto sul "*software*" quanto sull'"*hardware*" in quanto tale (sistema informatico o telematico).

Anche qui l'elemento soggettivo è costituito dal dolo generico in quanto non si richiede alcun fine specifico ma soltanto la coscienza e la volontà di commettere i fatti diretti a danneggiare i sistemi.

Come per tutti i delitti già trattati, anche in questo caso, si prevede una circostanza aggravante nel momento in cui ‹‹il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore di sistema››.

Con tale ultima affermazione si conclude questa analisi dei delitti di "danneggiamento" e, in generale, dei "reati informatici" che saranno alla base della trattazione del successivo capitolo riguardante nello specifico i *dual use software*.

CAPITOLO III

DUAL USE SOFTWARE

1.0 I *software* (nuovi possibili spazi per la criminalità)

Si è detto in precedenza come la criminalità informatica si sia specializzata nel corso del tempo, cimentandosi in una serie di attacchi di varia natura che possono essere di maggiore o minore gravità. Molti *cybercrimes*, ad oggi, vengono eseguiti utilizzando Internet "*as a tool*", dunque, usufruendo dell'accesso alla rete e ai sistemi dell'informazione e della comunicazione per commettere reati comuni (atti persecutori, adescamento di minorenni, *cyber extortion* ecc.) ma con uno strumento nuovo. Dall'altra parte, invece, si presentano sempre più spesso reati cibernetici a fattispecie complessa che richiedono una strumentazione così come un livello di conoscenze più elevato[185].

Hacker e *cracker* creavano in passato questo strumentario come un artigiano pensava ai propri mezzi per operare, con la differenza che tali soggetti agiscono per commettere atti illeciti. Con queste conoscenze e questi strumenti è possibile penetrare abusivamente all'interno di sistemi informatici o telematici, carpire dati o informazioni, danneggiare *hardware* o *software*, commettere truffe mediante *e-mail* (c.d. *scamming*), prendere il controllo di altri computer in modo da creare reti informatiche assoggettate al proprio volere (c.d. *botnet*) e utilizzare questa potenza di fuoco computazionale per colpire o ostacolare l'attività di siti e server (c.d. *DoS o DDoS, DDS attacks* ecc.) o prendere coscienza delle abitudini delle

[185] Come già usato nei capitoli precedenti, anche qui il termine "*malware*" verrà usato in senso ampio per riferirsi a tutti quei *software* che permettono di commettere illeciti penali, ed in particolare di accedere abusivamente ad un sistema informatico (*hacking tools*), di danneggiare dati o sistemi informatici (*virus, worm, ransomware* ecc.), di eludere misure tecnologiche che proteggono opere dell'ingegno (*cracking tools*) o di intercettare dati informatici (*spyware, trojan horses, key-logger* ecc.).

persone e degli utenti con tecniche di ingegneria sociale per rubare informazioni (*phishing, pharming, vishing* ecc.).

Normalmente tutto ciò avviene attraverso la creazione di appositi *software* malevoli (c.d. *malware*) che non sempre è facile utilizzare e che richiedono, dunque, delle specifiche conoscenze per poter essere utilizzati per commettere dei reati (informatici). Un tempo, quindi, questa tipologia di attività illecita era relegata ad un settore specializzato della criminalità che operava in determinati settori.

Ad oggi, invece, il fiorire dei mercati neri sul *Dark web* ha favorito l'incontro tra la domanda e l'offerta di questi strumenti[186]. A seconda della propria necessità criminale è semplicemente possibile visitare questi mercati virtuali – protetti dall'anonimizzazione e dalla schermatura che può dare un *browser* d'accesso come TOR – e trovare esattamente il *malware* che si desidera per l'occasione più propizia. Questi programmi malevoli sono correlati, al momento dell'acquisto, delle indicazioni specifiche su come utilizzarli e ciò rende possibile – per persone anche non particolarmente esperte – reiterare più volte un comportamento illecito con una semplice serie di *click*.

È ovvio, i *malware* più complessi rimangono in possesso della criminalità informatica più preparata come *hacker*, *cracker* e criminalità organizzata, spesso per commettere atti di matrice terroristica, tuttavia non bisogna sottovalutare la serialità con cui è ad oggi possibile, proprio tramite i programmi malevoli acquistabili su *Internet*, penetrare sistemi informatici o commettere reati contro gli stessi. L'elevata domanda di questi strumenti ha infatti portato ad un aumento dell'offerta con la fioritura del mercato nero di questi dispositivi, spesso con un carattere internazionale e di difficile repressione.

Presi dalla paura – peraltro alimentata dall'originaria incapacità di combattere questo fenomeno – sempre più spesso, negli ultimi anni, organismi internazionali hanno suggerito agli Stati l'adozione di norme atte a reprimere l'utilizzo di *software* con fini malevoli[187].

---

[186] Cfr. LACSON W.-JONES B., The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, in *IJCC*, vol. 10, Issue 1, 2016, 40 ss.

[187] L'art. 83 TFUE richiama anche la criminalità informatica nel settore della criminalità grave e transnazionale. Vedi al riguardo PICOTTI L., *La nozione di ‹‹criminalità informatica›› e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, n. 4, 2011, 827 ss.

Qui si può notare il primo problema e il punto cardine dell'intera questione: un programma, proprio come una pistola o un farmaco, non è di solito intrinsecamente malevolo. Una pistola, così come un *software*, può essere utilizzata per scopi ludici, ricreazionali o di difesa ma anche per commettere delitti particolarmente gravi. La creazione di programmi informatici, di base, è una condotta neutra che non va a ledere un qualche bene giuridico specifico (ad eccezione dei *malware* esclusivamente ed appositamente creati per commettere illeciti ma non sono la maggioranza).

Queste nuove incriminazioni coprono l'intrinseca pericolosità di questi programmi che, per loro natura, se nelle mani sbagliate possono favorire la criminalità, incentivando il proliferare di reati cibernetici.

La dottrina tedesca ha coniato un apposito termine per riferirsi a questa tipologia di norme incriminatrici, attualmente conosciute come "*software-Delikte*"[188]. Il loro centro focale è la pericolosità propria di questi programmi che ne rappresenta l'oggetto materiale del reato. Anche l'Italia non è stata a guardare e nel corso degli anni si è moltiplicata la normativa che prende il nome di "diritto penale dei *software*" a cominciare dalla disciplina atta a tutelare le opere coperte da *copyright* nei confronti degli strumenti rivolti a violare le misure poste a loro protezione, seguita da quella che colpisce i programmi atti a falsificare monete, carte filigranate o eventuali altri mezzi di credito e di pagamento o la disciplina di contrato all'accesso abusivo ad un sistema informatico o telematico ecc.

L'obiettivo di questa intera disciplina è quello di impedire o, comunque, ostacolare la creazione di *malware* che poi verranno utilizzati per commettere più gravi reati a tutela di beni giuridici di una certa rilevanza. In poche parole, questa materia si inserisce nel diritto penale c.d. "preventivo" cercando non tanto di reprimere condotte illecite già avvenute quanto di evitare la loro commissione futura[189]. Questa scelta legislativa è il frutto della natura stessa della tipologia di

---

[188] Si noti il primo utilizzo di tale termine ad opera di POPP A., *§* 202c StGB und der neue Typus des europäischen ‹‹Software-Delikts››, in *GA* 2008, 375 ss. che si inserisce a commento della fattispecie introdotta nell'ordinamento tedesco con il 41. *StrÄndG* del 7 agosto 2007, di cui al § 202c *D-StGB*.

[189] Vedi PICOTTI L., *Sicurezza, informatica e diritto penale*, in DONINI M.- PAVARINI M. (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, 217 ss., 221 ss. La dottrina tedesca si era già spesa, però, sulla materia dei reati preventivi in questa particolare tipologia di reati e si rimanda agli scritti di WOHLERS W., Deliktstypen des Präventionsstrafrechts. Zur Dogmatik „moderner"

reati che si intende contrastare: sia a livello nazionale che internazionale, infatti, gli studi criminologici sottolineano non solo la difficoltà di repressione di questi reati ma anche di individuazione dei responsabili essendo, spesso, fattispecie complesse che si articolano nell'opera di più persone – anche in Stati diversi – che sono particolarmente specializzate e che contribuiscono al risultato finale[190].

Come tale, la soluzione più logica fu quella di cercare di reprimere i reati prima che questi potessero essere attuati, togliendo agli stessi agenti la strumentazione necessaria per agire. Il legislatore non solo si è trovato costretto ad abbandonare la tipica forma del reato "d'evento" ma anche a superare i soliti criteri per punire una condotta a titolo di tentativo così come quelli per il concorso di persone nel reato[191]. Si è preferito scegliere nella fenomenologia delle condotte di reato quelle che manifestavano un oggettivo valore prodromico o di preparazione alla commissione dei reati nella rete: così facendo l'autorità di polizia può intervenire in un momento anticipato e non quando il danno sia già avvenuto. Al contempo, però, il legislatore si trova davanti ad una difficoltà non ignorabile. Come si è precedentemente detto, infatti, quasi tutti i *software* possono essere utilizzati, a seconda dei casi, con intenti positivi o negativi. In origine era facile riferirsi unicamente a quei programmi che sono creati specificatamente per commettere atti illeciti (per l'appunto, i *malware* come *virus*, *worm*, *trojan horse*, *spyware* ecc.) e che vanno a colpire beni giuridici considerati meritevoli di tutela di natura penale (la riservatezza e la sicurezza informatica, il patrimonio ecc.).

Sappiamo da quanto si è sopra detto, però, che la criminalità informatica si evolve ad una velocità incredibile e che, seguendo le normali tecniche legislative, si rischia di andare incontro ad un invecchiamento della normativa, trovandosi degli

---

Gefährdungsdelikte, Berlin, 2000, passim; e HASSEMER W., Sicherheit durch Strafrecht, in *ZIS*, 2006, 266 ss.; tale materiale ha ispirata la nostra dottrina nazionale che vi fa espresso riferimento in DONINI M., *Sicurezza e diritto penale. La sicurezza come orizzonte totalizzante del discorso penale*, in DONINI M.-PAVARINI M. (a cura di), *Sicurezza*, cit., 11 ss., 14 ss., che mostra come la sentita necessità di garantire una maggiore sicurezza alla collettività abbia fondamentalmente favorito il passaggio da uno Stato di diritto ad uno Stato di prevenzione.

[190] Per una più approfondita analisi delle organizzazioni criminali che opera sul web si rimanda a BROADHURST R.-GRABOSKY P.-ALAZAB M.-CHON S., Organizations and Cyber Crime: An analysis of the Nature of Groups engaged in Cyber Crime, in *IJCC*, vol. 8, *Issue* 1, 2014, 1 ss.

[191] Cfr. PALAZZO F.C., *Il tentativo: un problema ancora aperto? (Tipicità ed offesa tra passato e futuro)*, in AA. VV., *Scritti in onore di Francesco Coppi*, I, Torino, 2011, 247 ss., 259, che ha teorizzato la tipizzazione in forma autonoma di ‹‹segmenti comportamentali›› come reati prodromici al perfezionamento del reato finale.

articoli non più capaci di dare una vera e propria forma di tutela. Per evitare questo pericolo il legislatore fa riferimento ad un linguaggio tecnico-informatico di più ampio respiro così da permettere l'interpretazione delle norme e garantire la sopravvivenza senza dover incorrere di volta in volta ad un continuo aggiornamento. Così facendo, però, non è sempre facile o scontato andare ad individuare le condotte incriminate e l'interesse che si intende proteggere da un pericolo sottostante. Da una parte si ha la necessità di utilizzare termini volutamente elastici e, dall'altra, si deve considerare la necessità di garantire il principio di determinatezza-tassatività della norma stessa. È chiaro come il principale pericolo sia quello di incriminare programmi informatici che non siano oggettivamente dannosi. È qui, in particolar modo, che si inserisce la nostra trattazione.

Alcuni *software* che vengono usati per commettere attività illecite possono essere utilizzati anche per scopi del tutto legali. Come esempio si può prendere un programma informatico utilizzato per criptare determinati *files*, atto solitamente a proteggere il bene della riservatezza informatica nascondendo dietro una chiave di criptazione informazioni che si vogliono proteggere o non rendere di facile fruizione. Questi stessi programmi, però, potrebbero benissimo essere utilizzati per criptare determinate informazioni o l'intero computer di un altro soggetto senza il suo consenso, chiedendo poi un riscatto per sbloccarlo o restituire quanto si sia reso impossibile da raggiungere (questi *software* prendono il nome di *ransomware*, dando anche il nome a questa nuova fattispecie criminosa)[192].

Non è chiaramente un'attività semplice quella di distinguere i *software* pericolosi che possono essere utilizzati per commettere reati da quelli che, invece, sono benevoli.

Nell'ambito del "diritto penale dei *software*" ci si ritrova davanti a due principali inconvenienti a cui si è già fatto riferimento: da una parte, se si adottasse una tecnica di incriminazione troppo restrittiva, rivolta a punire solamente i programmi creati per commettere un reato, non si riuscirebbe a reprimere realmente tutti quegli intenti criminali che utilizzano *software* di natura neutra,

[192] Si tratta della tipologia di attacco impiegata nei noti casi *WannaCry* e *NotPetya* del 2017.

finendo per sanzionare solo pochissime ipotesi quasi scolastiche, visto che non esistono quasi mai *malware* esclusivamente creati per scopi unicamente illeciti[193].
Una tecnica di incriminazione troppo estensiva, al contrario, finirebbe per colpire anche tutte quelle condotte che non hanno una natura offensiva o che comunque non sono rivolte a commettere specificatamente fatti illeciti. Così facendo, si rischierebbe di punire fenomeni che non solo sono legittimi ma che, anzi, sono intrinsecamente inseriti all'interno della realtà fenomenica del settore informatico per migliorare non solo la sicurezza delle reti ma anche quella dei sistemi informatici o telematici in generale[194].
Si andrebbe ingiustificatamente a reprimere il settore dell'*Information and Communication Technology* (da ora in poi "*ICT"*) che non potrebbe sviluppare quell'insieme fondamentale di programmi atti a testare gli stessi *software* posti a difesa dei sistemi informatici o telematici (come antivirus o *firewall* ecc.). Commettere una simile leggerezza causerebbe un "*chilling effect*" sulle aziende dell'*ICT*, rallentando se non ostacolando l'evoluzione tecnologica in tutti i campi dell'informatica (*e-mail, cloud computing, home banking, social network, smart working* ecc.)[195].

2.0 Cos'è un *dual use software?*

Non è così semplice dare una risposta a questa domanda. I "*dual use software*" vanno incontro ad un gran numero di significati diversi[196]. Innanzitutto, tale locuzione viene interpretata per riferirsi ai beni e ai prodotti sia di carattere civile che militare e, per esempio, possiamo trovare un simile riferimento nel Regolamento 428/2009/CE che tenta una definizione affermando che per ‹‹prodotti a duplice uso›› si devono considerare ‹‹i prodotti, inclusi i *software* e le

[193] Si veda per una trattazione più approfondita CLOUGH J., Principles of Cybercrime, 2ª ed., Cambridge, 2015, 135.
[194] *Ibidem*.
[195] Si rimanda alla formulazione del § 202c D-StGB, BORGES S.-STUCKENBERG C.F.-WEGENER C., Bekämpfung der Computerkriminalität. Zum Entwurf Strafrechtsänderungsgesetzes
zur Bekämpfung der Computerkriminalität, in *DuD*, 2007, 275 ss., 277.
[196] Cfr. WETTER A., Enforcing European Union Law on Exports of Dual-use Goods, Oxford, 2009; TUCKER J.B., Introduction, in ID (ed.), Innovation, Dual Use and Security, Managing the Risks of Emerging Biological and Chemical Technologies, Cambridge, 2012, 1 ss., 2.

tecnologie, che possono avere un utilizzo sia civile che militare; essi comprendono tutti i beni che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari[197]››. Chiaramente, però, questo non è il nostro ambito d'applicazione.

Altra terminologia, invece, si riferisce al concetto di "duplice uso" nei confronti di quei materiali, beni, prodotti, *hardware* o informazioni che possono essere utilizzati sia per fini legittimi che per la produzione illecita di armi (che siano chimiche o nucleari)[198].

È palese, ormai, come il concetto di duplice uso è di ampio respiro ed in generale si riferisce a tutti quei beni o prodotti che possono avere due distinti utilizzi – tradizionalmente uno lecito ed uno illecito – e che per questo devono essere sottoposti ad una disciplina particolarmente stringente così da garantirne, ove possibile, un uso corretto che, da una parte, assicuri la sicurezza degli altri ma che, allo stesso tempo, non freni lo sviluppo o la produzione di quei beni a fini legittimi.

Certamente anche le nuove tecnologie dell'informazione e della comunicazione (da ora in avanti "TIC") non potevano sfuggire allo stesso destino e tra di essi non possono non menzionarsi i *software* – il cui tema è già stato precedentemente introdotto – che sono particolarmente osservati per la loro possibile carica lesiva.

Il già indicato Regolamento 428/2009/CE, che si occupa specificatamente della materia, faceva riferimento espresso ai *software* e, nonostante questo, non citata neanche una volta quelli a "duplice uso" nell'allegato specificativo[199].

Proprio questa non chiara lacuna legislativa a livello internazionale e comunitario ha portato i vari Stati ad adottare apposite discipline che hanno cercato di risolvere il problema posto dall'incriminazione di questi programmi informatici.

Ma, esattamente, cosa sono i "*dual use software*"? Tale definizione è tecnicamente usata per indicare tutti quei programmi informatici che non hanno

---

[197] Si è citato l'articolo 2, n. 1) del Regolamento (CE) n. 428/2009 del Consiglio, che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso.

[198] *Ibidem*.

[199] Le altre categorie elencate erano: materiali nucleari, impianti ed apparecchiature (cat.0); materiali speciali e relative apparecchiature (cat. 1); trattamento e lavorazione di materiali (cat. 2); materiali elettronici (cat. 3); calcolatori (cat. 4); telecomunicazione e "sicurezza dell'informazione" (cat. 5); sensori e laser (cat. 6); materiale avionico e di navigazione (cat. 7); materiale navale (cat. 8); materiale aerospaziale e di propulsione (cat. 9).

un'evidente o tacita pericolosità ma che possono essere ben utilizzate al contempo per fini illeciti o leciti. A questa terminologia si possono ricollegare due gruppi: 1) i *software* multifunzionali e 2) i *software* multiscopo[200].

Nella prima categoria si fanno rientrare tutti quei programmi che sono intrinsecamente capaci di svolgere più funzioni tra le quali una è solamente rivolta alla commissione di un illecito. Per semplificare: il *software* si maschera come un programma benevolo ma, in realtà, nasconde nel suo codice un c.d. "*payload*", una funzione che mira specificatamente a cagionare un danno o ad eseguire qualche attività in maniera abusiva (prendere il controllo dell'elaboratore, copiare determinate informazioni ecc.). Tra i tanti esempi che potrebbero essere fatti al riguardo vi era anche VLC *Media Player* che tra le molteplici funzioni assolutamente lecite ne nascondeva anche una che permetteva la riproduzione dei DVD aggirandone alcune restrizioni e permettendo così la visione di determinato materiale contraffatto. In questo specifico caso, bisogna prima di tutto capire se la funzione benevola prevalga su quella malevola o viceversa così da poter correttamente definire i *software* multifunzionali. Se, infatti, la funzione malevola è quella principale il programma può essere correttamente definitivo come *malware* e fatto rientrare come oggetto materiale di reato[201].

I *software* multiscopo sono, invece, quelli a cui finora ci si è prettamente riferiti. Si parla, infatti, di programmi che possiedono più scopi e che potrebbero benissimo essere utilizzati, a seconda della volontà dell'utilizzatore, sia per fini legittimi che illegittimi. Prendiamo come esempio pratico gli *hacking tool*, cioè quell'insieme di strumenti che vengono solitamente utilizzati per penetrare all'interno di un sistema informatico o telematico. Questi programmi prendono il loro nome dal fatto che sono i "migliori amici" degli *hacker* in quanto gli permettono di aggirare le misure di sicurezza di un *computer* (come, d'altronde, un grimaldello permette ad uno scassinatore di entrare all'interno di un domicilio o di aprire una cassaforte). Essi, però, possono essere e vengono anche utilizzati per lo scopo esattamente opposto: le aziende dell'ICT, infatti, li usano per testare

[200] Tale suddivisione è stata suggerita da ALBRECHT M., Die Kriminalisierung von Dual-Use-Software, Berlin, 2014, 18.
[201] Vedi *infra*, capitolo III, § 3.4.1, per una più dettagliata trattazione.

le loro misure di sicurezza, così da rendersi conto di quanto un loro prodotto sia sicuro in modo da poter riparare eventuali vulnerabilità riscontrate.
Allo stesso tempo, su ordine di un giudice, la polizia giudiziaria potrebbe usare gli stessi strumenti per penetrare nel computer di una vittima d'omicidio così da entrare in possesso di informazioni che potrebbero rivelare di più sul delitto appena commesso.
In poche parole i *software* multiscopo variano la loro funzione a seconda dell'obiettivo del proprio utilizzatore: le aziende dell'informatica svolgono "*penetration test*" per elevare i propri livelli di sicurezza, mentre gli *hacker* cercano di creare sempre nuovi *malware* che gli possano permettere di aggirare queste misure in una sorta di continua corsa agli armamenti. Se si incriminassero indistintamente tutti questi *software* si andrebbe a causare un danno alla stessa industria dell'informatica. Ad esserne lesi, infatti, sarebbero soprattutto coloro che questi programmi informatici li creano alla luce del sole per fini illeciti, non certamente gli *hacker* di cui spesso neanche si conosce l'esatta ubicazione.
Nel criminalizzare i *software* multiscopo (che è la categoria di *dual use software* che a noi interessa maggiormente ai fini di questa trattazione a causa dei più netti caratteri di complessità e criticità nella materia) il legislatore deve fare particolare attenzione a non cagionare un "*chilling effect*". Per forza di cose si dovrà valorizzare il movente che spinge il soggetto attivo ad agire, colpendo quindi solo quegli agenti che sono spinti da un fine illecito.
Un compito decisamente non facile e un distinguo sul quale si tornerà più avanti[202].

3.0 Tutela a livello sovranazionale

Si è già accennato come la disciplina attuale riguardante i *software* pericolosi si deve in gran parte a normativa dei vari Stati che, però, è stata ispirata dalla normativa a livello sovranazionale con un'implementazione degli obblighi riguardanti questa materia. Alcune volte queste normative sono così dettagliate che sono state direttamente inserite all'interno degli ordinamenti nazionali, tant'è

[202] Si rimanda ad *infra*, capitolo III, § 3.4.2, 3.4.3, 3.4.4 e 3.6 per una più esaustiva trattazione.

che in molti aspetti la disciplina dell'intera materia trattata risulta essere quasi armonizzata.

Come spesso accade nel modello sovranazionale, in realtà, difficilmente si tende ad imporre agli Stati di punire determinati comportamenti con lo strumento penale, lasciando la decisione al legislatore nazionale riguardo al tipo di sanzione a cui ricorrere (penale, civile o amministrativa). Non ci si deve stupire, quindi, se in alcuni Stati europei la stessa condotta sia vista come un illecito amministrativo mentre in altri sia un illecito penale.

Le principali fonti sovranazionali ad oggi esistenti che trattano del tema dei *dual use software* e a cui si farà soprattutto riferimento sono quelle in ambito europeo: da una parte il Consiglio d'Europa, dall'altro l'Unione Europea. Si tenderà, in particolar modo, a compiere un'analisi di tipo comparatistico, ove possibile e necessario, al fine di verificare se le diverse modalità di applicazione della normativa tra i vari paesi siano dovute a scelte politico-criminali o a più banali errori di traduzione come alcune volte sembra essere.

3.1 Convenzioni del Consiglio d'Europa

Nell'ambito del Consiglio d'Europa si sono adottati due strumenti con cui cercare di spingere gli Stati membri a sviluppare una disciplina eterogenea nell'ambito dell'oggetto dei programmi informatici.

Il primo è stata la Convenzione Europea sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato[203] nella quale si imponeva ai Paesi membri di sanzionare i comportamenti posti in essere per finalità commerciali in favore dei suddetti oggetti[204]. In quest'ambito si citavano dei ‹‹dispositivi illeciti›› nei quali si dovevano ricomprendere anche ‹‹i programmi per elaboratori elettronici concepiti o adattati al fine di rendere possibile l'accesso

[203] Convenzione di Strasburgo del 24 gennaio 2001.

[204] Vi rientrano la "fabbricazione", la "produzione", l'"importazione", la "distribuzione", la "vendita", il "noleggio", il "possesso", l'"installazione", la "manutenzione", la "sostituzione" di ‹‹dispositivi illeciti ovvero nel fare promozione commerciale, marketing o pubblicità››.

in forma intellegibile ad uno dei servizi senza l'autorizzazione del fornitore di servizi››[205].

Decisamente più famosa, invece, è la spesso citata Convenzione *Cybercrime*[206] che richiede agli Stati membri di punire chi, per commettere un reato informatico, ‹‹vende››, ‹‹distribuisce››, ‹‹mette a disposizione›› o ‹‹possiede›› codici d'accesso, *password* o programmi informatici ‹‹principalmente concepiti o destinati alla commissione›› di crimini informatici dannosi per la riservatezza informatica, la disponibilità e l'integrità di dati o di sistemi informatici di quelli previsti dagli articoli 2 e 5 della Convenzione di Budapest.

3.2 Decisioni quadro e direttive dell'Unione Europea

Non potevano mancare direttive sulla questione anche nell'ambito più ristretto dell'Unione Europea: in particolar modo, il primo accenno alla questione si trova nella Direttiva 91/250/CE, poi modificata dalla Direttiva 2009/24/CE a riguardo della protezione giuridica dei *software*.

Queste disposizioni richiedevano ai Paesi membri di adoperarsi al fine di adottare delle misure di repressione e sanzione nei confronti di tutti quei comportamenti aventi ad oggetto un mezzo qualunque ‹‹unicamente inteso a facilitare›› la rimozione abusiva o l'aggiramento di misure di sicurezza possibilmente applicate a difesa di programmi informatici[207].

Sotto l'aspetto della protezione dei servizi ad accesso condizionato l'Unione Europea si era mostrata anche più avanti rispetto al Consiglio d'Europa, anticipando la disciplina specifica della Convenzione di Budapest del 2001 con la Direttiva 98/84/CE che, all'articolo 4, lettera a), conteneva il precetto per gli Stati membri di adottare tutte le formule necessarie (questa volta di natura strettamente penalistica) per contrastare le condotte svolte ‹‹a fini commerciali››[208]. Ai fini

[205] Art. 2, lett. d) della sopra citata Convenzione di Strasburgo del 24 gennaio 2001.
[206] Convenzione di Budapest del 23 novembre 2001.
[207] Direttiva 2009/24/CE, art. 7, par. 1, lett. c).
[208] Le condotte richiamate erano quelle di "fabbricazione", "importazione", "distribuzione", "vendita", "noleggio", "possesso", "installazione", "manutenzione" e "sostituzione" di dispositivi illeciti o di "impiego" di comunicazioni commerciali al fine di pubblicizzare tali strumenti. Non si può ignorare una somiglianza con le condotte che poi verranno in seguito richiamate dalla Convenzione di Budapest del 2001.

della specificazione dell'oggetto del reato, nei ‹‹dispositivi illeciti›› rientravano tutte le apparecchiature elettroniche o, per meglio dire, ‹‹i programmi per elaboratori elettronici concepiti o adattati al fine di›› permettere l'introduzione logica all'interno di un sistema protetto da misure di sicurezza.

Altro riferimento ai *software* multiscopo si riscontra nella Direttiva 2001/29/UE, riguardante l'armonizzazione di alcuni aspetti del diritto d'autore all'interno della società dell'informazione. In questo specifico caso si richiedeva che tutti gli Stati membri si assumessero la responsabilità di reprimere le solite condotte già richiamate di ‹‹fabbricazione››, ‹‹distribuzione››, ‹‹vendita››, ‹‹importazione››, ‹‹noleggio››, ‹‹pubblicità per la vendita o il noleggio›› e di ‹‹detenzione a scopi commerciali›› delle apparecchiature (tra cui rientrano anche i *software*), componenti o prodotti che rientrassero nell'‹‹oggetto di una promozione, di una pubblicità o di una commercializzazione›› per finalità di aggiramento di misure di protezione "efficaci" o ‹‹principalmente progettati, prodotti, adattati o realizzati con la finalità di›› permettere o semplificare l'aggiramento di queste stesse misure[209].

Tale formulazione, in realtà, è stata più volte ripresa in ambito europeo tanto da ritrovarsi anche nel settore del terzo pilastro[210].

Tra le diverse disposizione si può far riferimento, per esempio, alla Decisione quadro 2000/382/GAI sul ‹‹rafforzamento della tutela per mezzo di sanzioni penali e altre sanzioni contro la falsificazione di monete in relazione all'introduzione dell'euro››, da poco sostituita dalla Direttiva 2014/62/UE. Tale direttiva contiene l'imposizione per gli Stati membri di sanzionare il fatto di ‹‹produrre fraudolentemente, ricevere, ottenere o possedere strumenti, oggetti ovvero programmi o dati informatici che sono per loro natura particolarmente atti a falsificare o alterare monete››[211].

Altra ipotesi un tempo appartenente al terzo pilastro è la Decisione quadro 2001/413/GAI riguardante la lotta contro le frodi e la falsificazione dei mezzi di

[209] Direttiva 2001/29/UE, art. 6, n. 2, lett. a) e b).

[210] I pilastri furono istituiti nel 1992 con il trattato di Maastricht. Il terzo, in particolar modo, riguardava ‹‹la cooperazione nei settori della giustizia e degli affari interni (CGAI), divenuta, in seguito alle modifiche introdotte dal Trattato di Amsterdam, cooperazione di polizia e giudiziaria in materia penale››.

[211] Direttiva 2014/62/UE, art. 3, par. 1, lett. d).

pagamento diversi dai contanti. Questa disposizione prevede, infatti, che si debbano punire le condotte di ‹‹produzione fraudolenta o ricevimento, ottenimento, vendita o cessione ad altri di programmi di computer appositamente allestiti per la perpetrazione della contraffazione e della falsificazione di strumenti di pagamento ai fini della loro utilizzazione fraudolenta ovvero programmi di computer il cui scopo sia la commissione di una frode informatica››[212].

Si sarebbe potuto far riferimento anche alla Decisione quadro 2005/222/GAI ad oggi, però, sostituita dalla Direttiva 2013/40/UE che cerca di reprimere – attraverso la trasposizione della disciplina nella normativa degli Stati membri – il comportamento di coloro che, ‹‹intenzionalmente e senza diritto››, ‹‹fabbricano, vendono, procurano approvvigionamenti per l'utilizzazione, importano, distribuiscono o mettono a disposizione un programma per computer destinato o modificato principalmente al fine di commettere un illecito contro la riservatezza informatica, l'integrità o la disponibilità di dati o di sistemi informatici di cui agli artt. 3 e 6››[213].

4.0 Bilancio critico su quanto finora fatto a livello sovranazionale

A un primo sguardo si rilevano, quindi, ben due Convenzioni del Consiglio d'Europa e un numero non indifferente di provvedimenti dell'Unione Europea che cercano di regolamentare, dove possibile, questa complessa quanto spinosa disciplina. Da un'analisi comparatistica di queste disposizioni si può trarre una differenziazione abbastanza netta tra i *software* che sono: a) ‹‹principalmente concepiti o adattati per commettere o facilitare la commissione di un reato››; b) ‹‹oggetto di una promozione, di una pubblicità o di una commercializzazione con

[212] Decisione quadro 2001/413/GAI, articolo 4. In essa, sebbene le traduzioni non coincidano perfettamente (soprattutto quella francese ed inglese), si riesce comunque ad evincere come la volontà del legislatore europeo fosse quella di scegliere i *software* configurati oggettivamente per commettere reati. Tale interpretazione è avallata dal testo tedesco e spagnolo che si riferiscono in modo più letterale a questa formulazione.

[213] Direttiva 2013/40/UE, articolo 7. Bisogna sottolineare come la scelta di traduzione italiana si discosta da quella di tutte le altre lingue. Nella versione italiana, infatti, parrebbe che si voglia porre l'accento sulla volontà del soggetto che ha appositamente creato o adattato quel programma informatico quando, invece, sembrerebbe che il legislatore europeo avesse inteso sanzionare il *software* oggettivamente creato o adattato dal programmatore per commettere o facilitare la commissione di un reato (informatico).

la finalità di commettere o facilitare la commissione di un reato››; c) ‹‹il cui scopo consiste nel commettere o facilitare la commissione di un reato››.

Per cercare di evitare un eccessivo ampliamento della disciplina, i provvedimenti che suggeriscono o obbligano all'adozione di queste disposizioni contengono, alcune volte, anche il riferimento alla locuzione ‹‹abusivamente››, che in questa specifica materia deve essere tradotto come "senza diritto"[214]. Tale riferimento è estremamente importante non solo perché incide sull'elemento soggettivo del reato ma anche sullo stesso fatto-base, diventando il punto cardine della materia[215].

Ma sono questi elementi sufficienti a risolvere la problematica dei *dual use software*? Nei prossimi paragrafi si proverà proprio a rispondere a questa domanda, dovendo in particolar modo denotare l'efficacia di questi provvedimenti riguardo alla rilevanza penale conferita alle condotte illecite lesive per determinati beni giuridici e allo stesso tempo la necessità di garantire adeguata impunità a tutti quei comportamenti che, invece, sono legittimamente svolti dai soggetti che operano nel settore ICT per quanto riguarda la tutela ed il rafforzamento delle misure di sicurezza ai sistemi informatici e telematici.

Durante l'analisi degli attuali tentativi di risoluzione della diatriba si partirà dalla differenziazione tra "*software* multifunzione" e "*software* multiscopo" e si scenderà successivamente nella differenziazione interna tra le tre categorie che si sono appena trattate nel corso di questo stesso paragrafo[216].

4.1 Programmi informatici ‹‹concepiti o adattati per commettere o facilitare la commissione di un reato››.

Sia concesso partire dalla prima classe che è stata sopra esposta, quella dei programmi informatici che sono stati espressamente pensati e poi creati o adattati

[214] Si è già trattato estensivamente l'argomento *supra*, capitolo II, § 2.0.1.1, a cui si rimanda per maggiori dettagli.
[215] Vedi *infra*, capitolo III, § 3.0.
[216] Sia concesso dire che queste ultime categorie si adattano maggiormente ai "s*oftware* multiscopo" per via della loro più complessa natura e che verranno utilizzate proprio per facilitare la trattazione della materia nelle parti a questi riferite.

per un fine illecito[217]. In questa categoria rientrano quindi tutti i *software* la cui funzione originaria è quella di commettere un reato (un danneggiamento informatico, un furto d'identità digitale, l'accesso abusivo ad un sistema informatico o telematico ecc.). Non si può non notare come sia importante l'elemento soggettivo del reato in questo specifico caso visto che l'originario creatore aveva in mente un piano ed un'idea ben chiara da realizzare, allo stesso tempo però non si deve cadere nell'errore di dare un'eccessiva importanza a questo elemento. La volontà, infatti, è un criterio molto vago che è difficile da ricostruire *a posteriori*. È dunque necessario trovare degli elementi sul piano oggettivo che permettano di riscontrare *ex ante* l'intenzione del soggetto agente riflessa nel reato. Risultano importanti, alla luce di quanto detto, tutti quegli elementi intrinseci al programma informatico (come il suo codice o l'algoritmo di funzionamento) che rendano possibile svelare la vera anima di questo strumento nei confronti della commissione di un fatto illecito. Non si deve, però, ricadere nella semplicista affermazione che più un *software* è pericoloso e più questo deve essere per forza stato pensato per commettere un reato. Anche in questo caso si dovrà considerare fin dal principio la sua base di partenza, iniziando proprio dalla volontà dei suoi creatori e dalla sua effettiva capacità di cagionare o semplificare l'esecuzione di un reato, cosa che si riflettere sulla sua oggettiva configurazione.

È facile notare come questa corrente di pensiero sia stata appositamente formulata per escludere dal novero di questi *software* quelli che non sono stati originariamente creati per commettere un reato nonostante la loro virtuale offensività: un programmatore in buona fede, ad esempio, che lavora su di un *malware* per *penetration test* alla luce del sole per un'azienda di sicurezza informatica.

Risalta all'occhio, però, come, per quanto corretta, questa formulazione legislativa scopra il fianco a numerose critiche e vulnerabilità. Escludiamo per un momento i dilemmi più lampanti legati alla possibilità di riscontrare nel programma informatico elementi che senza dubbio indichino come esso sia stato pensato o meno per commettere un reato. Ne restano molti altri a partire dal fatto che un *software* eventualmente capace di cagionare un reato, anche se pensato all'origine

[217] Questa tipologia di formulazione si ritrova sia nella Direttiva 2001/29/UE sia nella Convenzione sulla tutela dei servizi ad accesso condizionato voluta dal Consiglio d'Europa.

in buona fede, poi continua ad esistere e nulla impedisce che possa successivamente essere trafugato o messo sul mercato nero dai suoi stessi creatori in cerca di facile guadagno. Resta, infatti, l'offensività di questo vero e proprio *malware* che farebbe rientrare negli estremi dell'incriminazione penale chiunque si ritrovi in possesso dello stesso successivamente, che abbia o meno intenti illeciti (come un *Data Protection Officer* – di seguito semplicemente DPO – che si procuri il programma dall'azienda IT per testare i meccanismi di difesa approntati dall'impresa per cui lavora, un vero e proprio *hacking tool* sebbene se lo sia procurato per scopi legali e positivi).

Per evitare di scoraggiare la creazione di questa tipologia di programmi informatici a fini legali è necessario che alla materia sopra esposta si affianchino altre disposizioni che chiariscano la questione una volta per tutte. I *software* non solo, per non rientrare nella disciplina repressiva, non dovrebbero essere creati a fini illeciti ma non dovrebbero essere neanche utilizzati successivamente per commettere reati. Così facendo non si impedirebbe la loro creazione né, d'altra parte, alle aziende IT di commercializzare questi strumenti facendoli finire nelle mani di soggetti senza intenti malevoli.

Ancora una volta, però, questa apparente soluzione appena esposta presenta non pochi problemi che si riscontrano non appena ci si fermi un attimo a riflettere sulla natura della stessa. Cercando, ancora una volta, di ignorare le difficoltà che facilmente incorrerebbero nel ricercare i criteri di valutazione dell'originale fine legittimo che non solo ha portato alla nascita di quel programma informatico ma anche alla sua successiva vendita ed utilizzazione, altra criticità sarebbe legata al fatto che non rientrerebbe nell'ambito della condotta sanzionabile l'operato di colui che, pur creando un *software* a fini illeciti, nascondesse tale funzione sotto molte altre assolutamente lecite (si parla, quindi, di *software* "multifunzionale" in questo caso). Essendo una funzione "secondaria" non si potrebbe dire che il programma fosse stato pensato esclusivamente per commettere un reato, eludendo così la disciplina con estrema facilità.

L'idea di far dipendere tutto dalla idoneità criminosa del programma informatico affiancata dall'originale motivazione del suo creatore non può essere adeguata alla garanzia di una sufficiente precisione sull'oggetto materiale in queste ipotesi

punitive, andando eccessivamente a far affidamento sulla mistione di non ben specificati elementi soggettivi ed oggettivi.

4.2 Programmi informatici ‹‹principalmente concepiti o adattati per commettere o facilitare la commissione di un reato››

Si è precedentemente detto come alcune normative sovranazionali richiedano ai Paesi membri di punire i *software* pensati e creati "principalmente" per commettere un reato[218]. Se la disciplina elencata al paragrafo precedente sembrava più correttamente dedicata ai "*software* multifunzionali", questa modalità di formulazione normativa meglio si adatta ai "*software* multiscopo" – sebbene non si debba commettere l'errore di tagliare fuori una delle due categorie – e si differenzia per il fatto che si richiede esplicitamente la "principale" concezione del programma informatico per una propensione all'attività criminale.
Per rientrare all'interno di questa categoria, dunque, un programma informatico dovrà essere stato pensato quasi esclusivamente per commettere un determinato delitto o una serie di reati informatici[219]. Si è scritto "quasi esclusivamente" perché questo è il termine più corretto.
Molto a lungo in seno al Consiglio d'Europa si discusse, prima di adottare la Convenzione di Budapest del 2001, se optare per l'incriminazione di quei *software* creati "esclusivamente" per commettere un reato o solo per quelli che sono stati "principalmente" pensati per quello scopo[220]. Alla fine si scelse la seconda opzione perché la prima sembrava fin troppo stringente: in sede processuale, infatti, ci si sarebbe dovuti imbattere nella grande difficoltà, data dalla definizione, di quando un programma informatico sia "esclusivamente" pensato o adattato per la commissione di un reato, finendo per portare a differenziazioni che avrebbero ridotto di molto la portata della norma e dunque la

[218] Si ricordino il precedentemente citato articolo 6 della Convenzione di Budapest del 2001, l'articolo 3, numero 1, lettera d) della Decisione quadro 2000/383/GAI, l'articolo 6, numero 2, lettera c) della Direttiva 2001/29/UE ed anche l'articolo 7 della Direttiva 2013/40/UE.
[219] V. ALBRECHT M., op. cit., 178, 181.
[220] Così si legge in Council of Europe, Explanatory Report, cit., par. 73.

sua tutela penale (soprattutto non potendo in alcun modo adattarsi alla disciplina dei *dual use software* che sarebbero stati, dunque, tagliati fuori)[221].

Non si volle, però, ricadere anche nell'errore esattamente opposto di dare vita a un eccessivo ambito di criminalizzazione che avrebbe portato tutti i *software* potenzialmente capaci di permettere la commissione di un reato ad essere ritenuti illeciti (compresi, quindi, tutti quelli a "duplice uso").

Nel tentativo di trovare un compromesso che non scomodasse nessuno si optò per aggiungere la locuzione "principalmente", creando così una formulazione maggiormente elastica che si sperava avrebbe permesso una corretta applicazione della normativa solo a quei *software* realmente dannosi.

Se, però, questa clausola si sarebbe potuta adattare bene ai "*software* multifunzione", non si può dire lo stesso per quanto riguarda i "*software* multiscopo": un programmatore può creare il codice di un programma informatico affinché, molte volte, svolta più funzioni o serva a perseguire diversi obiettivi. Non rientrerebbero, quindi, nella categoria quei programmi in cui la funzione illecita è meno importante della altre (potendo essere usato sia per scopi legittimi che illegittimi) o quei programmi pensati in origine per fini leciti ma che vengano poi convertiti alla criminalità da un secondo o terzo utilizzatore che ne entri in possesso.

Il riferimento alla locuzione "principalmente" che avrebbe dovuto risolvere qualsiasi problema, in realtà, non ne risolve nessuno perché non è un criterio oggettivamente capace di precisare in modo pratico l'oggetto materiale del reato (basterebbe, per un programmatore in malafede, dare più scopi al proprio *software* per evitare che questo venga definito "principalmente" rivolto alla commissione di un reato).

Ancora una volta, per non incorrere nella punibilità anche dei creatori di programmi malevoli in buona fede, ci si dovrebbe rivolgere a criteri di natura soggettiva che tutto sono fuorché capaci di delimitare oggettivamente l'ambito d'applicazione di un reato. I redattori della Convenzione di Budapest del 2001, però, non trovarono altra soluzione e quindi si assiste alla presentazione di un "dolo specifico" in cui il fatto deve anche essere sorretto dall'intenzione di

[221] Cfr. ALBRECHT M., op. cit., 182

commettere un reato contro la riservatezza informatica, l'integrità o la disponibilità di dati o di sistemi informatici di altri (i c.d. *CIA offence*)[222]. Tale obiettivo è reso palese proprio nel rapporto esplicativo alla Convenzione che si riferisce all'intento di non andare a colpevolizzare la creazione di *malware* a fini positivi da parte delle aziende nel settore ICT[223].

Così facendo, prevedendo questo particolare elemento soggettivo, si riesce anche a coprire il comportamento di coloro che mettono a disposizione o vendono ad un terzo il proprio programma affinché sia lui ad utilizzarlo successivamente per scopi illeciti[224]. Almeno per questo caso, dunque, il dolo specifico si è dimostrato prettamente opportuno al fine della corretta esplicazione della norma[225].

Seguendo questa strada è indifferente che il *software* sia ancora nella signoria del suo originario creatore o finisca nelle mani di altro soggetto agente, responsabilizzando in un certo senso anche le aziende ICT che programmano questi *software*. Bisogna ammettere, però, che questo dolo specifico non copre tutte le modalità di applicazione del fatto nella realtà materiale delle cose. Per esempio, non può in alcun modo riferirsi a quelle imprese informatiche che, dopo aver creato un programma capace di permettere la commissione di un reato, lo vadano a cedere non tanto al fine della commissione dell'illecito ma per trarre un mero profitto economico dalla sua vendita o diffusione. In questo modo non si potrebbe in alcun modo sanzionare quella serie di comportamenti che rendono possibile la circolazione, soprattutto nel mercato nero, di questa tipologia di prodotti.

Il medesimo problema si riscontrerebbe nel caso in cui il programmatore mettesse semplicemente il *software* disponibile in rete, ponendolo virtualmente alla mercé di persone che potrebbero utilizzarlo per compiere un reato. In entrambi i casi, infatti, non basterebbe ad integrare l'ipotesi richiesta dal dolo specifico il fatto che il produttore abbia immaginato che tale programma informatico potesse essere

[222] Cfr. Council of Europe, Explanatory Report, cit., par. 73.
[223] Cfr. Council of Europe, Explanatory Report, cit., par. 76.
[224] Si ritrova la stessa formulazione nella Direttiva 2013/40/UE che ha ad oggetto la repressione degli attacchi informatici. In questa previsione si richiede agli Stati membri di punire un discreto numero di comportamenti aventi ad oggetto un programma informatico malevolo a patto che l'agente lo utilizzi con l'intenzione di commettere un accesso abusivo o un'intercettazione informatica o un danneggiamento di dati o di sistemi informatici.
[225] Si rimanda *infra*, capitolo III, § 5.2.

usato in malo modo, essendo necessaria l'espressa volontà del suo creatore di dar vita ad un *software* allo scopo chiaro e principale di commettere o rendere più facile la commissione di un reato (non rientrandovi le ipotesi in cui, invece, si persegue un profitto di qualche tipologia)[226].

Un'altra tipologia di approccio, comunque molto simile, è quella contenuta nella Direttiva 2014/62/UE che ha come fine quello della protezione della moneta unica, imponendo ai Paesi membri di sanzionare le condotte aventi ad oggetto ‹‹programmi informatici che per loro natura sono "particolarmente atti" alla contraffazione o all'alterazione di monete››.

A differenza dell'ipotesi precedente il legislatore europeo ha cercato di meglio chiarire la questione non tanto prevedendo un dolo specifico quanto richiedendo la "fraudolenza" del comportamento posto in essere[227]. Tale formulazione ha, però, delle altre criticità dato che tale fraudolenza viene normalmente interpretata come ‹‹allo scopo di commettere una truffa››[228], escludendo dunque tutte quelle imprese e aziende che operano regolarmente nel mercato in ambito ICT (e che quindi non agiscono con lo scopo specifico di ingannare o di commettere una truffa)[229].

Bisogna, però, sottolineare come nell'ambito dell'ordinamento italiano, per quanto riguarda ad esempio l'articolo 617-*quater* c.p. ("intercettazione, impedimento o interruzione illecita di comunicazione informatiche o telematiche"), l'avverbio "fraudolentemente" sia stato utilizzato per connotare la condotta tipica in materia di disvalore senza riflessi sull'elemento soggettivo del reato[230]. In questo modo sembrerebbe possibile escludere dal novero delle

---

[226] Non bisogna però escludere in maniera automatica che il dolo specifico non sia mai compatibile con il dolo eventuale. V. PICOTTI L., *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, 595 ss., 608 ss.

[227] Il riferimento alla "fraudolenza" non è qualcosa che viene spesso rinvenuta negli ordinamenti europei ma che appartiene, invece, specificatamente al nostro ordinamento nazionale che lo richiama più volte in diversi reati (come, ad esempio, l'articolo 617-*quater* c.p. in materia di intercettazione fraudolenta di comunicazioni informatiche o telematiche).

[228] Cfr. ALBRECHT M., op. cit., 200.

[229] Sempre ALBRECHT M., op.cit., 201, che a sostegno di questa teoria richiama addirittura una comunicazione della Commissione Europea relativa alla Decisione quadro 2001/413/GAI nella quale si proponeva di dare rilevanza penale ai comportamenti aventi ad oggetto i programmi informatici destinati a commettere una falsificazione di monete.

[230] PICA G., *Diritto penale delle nuove tecnologie.* Computer's crimes *e reati telematici*, Internet, *banche dati e* privacy, Torino, 1999, 117; PECORELLA C., *Sub art. 617*-quater *c.p.*, in DOLCINI E.-MARINUCCI G. (a cura di), *Codice penale commentato*, III, IV ed., Milano, 2015, 670 ss., 673.

fattispecie di reato le condotte di coloro che producano, cedano o entrino in possesso dei *software* malevoli atti a testare le proprie misure difensive contro attacchi su sistemi informatici o reti telematiche.

4.3 Programmi informatici ‹‹oggetto di una promozione, di una pubblicità o di una commercializzazione con la finalità di commettere o facilitare la commissione di un reato››

La seconda categoria di tecniche normative utilizzate in ambito sovranazionale[231] si differenzia da quanto detto finora in modo abbastanza marcato. Non si cerca più di dare importanza, infatti, alla volontà del programmatore al fine di riempire di significato la "principale" funzione del *software* che deve essere stato creato o adattato alla commissione di un reato, quanto si sottolinea la circostanza che questo venga diffuso apertamente o pubblicizzato come un *hacking tool* specificatamente pensato per commettere reati.
L'obiettivo non è quello di reprimere la messa a disposizione di programmi informatici che siano realmente in grado di essere offensivi quanto, piuttosto, quello di sanzionare coloro che reclamizzino un loro prodotto – indipendentemente dal suo contenuto – affermando che con esso possa essere commesso un crimine (informatico).
Il legislatore europeo, in questo ambito, sembra aver gettato direttamente la spugna e davanti alle difficoltà di segnalare quando un programma informatico sia realmente ed oggettivamente dannoso ha preferito punire chiunque vada a pubblicizzare un *malware* capace (virtualmente) di commettere o facilitare la commissione di un reato.
Se ad una prima analisi, sbrigativa, questa formulazione sembrerebbe priva di imperfezioni nella sua limitatezza in realtà anch'essa ha diverse vulnerabilità. Applicando pedissequamente questo criterio, infatti, si punirebbe anche colui che produce e pubblicizza uno strumento informatico (magari sottolineando proprio le sue capacità offensive) per permettere alle aziende di eseguire un "*penetration*

[231] Indicate nella Direttiva 2001/29/UE (riguardante il diritto d'autore) all'articolo 6, numero 2, lettera c).

test" particolarmente valido. Dall'altro lato, invece, non potrebbe essere punito l'*hacker* che crea davvero un pericolosissimo programma informatico per il solo e semplice fatto che, pur avendolo messo in circolazione, non vada in alcun modo a reclamarlo come tale (spacciandolo per altro o nascondendo la sua vera funzione).

4.4 Programmi informatici ‹‹il cui scopo consiste nel commettere o facilitare la commissione di un reato››

L'ultima categoria sembrerebbe riferirsi quasi specificatamente ai "s*oftware* multiscopo" dato che pone l'accento proprio sullo ‹‹scopo›› del prodotto[232].
Lo "scopo" – così come il "fine" – è un termine che si lega alla volontà con cui le persone agiscono e per quale obiettivo. Parte della dottrina tedesca sottolinea come questo concetto, essendo fin troppo legato alla volontà, non potrebbe in alcun modo essere applicato ad un oggetto ma debba invece sempre ruotare intorno ad una persona che può utilizzare gli oggetti per "scopi" diversi a seconda della sua finalità[233].
Ancora una volta, esattamente come i programmi concepiti o adattati per perseguire un reato, lo "scopo" di un *software* potrebbe legarsi ed essere specificato da dati statistici[234]: di volta in volta, quindi, si dovrebbe procedere alla scelta di quei programmi informatici che più spesso vengono utilizzati per commettere un reato. È chiaro che così facendo, però, ci si troverebbe di fronte a non poche perplessità sull'oggetto materiale del reato.
Prima di tutto si finirebbe per sanzionare anche le persone che magari utilizzano quel *software* a fini leciti e solo perché la maggioranza dei soggetti, invece, lo adopera per fini illegittimi[235]. Allo stesso tempo un programma potrebbe avere delle funzionalità estremamente pericolose che sono, però, a conoscenza solo di un ristrettissimo gruppo di criminali informatici mentre tutti gli altri lo utilizzano

[232] Troviamo diversi riferimenti alla materia a partire dalla Decisione quadro 2001/413/GAI (sulla lotta alla frode e alla falsificazione dei mezzi di pagamento), articolo 4, par. 2, così come nella Direttiva 2014/22/UE sulla protezione della valuta unica europea e di altre monete.
[233] Cfr. ALBRECHT M., op. cit., 188.
[234] *Ibidem*.
[235] Cfr. ALBRECHT M., op. cit., 189, nota 462.

in buona fede (cosa che andrebbe ad escludere il *software* dal novero statistico dei prodotti informatici utilizzati soprattutto per uno scopo illecito).
Questa formulazione appare fin troppo legata all'elemento soggettivo, dovendosi dare maggiore importanza, invece, alla pericolosità intrinseca del programma informatico che dipende dal suo codice o dall'algoritmo contenuto nella sua matrice.
Facendo un esempio, non si può dire che il *software* TOR sia pericoloso solo perché molte persone lo utilizzano per accedere al *DarkNet* e commettere fatti illeciti, al massimo gli si può conferire questa definizione perché l'anonimizzazione ed il suo essere una palese e conosciuta porta al mondo del *Dark web* lo rendono particolarmente pericoloso proprio per il suo codice di programmazione.
Tale categoria normativa si pone, in un certo senso, in modo diametralmente opposto rispetto ai programmi informatici ‹‹creati o adattati per commettere reati›› poiché se in questi si dava la massima importanza all'elemento oggettivo qui, invece, si sottolinea solo l'elemento soggettivo.
È vero, questa definizione permetterebbe di restringere il numero di *software* perseguibili solo a quelli che per natura ed uso sono utilizzati per commettere atti criminali ma ciò non escluderebbe dal novero di soggetti punibili i tecnici dell'informatica che utilizzano questi programmi per fini leciti, magari usando un *malware* conosciuto per "stressare" le proprie misure di sicurezza aziendali.
Per cercare di restringere il piano applicativo di questa norma si dovrebbe aggiungere anche in questo caso il dolo specifico all'elemento soggettivo del reato, chiedendo che questi specifici prodotti – statisticamente usati per scopi illeciti – vengano utilizzati per commettere o facilitare la commissione di un reato da parte del soggetto agente al fine d'essere considerati rilevanti ai fini della repressione penale.

5.0 L'incriminazione dei "*dual use software*" nel diritto penale

Nei paragrafi precedenti si è fatto riferimento a una serie di prescrizioni derivanti dal Consiglio d'Europa o dall'Unione Europea che imponevano l'adozione di

diverse norme, che in effetti lo sono state. Si è quindi assistito a un proliferare di legislazioni sia di *common law* che di *civil law* che hanno avuto come loro fondamento tutte quelle condotte precedentemente indicate che ricadevano su dati e programmi informatici pensati, creati o adattati per rendere possibile la commissione di un reato (informatico).

Si è anche già accennato che non sempre gli organismi sovranazionali hanno imposto la repressione di queste condotte tramite il diritto penale, lasciando ampio spazio di manovra ai singoli Paesi membri per poter scegliere tra una sanzione di tipo penale, amministrativa o civile che fosse. L'unica richiesta che veniva fatta era quella di seguire il principio di adeguatezza, quindi adottare discipline che fossero efficaci, persuasive e proporzionate.

Per esempio, la Direttiva 98/84/CE riguardante la protezione dei servizi ad accesso condizionato – in particolare tramite il divieto di un ventaglio di comportamenti con oggetto ‹‹programmi per elaboratori elettronici competi o adattati›› per permettere l'accesso abusivo ad un sistema protetto – è stata da molti ordinamenti recepita tramite l'utilizzo della strumentistica penale[236]. Si è deciso di seguire molto da vicino la formulazione che il legislatore sovranazionale aveva suggerito, mantenendone la forma.

Non sempre, però, si è risolta la questione in maniera così semplice e armonica. A seconda della propria tradizione di diritto, infatti, gli Stati hanno optato non solo per gravità di sanzione diverse ma anche per forme differenti di repressione dell'attività criminosa.

Prima di concentrarci specificatamente su come la questione si è presentata in Italia, converrà soffermarsi sul destino delle altre normative sovranazionali che hanno bene o male trattato l'argomento dei prodotti "a duplice uso" e di come esse si siano andate a tradurre nel tempo nei principali ordinamenti europei.

---

[236] Troviamo tale fattispecie, ad esempio, in Spagna (art. 286.1, n. 1, CP), nel Regno Unito (S. 297A(1)(b) *Copyright, Designs and Patents Act 1988*; di seguito CDPA), in Austria (§ 10 *Zugangskontrollgesetz-ZuKG*), in Lussemburgo (art. 2, 2), l. 2 agosto 2002) e in Belgio (art. 3.1, *Loi concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel relatifs aux services de la société de l'information*, 12 maggio 2003). Il legislatore tedesco ha invece preferito ricorrere alla sanzione amministrativa (§ 5 della *Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten* (ZKDSG) del 19 marzo 2002).

5.1 Nel diritto comparato

Continuando sul solco scavato nelle righe precedenti possiamo fare riferimento, ad esempio, alla Direttiva 91/250/CE – ad oggi sostituita dalla Direttiva 2009/24/CE – in materia di tutela dei *software* che richiedeva agli Stati membri di reprimere la condotta avente ad oggetto qualunque elaboratore o programma informatico ‹‹unicamente inteso a facilitare›› la rimozione abusiva o l'aggiramento di misure di sicurezza eventualmente applicate ad un programma informatico.

Si è visto, anche in questa fattispecie, che molti Paesi hanno deciso di sanzionare la condotta criminosa con una sanzione di tipo penalistico[237], considerata la più adatta a raggiungere l'obiettivo anche se non specificatamente richiesta dal legislatore sovranazionale.

In questo specifico caso si è deciso di restare quanto più possibile legati alle disposizioni comunitarie, adottando anche le stesse definizioni che si ritrovano ad oggi in vari ordinamenti. Ad esempio, il legislatore spagnolo reprime all'articolo 270, par. 3, CP sp. il comportamento di coloro che fabbricano, importano, distribuiscono o possiedono un mezzo qualunque (anche un *software*, quindi) ‹‹specificatamente destinato›› alla soppressione abusiva di misure di sicurezza a protezione delle opere d'ingegno.

Per cercare di delimitare l'ambito di applicazione della norma – che scontava tutte le imprecisioni che si sono sopra descritte riguardo all'ambito di incriminazione tra ciò che è lecito e ciò che non lo è – la dottrina spagnola aveva pensato di affiancarsi a quella parte dell'interpretazione che riteneva la condotta concernente esclusivamente quei *software* la cui "unica" funzione fosse quella di danneggiare o distruggere le misure di sicurezza poste a protezione delle opere coperte da

[237] Scelta adottata dal legislatore italiano (art. 171-*ter*, lett. f-*bis*), l. dir. aut. e succ. mod.), francese (art. L335-3-1, II, 2 *Code de la propriété intellectuelle*), austriaco (§§ 90b, 91 *Urheberrechtsgesetz* (UrhG), svizzero (Art. 69a, lett. b), n. 3, *Bundesgesetz über das Urheberrecht und verwandte Schutzrechte*- URG), belga (Art. XI.291 § 1r, *Code de droit économique*), ed inglese (S. 296ZB *CDPA*). Il legislatore tedesco, come al solito, ha invece punito le condotte concernenti i menzionati programmi informatici con la sanzione amministrativa della multa (§§ 95a, Abs. 3, 111a, Abs. 1, b), *Gesetz über Urheberrecht und verwandte Schutzrechte- UrhG*).

copyright[238]. In virtù di questo non sarebbe rientrato nella fattispecie il comportamento di coloro che fabbricano, vendono o dispongono di un programma informatico avente anche altre funzionalità. Allo stesso tempo, dal punto di vista dell'elemento soggettivo si richiedeva anche che queste condotte fossero messe in atto per un fine prettamente commerciale[239].

Tale norma è però andata incontro, come molte altre, alla riforma organica del codice penale spagnolo avvenuta con legge 30 marzo 2015, n. 1, che ha accolto l'opinione della dottrina maggioritaria. Si è deciso, in particolare, di rimuovere il riferimento all'"esclusività" della condotta all'interno dell'art. 270, par. 6, CP sp. per sostituirlo con ‹‹qualunque mezzo principalmente concepito, prodotto, adattato o realizzato per›› facilitare la commissione di un reato, a fini commerciali, legato alla lesione di un prodotto per elaboratori elettronici o altre opere coperte da *copyright* e protette da misure di sicurezza informatiche di qualsiasi genere[240].

Molti ordinamenti europei hanno ormai recepito e inserito all'interno del proprio ordinamento la Convenzione di Budapest del 2001, in particolar modo hanno accettato di impegnarsi – per quello che ci interessa – nella repressione delle condotte di ‹‹produzione, vendita, procurarsi per l'utilizzo, importazione, distribuzione, rendere disponibile o anche il solo mero possesso di programmi informatici "principalmente concepiti o destinati" per la commissione di reati (in particolar modo i c.d. CIA *offense*). Si faccia riferimento, ad esempio, sempre all'ordinamento spagnolo che nella riforma già citata del 2015 ha introdotto nel suo codice penale gli articoli 197-ter, par. 1, lett. a) e 264-ter, par. 1, lett. a)

---

[238] BARREIRO JORGE A., *Sub art. 270 CP*, in MOURULLO RODRIGUEZ G. (dir.), Comentarios al Código penal, Madrid, 1997, 776; RUS GONZÀLEZ J.J., Delitos contra el patrimonio y contra el orden socioeconómico (VIII). Delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores, in COBO DEL ROSAL M. (coord.), Curso de Derecho penal español, Parte especial, II ed., Madrid, 2005, 569 ss., 582. *Contra* GONZÀLEZ GOMEZ A., El tipo básico de los delitos contra la propiedad intelectual. De la reforma de 1987 al Código Penal de 1995, Madrid, 1998, 204.

[239] Come richiesto dall'articolo 102, lettera c), LPI.

[240] Cfr. MUNOZ GALÀN A., *La reforma de los delitos contra la propiedad intelectual e industrial*, in QUINTERO OLIVARES G. (dir.), *Comentario a la reforma penal de 2015*, Navarra, 2015, 585 ss., 593 ss., in specie 596 ss.

riguardanti le condotte con oggetto gli *hacking tools* ed i *software* malevoli ‹‹concepiti o adattati principalmente per commettere reati (informatici)››[241].

In Germania, invece, con il 35. *StrÄndG* del 2003 si è data attuazione alla Decisione quadro 2001/413/GAI (riguardo alle frodi e alle falsificazioni nei sistemi di pagamento). Il legislatore tedesco ha deciso di colpire il comportamento di colui che, al fine di compiere una frode informatica, produce, si procure, vende, cede o custodisce *software* ‹‹il cui scopo è di commettere›› un reato di truffa[242].

Nel tentativo di non incriminare anche i *dual use software* la dottrina ha cercato di restringere il campo di applicazione della norma solo a quei programmi informatici che abbiano come ‹‹scopo essenziale›› quello di rendere possibile un reato di frode. Si cerca dunque di restringere l'oggetto materiale del reato solo a quei programmi specificatamente pensati o modificati per falsificare monete o per eseguire una frode informatica. Vengono così salvati, invece, tutti quei *software* che oggettivamente sono pericolosi e che potrebbero essere utilizzati anche per finalità illecite ma che per la loro configurazione interna sono per lo più rivolti a perseguire obiettivi legittimi[243].

Anche la dottrina tedesca è incappata nelle stesse criticità, però, che si sono precedentemente sottolineate per la normativa sovranazionale. Non esistono, infatti, programmi informatici che abbiano il fine oggettivo di perseguire reati[244]. Pensiamo a un'applicazione che permette di compiere un accesso ad un sistema informatico o telematico e che sia stata appositamente pensata dall'*hacker* per

---

[241] In ottemperanza alle richieste della Convenzione anche il codice belga ha introdotto norme aventi ad oggetto strumenti per permettere la commissione di un reato di intercettazione informatica (art. 341-bis, § 2-bis CP), di accesso abusivo ad un sistema informatico ovvero di danneggiamento di dati o di sistemi informatici (art. 550-bis, § 5 CP). La legge 18 dicembre 2013, n. 410, ha modificato l'art. 323-3-1 CP fr., prevedendo la punibilità di chi, illegittimamente o comunque per ragioni non riconducibili alla ricerca o alla sicurezza informatica, importa, offre, cede, mette a disposizione ovvero detiene un dispositivo, dati o programmi informatici destinati o specialmente adatti a commettere un accesso abusivo ad un computer (art. 323-1 CP) o un danneggiamento informatico (artt. 323-2 e 323-3 CP). Altro esempio è dato dal § 126c, Abs. 1, Z. 1, Ö-StGB che sanziona un ampio ventaglio di condotte concernenti un programma informatico che, per le sue caratteristiche intrinseche, è stato evidentemente creato o adattato per commettere reati informatici.

[242] Cfr. POPP A., § 202c StGB, cit., 375 ss.; HILGENDORF E.-VALERIUS B., Computer-und Internetstrafrecht, 2. Aufl., Berlin-Heidelberg, 2012, 171 ss.; EISELE J., Computer- und Medienstrafrecht, München, 2013, 47 ss.

[243] CORNELIUS V. K., Zur Strafbarkeit des Anbietens von Hackertools, in CR, 2007, 682 ss., 687; HILGENDORF E.-VALERIUS B., Computer- und Internetstrafrecht, cit., Rn. 530, 158.

[244] V. POPP A., § 202c StGB, cit., 388; TIEDEMANN K.-VALERIUS B., § 263a StGB, cit., Rn. 84, 392.

sfruttare le vulnerabilità di un elaboratore elettronico per fini illeciti, potrebbe essere utilizzata anche dalla polizia giudiziaria per introdursi in un *computer* al fine di trovare informazioni capaci di rivelare la posizione di un pericoloso criminale o salvare la vita di un ostaggio (dunque con fini nobili e resi leciti, magari, dal provvedimento di un giudice). In questo caso la norma, così come scritta nel codice tedesco, non si potrebbe applicare perché mancherebbe la volontà di introdursi in un sistema usando il programma informatico con fini illeciti[245].

Per tornare all'argomento trattato nella disciplina tedesca di riferimento, quello della frode informatica, è chiaro che un programma informatico potrebbe essere intrinsecamente capace di permettere la commissione della frode, ma se si dovesse esclusivamente seguire un criterio oggettivo si finirebbe per reprimere anche le condotte di soggetti che creano questi *software* per finalità assolutamente lecite[246]. Proprio per evitare di cadere in questo errore una parte della dottrina ha sposato la teoria dell'importanza dell'elemento soggettivo, prevedendo che il programma informatico per poter essere sussunto ad oggetto della fattispecie debba essere stato volutamente pensato e creato o adattato per commettere un reato o rendere possibile ad altri, tramite cessione, tale commissione[247]. In poche parole, si cerca di far riferimento a un non ben chiaro criterio per il quale il *software* dovrebbe essere stato specificamente destinato dal suo produttore o possessore alla commissione di una frode informatica.

5.2 Nel diritto penale italiano

Nel nostro ordinamento si ritrovano sette norme che incriminano l'utilizzo di un programma informatico come oggetto materiale di un reato in cui un *software* è utilizzato per fini illeciti: tra queste, quattro sono situate all'interno del codice

[245] Cfr. DUTTGE G., § 263a StGB, cit., Rn. 35, 1528.
[246] Cfr. DUTTGE G., Vorbereitung eines Computerbetruges. Auf dem Weg zu einem "grenzlosen" Strafrecht, in FS-Weber, Bielefeld, 2004, 285 ss.; *idem* CRAMER P.-PERRON W., § 263a StGB, in SCHÖNKE A.-SCHRÖDER H. (Hrsg.), Strafgesetzbuch, 28. neu bearb. Auf., München, 2010, Rn. 33, 2388.
[247] CORNELIUS K., Zur Strafbarkeit, cit., 687 s.; EISELE J., Payment Card Crime: Skimming, in CR, 2011, 131 ss., 134.

penale mentre le restanti nel diritto complementare, specificatamente sparse nella normativa riguardante il diritto d'autore.

Sia permesso intraprendere l'analisi proprio dalle fattispecie che sono contenute nel nostro codice penale e che sono poste a tutela della fede pubblica (articolo 461 c.p.), dell'inviolabilità del domicilio (articoli 615-*quater* c.p. e 615-*quinquies* c.p.) e dell'inviolabilità dei segreti (articolo 617-*quinquies* c.p.).

Il primo riferimento a questa tipologia di reato trova riscontro nel nostro ordinamento ben prima della normativa del legislatore europeo con la legge 23 dicembre 1993 n. 547. Molti di questi articoli sono già stati diffusamente analizzati nel corso del capitolo II della presente trattazione, qui si cercherà quindi di riprendere solo i temi più vicini e affini ai *dual use software* in modo da ampliarli e in caso mettere in luce sia criticità che eventuali soluzioni che sono state adottate dalla giurisprudenza e dalla dottrina nel corso del tempo, partendo dalle scelte legislative fatte.

Si incominci dall'articolo 615-*quater* riguardante la ‹‹detenzione e diffusione abusiva di codici d'accesso a sistemi informatici o telematici››[248]. La norma sanziona il comportamento prodromico – preparatorio – all'esecuzione del più grave reato di accesso abusivo ad un sistema informatico o telematico di cui all'articolo 615-*ter* c.p[249]. Le condotte sanzionate sono di due tipi e riguardano l'entrare in possesso di codici di accesso o *software* o altri strumenti che siano in grado di far accedere ad un sistema protetto da misure di sicurezza ovvero il "fornire" questi stessi mezzi a soggetti terzi[250].

Queste condotte devono essere poste in essere in modo "abusivo"[251], dunque senza autorizzazione o cause di giustificazione[252]. Secondo alcuni l'utilizzazione

---

[248] Per la trattazione si rimanda *supra*, capitolo II, § 1.2. Si è speso sull'analisi critica dell'articolo anche PECORELLA C., *Diritto penale dell'informatica*, rist. agg., Padova, 2006, 356 ss.

[249] Si rimanda sempre a quanto già trattato *supra* e a SALVADORI I., *L'accesso abusivo ad un sistema*, cit., 125 ss.

[250] Da notare come non si vada ad incriminare la semplice detenzione o possesso di questi mezzi, essendo necessaria una condotta attiva di procurarseli in qualche modo. Bisogna sottolineare, però, come sia ormai pacifico che il "procurarsi" sia una condotta necessariamente prodromica al mero possesso, andando dunque a ricomprendere questa fattispecie nella condotta come sottolineato da D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, in AA. VV., *Profili penali dell'informatica*, 1994, 39 ss., 81; SALVADORI I., *I reati di possesso*, cit., 7.

[251] Si è già diffusamente trattato l'argomento *supra*, capitolo II, § 1.1.1.

[252] Cfr. MARINI G., *Delitti contro la persona*, Torino, II ed., 1996, 390; MANTOVANI F., *Dir. pen.*, PS, I, V ed., Padova, 2013, 575.

di questo termine sarebbe ridondante se accostato alle condotte illecite già elencate, poiché queste ultime sarebbero di per sé in grado di distinguere le attività illegittime da quelle lecite. Tale formulazione è stata scelta, però, perché il legislatore credeva che restringere i comportamenti considerati lesivi solo alle condotte di coloro che agiscano allo scopo di trovare un profitto o cagionare un danno avrebbe permesso una ancor più chiara delimitazione. Ciò, tuttavia, non si è dimostrato corretto nella pratica.

Si è più volte fatto riferimento al comportamento di quelle aziende nel settore ICT che basano il loro intero *business* sulla produzione e la commercializzazione di programmi informatici malevoli che vengono poi venduti alle imprese per permettere di compiere i *penetration test* necessari alla valutazione del livello interno di sicurezza informatica. Ora, non si può dire che questa condotta non andrebbe a rientrare nella fattispecie di cui all'articolo 615-*quater* c.p. visto che queste aziende operano con un fine di profitto. È per questo che si decise di fare riferimento alla nota dell'abusività, proprio per evitare che queste attività lecite e propositive finissero per essere criminalizzate ingiustamente. Non si può considerare penalmente rilevante la condotta di un DPO che acquisti un *malware* per eseguire un *test* sui sistemi operativi dell'impresa per cui lavora fintanto che lo faccia nei limiti imposti dalla legge, dall'autorizzazione che gli è stata concessa e delle norme extrapenali che regolano l'attività di chi lavora nel settore della sicurezza informatica. Il riferimento all'abusività in quanto clausola di antigiuridicità speciale, quindi, prima ancora di avere un riscontro nell'ambito della soggettività pone le proprie basi nell'elemento oggettivo del reato[253]: la condotta che si va a tenere non può essere considerata illecita fintanto che si muove nei confini imposti non solo dalle mere cause di giustificazione ma da tutto quell'insieme di nome – penali ed extrapenali – che regolano l'attività nel settore professionale in cui l'agente opera[254].

---

[253] Come tale si potrà considerare illecita solo la condotta dell'agente che sia a conoscenza dell'abusività del suo agire poiché nell'elemento del dolo rientra la conoscenza della normativa di riferimento. ROMANO M., *Pre-Art. 39/63-64,* in *Commentario sistematico del Codice penale,* 3ª ed. rinn. e ampl., Milano, 2004, 324; PULITANÒ D., *Illiceità espressa e illiceità speciale*, in *Riv. it. dir. proc. pen*, 1967, 65 ss., 73; MORGANTE G., *L'illiceità speciale nella teoria del reato*, Torino, 2002, 27 ss., 30 ss., 61 ss.

[254] PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, n. 2, 2005, 189 ss., 197.

In generale non si è fatto un riferimento particolare ai *software* multifunzione o a quelli multiscopo avendo deciso il legislatore italiano, nell'alveo di questa norma, di sanzionare indistintamente i programmi informatici "idonei" a commettere il reato di accesso abusivo ad un sistema informatico o telematico. L'intera distinzione tra ciò che è lecito e ciò che è illecito, infatti, è data dal riferimento al carattere dell'abusività e al dolo specifico appositamente richiamato per definire la condotta del soggetto agente.

Il secondo articolo che viene in rilievo è il 615-*quinquies* c.p., anch'esso già ampiamente definito in precedenza e che sanziona la condotta di chi ‹‹diffonde programmi diretti a danneggiare o interrompere un sistema informatico››[255].

Salta subito all'occhio come sembrerebbe che il legislatore abbia voluto punire solo le condotte di coloro che mettono a disposizione di altri questi programmi informatici e si è già discusso di come ciò parrebbe più che altro da riportare ad una svista del legislatore.

Quello che più interessa, però, è la mancanza del riferimento all'"abusività" e dunque al carattere dell'azione dell'agente. Da una parte vi rientrano tutti i *software* aventi lo scopo – cosa che si è già notato non funzionare particolarmente a livello sovranazionale – e per di più "aventi l'effetto" di danneggiare dati o sistemi informatici altrui.

Il riferimento all'evento non solo crea una pericolosa sovrapposizione con il delitto *ex* articolo 635-*bis* che tratta direttamente il "danneggiamento informatico"[256] ma si dimostra anche incapace di distinguere tra le varie tipologie di *malware* e le ragioni per cui possono essere creati. Rientrano apparentemente nella fattispecie, quindi, sia i *software* multifunzione che quelli multiscopo poiché creati per compiere un danneggiamento e ben capaci di poterlo fare (se non fossero idonei a funzionare, nessuno se li procurerebbe per compiere i *penetration test*).

Questa criticità fu più volte sottolineata in dottrina dato che il testo della legge così scritto contrastava con i principi di determinatezza, tassatività ed offensività

[255] Per una più ampia trattazione dell'argomento si rimanda *supra*, capitolo II, § 1.3. In dottrina PECORELLA C., *Diritto penale dell'informatica*, cit., 235 ss.
[256] PECORELLA C., *Diritto penale dell'informatica*, cit., 245 ss.

ed incriminava anche attività di per sé prive di un qualsivoglia disvalore sociale e che, anzi, sono utili alla collettività[257].

La ratifica della Convenzione di Budapest del 2001, avvenuta in Italia con la legge 48/2008, ha modificato questa fattispecie nel tentativo di adeguarla ai livelli di tutela sovranazionali, obiettivo che non è stato però perseguito fino in fondo.

Si è tentato di riavvicinare l'articolo 615-*quinquies* alla fattispecie dell'articolo 615-*quater*, includendo anche la condotta di chi si procura o entra in possesso di questi programmi informatici. Oltretutto si è aggiunta anche la previsione del dolo specifico, omettendo però il riferimento alla clausola di illiceità speciale dell'abusività. Questa mancanza ha creato degli scompensi nella materia che ad oggi si riferisce ancora ai semplici "dispositivi" intrinsecamente pericolosi con condotte assolutamente neutre: è illecito il procurarsi o il mettere a disposizione *malware*, facendo sorreggere il tutto sul fine illecito che si deve perseguire (‹‹allo scopo di danneggiare illecitamente un sistema informatico o telematico››)[258].

Risulta palese che così facendo, però, non si ha una condotta con offensività oggettiva: vi rientra, per esempio, l'azione del programmatore che mettendo a disposizione un programma informatico dannoso per eseguire un *penetration test*, lo facesse consapevole che tale *software* sia in grado di commettere uno dei reati *ex* articolo 615-*ter*, 635-*bis*, 635-*quater*, 635-*quinquies* del codice penale[259].

Altro articolo che si è citato è stato il 617-*quinquies* c.p., introdotto per punire chi ‹‹fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad una sistema informatico o telematico ovvero intercorrenti tra più sistemi›› e che è già stato, anch'esso, precedentemente trattato[260].

Tale fattispecie mostra – già a partire dalla gravità della sanzione, pari a quella che si commina a chi le comunicazioni le intercetta – quanto il legislatore consideri pericolosi i *software* (vi rientrano, ad esempio, *spyware*, *sniffers*, *keylogger*, *trojan horse* ecc.) che permettano, una volta introdotti in un sistema

[257] Cfr. SARZANA C., *Comunità virtuale e diritto: il problema dei* Bullettin Board System, in *Dir. pen. proc*., 1995, 375 ss.; PICOTTI L., *La ratifica della Convenzione* Cybercrime, cit., 708-709.
[258] V. PICOTTI L., op. cit., 709 ss.
[259] Cfr. SALVADORI I., *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. proc. pen*., n. 1, 2012, 204 ss.
[260] Vedi supra, capitolo II, § 2.2.

informatico o telematico, di poter tenere traccia delle informazioni e delle comunicazioni che passano attraverso di esso.

In questo caso il *discrimen* tra ciò che è lecito e ciò che è illecito non è dato dal carattere dell'abusività della condotta né tantomeno dal riferimento ad un dolo specifico, quanto dal fatto che tale comportamento si sia tenuto ‹‹fuori dai casi consentiti dalla legge››, ipotesi che era già stata inserita e impiegata dal legislatore nell'articolo 617-*bis* c.p. con la legge 8 aprile 1974, n. 98.

Nell'articolo appena nominato, riguardante l'installazione di ‹‹apparecchiature atte a intercettare o impedire comunicazioni o conversazioni telegrafiche o telefoniche››, il legislatore con il riferimento ai casi "consentiti dalla legge" intendeva tutto quell'insieme di condotte consentite dall'autorità giudiziaria. Essendo questo il significato attribuito a questa clausola non vi è ragione per considerare "i casi consentiti dalla legge" ed introdotti nell'articolo 617-*quinquies* c.p. in modo diverso. In quest'ambito, però, è chiaro che se si dovesse dare valore solo al significato letterale della clausola il risultato sarebbe quello di estendere l'applicazione della fattispecie di reato anche a tutte quelle condotte solitamente prive di offensività come, ad esempio, l'operare di un amministratore di sistema che installi uno *spyware* nel proprio sistema di rete aziendale per vagliare la corretta funzionalità ed utilizzo delle apparecchiature fornite dall'ufficio ai dipendenti. Anche in questo caso, dunque, sarebbe stato quantomai efficace utilizzare la clausola dell'abusività per meglio delineare l'ambito applicativo di tale norma.

Articolo finora mai nominato, invece, è il 461 c.p. che fu introdotto così come noi oggi lo conosciamo dalla legge 23 novembre 2001, numero 409, per dare attuazione alla Decisione quadro 2000/383/GAI riguardante la tutela contro la falsificazione dell'euro.

Si nota subito come l'impronta del legislatore sovranazionale si faccia sentire in questa materia a partire dalle condotte richiamate: l'articolo sanziona chi ‹‹fabbrica, acquista, detiene, aliena filigrane, strumento o *software* destinati "esclusivamente" alla contraffazione o alterazione di monete […]››.

Essendosi ripetuta *in toto* la terminologia impiegata a livello europeo non si può che sottolinearne le stesse vulnerabilità. Prima tra tutte il fatto che non esiste al

mondo un programma informatico che sia pensato esclusivamente per commettere un reato, figurarsi uno così specifico come quello di contraffare o alterare moneta o altri valori. Così facendo si è reso l'articolo di difficile se non di impossibile applicazione, relegandolo ad una funzione quasi simbolica a causa della sua eccessivamente restrittiva previsione legale.

Per quanto riguarda, invece, la legislazione complementare le tre norme al riguardo si trovano tutte in materia di diritto d'autore. Si farà, dunque, riferimento alla legge 22 aprile 1941, numero 633 (c. d. "l. dir. aut."), così come modificata dal D.lgs 9 aprile 2003, numero 68 per attuale in Italia la Direttiva 2001/29/CE[261].

Partiamo dall'articolo 171-*bis*, comma 1, l. dir. aut. che sanziona ‹‹chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE)›› e con la stessa pena ‹‹il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori››[262].

Il primo carattere di criticità è dato dal fatto che il programma informatico debba essere ‹‹inteso a›› compiere una delle condotte sopra elencate, il problema è che questo termine viene solitamente usato per indicare uno "scopo". A dare un fine ad un oggetto non può essere l'oggetto stesso ma il suo creatore, andando ancora una volta a far ricadere la punibilità di una determinata condotta non su un criterio oggettivo bensì su uno di natura soggettiva. A nulla, oltretutto, valgono i riferimenti all'"esclusività" della funzione malevola che il *software* dovrebbe svolgere: si è, infatti, più volte detto che è quasi impossibile che un programma informatico abbia solo una specifica funzione criminosa, e se anche fosse così basterebbe per un *hacker* programmare il *malware* affinché faccia un'altra cosa qualsiasi per aggirare la previsione legale, circostanza che ancora una volta relega una simile ipotesi ad una funzione meramente simbolica.

---

[261] Si rimanda *supra*, capitolo III, § 3.2.

[262] Su come debba intendersi il requisito della "natura commerciale" di tali condotte si rimanda a FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Milano, 2010, 279 ss.

Altra questione è posta dall'articolo 171-*ter*, comma 1, lettera f), l. dir. aut. che sanziona ‹‹introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto››.

Anche in questo caso si vanno ad incriminare una serie di condotte "neutre" che hanno ad oggetto programmi informatici capaci di accedere illecitamente ad un servizio criptato. Ci si riferisce, quindi, a *software* considerati unicamente per la loro pericolosità intrinseca la cui definizione è legata ad un non ben specificato carattere "commerciale" e per uso non personale[263]. Verrebbero quindi escluse tutte quelle condotte aventi lo stesso identico oggetto ma prive di carattere patrimoniale. Non si potrebbe in alcun modo punire il comportamento di un parente che installi nella televisione del genero un programma in grado di decriptare il segnale specifico di un *decoder* quando ciò avvenga in modo totalmente gratuito. Al contrario, invece, si punirebbero le aziende dell'ICT che vendano o mettano sul mercato strumenti di decodificazione di segnale, solitamente acquistati dalle stesse imprese del settore che forniscono un servizio a pagamento per vagliare la funzionalità e l'efficacia delle misure di criptazione che si sono adottate.

Strettamente collegato è l'ultimo articolo della disciplina complementare che si andrà a trattare, il 171-*ter*, comma 1, lettera f-*bis*), l. dir. aut che punisce chi ‹‹fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-*quater* ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni,

[263] V. FLOR R., *Tutela penale e autotutela tecnologica*, cit., 216 ss., 219.

ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale››.
Esattamente come per tutti gli altri esempi finora riportati, le modalità adottate dal legislatore per distinguere ciò che è illecito dalle condotte che non lo sono, appaiono decisamente poco chiare e non sufficienti a garantire una corretta suddivisione tra i programmi informatici che sono intrinsecamente dannosi o pericolosi ma che, allo stesso tempo, non presentano caratteri di offensività.

6.0 La struttura dei reati il cui oggetto materiale è rappresentato da un *software*

Da quanto si è finora detto si può evincere che l'intenzione del legislatore – nazionale o sovranazionale – sia sempre stata quella di incriminare, ove possibile, condotte aventi ad oggetto programmi informatici malevoli che rendessero possibile la commissione del reato. Così facendo, però, si sono andate a delineare molte prescrizioni che hanno, di volta in volta, avuto come risultato diverse linee di disvalore. Bene o male le condotte che si sono viste si ripetono in un ventaglio specifico costituito da ‹‹produzione, fabbricazione, vendita, distribuzione, messa a disposizione, procurarsi o procurare ad altri per uso, procacciare, acquistare, detenere per scopi personali o commerciali, possedere, approvvigionarsi per l'uso, importare, distribuire, ricettazione, installazione o manutenzione a fini commerciali››.
Nell'alveo della disciplina della tutela del diritto d'autore le condotte si avvicinano tutte quante per il peculiare fattore della commercialità/patrimonialità con cui si ‹‹pubblicizzano, vendono, noleggiano, detengono, duplicano, importano, concedono in locazione›› programmi informatici con cui si possono rimuovere o aggirare servizi a pagamento non pubblici.
In generale, tutte queste condotte e gli articoli che le contengono si rassomigliano a livello sanzionatorio e hanno in comune l'oggetto materiale del reato, pur avendo un diverso grado di disvalore a seconda del bene che si va a ledere con la propria condotta. Alcuni di questi comportamenti sono anche affiancati da un dolo specifico che ne rappresenta l'elemento finalistico. Da uno sguardo

omnicomprensivo, dunque, si possono suddividere tutti gli articoli finora elencati in due categorie.

In una ricadono tutte quelle condotte che sono caratterizzate dall'elemento della signoria sul *software*[264], mentre nella seconda confluiscono quei comportamenti rappresentati dal volontario concedere ad altri tali *software* per la commissione del reato[265].

Bisogna ammettere, però, come la classificazione qui proposta[266] trovi i suoi limiti nella grande versatilità dei programmi informatici che possono rientrare, spesso, in entrambe le categorie a seconda dell'utilizzazione che il suo creatore o possessore deciderà di perseguire. Niente impedisce, allo stesso tempo, di dar valenza a tale differenziazione per semplificare l'argomento che si sta trattando. Da una parte, infatti, essa permette di operare una prima distinzione basandosi sulla pericolosità di un *software* nei confronti del bene giuridico che si vuole tutelare mentre, dall'altra, consente di porre il *focus* dell'argomento sulle scelte politico-criminali del legislatore.

6.1 La signoria su di un *software* "pericoloso"

Quando ci si riferisce alle condotte di "fabbricare", "procurarsi, "acquistare", "detenere", "produrre" e "conservare" un *software* per commettere un reato non si può non notare che tutte hanno in comune l'espressione di un controllo o una proprietà sul programma informatico.

Le fattispecie che rientrano in questa categoria non sono sempre caratterizzate dal dolo specifico, sostanziandosi a volte anche intorno a motivazioni di natura economica o commerciale. Questo fa sì che tali delitti non vedano necessariamente il possesso sul *software* da parte dell'agente come mirante a commettere il delitto ma vi rientrano anche quelle condotte che si sostanziano solo nel metterlo, eventualmente, a disposizione di un terzo in cambio di un ritorno

[264] V. *infra*, capitolo III, § 6.1.
[265] V. *infra*, capitolo III, § 6.2.
[266] Cfr. SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"* in *Rivista italiana di diritto e procedura penale*, , Vol. 60, N. 2, 2017, pag. 747-788.

economico. La dottrina tedesca ha coniato un apposito termine per definire questa tipologia di reati: "reati di connessione" (*Abschließungsdelikte*)[267].

La condotta lesiva del bene giuridico tutelato, quindi, non è propriamente quella del soggetto che ha la signoria sul programma informatico, bensì quella del terzo che si "aggancia" con una sua autonoma condotta lesiva. Tipici esempi sono quelli del programmatore che venda sul *DarkNet* il suo *software* malevolo che può essere poi acquistato o meno con intenti malevoli da parte di terze persone.

Non ha alcuna importanza per la consumazione del delitto in questione che, poi, l'evento avvenga realmente o meno[268].

Se si decidesse di dare maggiore rilievo all'aspetto politico-criminale anziché alla struttura della norma, si potrebbe ben affermare che tutti questi comportamenti caratterizzati dal possesso e controllo su un programma informatico malevolo rientrino nel gruppo dei reati c.d. "ostativi"[269]. Se, invece, ci si concentrasse sulla struttura normativa, il risultato sarebbe quello di considerare questa categoria come reati di pericolo indiretto[270]. Infatti, si tratta di reati che sanzionano, in definitiva, il pericolo di pericolo. Per esempio, acquistando o entrando in possesso di un macchinario capace di contraffare monete si punisce il rischio che successivamente questo strumento possa essere realmente usato per la sua funzione illecita (art. 461, comma 1, c.p.).

Se esiste, però, questa tipologia di reati bisogna anche notare come altri che hanno ad oggetto un programma informatico su cui si esercita una qualche forma di signoria sono invece sostenuti dalla presenza di uno scopo ultimo nella commissione di un qualche reato specifico[271]. Ci riferiamo, dunque, a quei reati

---

[267] Il termine si riscontra per la prima volta in SIEBER U., Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt. Eine Analyse der Vorfeldtatbestände im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten", in NStZ, H. 7, 2009, 353 ss., 358.

[268] *Ibidem*.

[269] Cfr. PAGLIARO A., *Il reato, in Trattato di diritto penale*, PG, diretto da GROSSO C.F.-PADOVANI T.-PAGLIARO A., Milano, 2007, 34; MANTOVANI F., *Dir. pen*., PG, 9ª ed., Padova, 2015, 218; PRADEL J., Droit pénal général, 20ª ed., Paris, 2014, 367 ss.

[270] Cfr. MANZINI V., *Trattato di diritto penale italiano*, I, 2ª ed., Torino, 1920, 686; GRISPIGNI F., *Diritto penale italiano. La struttura della fattispecie legale oggettiva*, II, 2ª ed., Milano, 1952, 77; ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, 176 ss; MARINUCCI G.-DOLCINI E., *Manuale di diritto penale*, PG, 5ª ed., Milano, 2015, 593 ss.; SALVADORI I., *I reati di possesso*, cit., 234 ss.

[271] Cfr. MORGANTE G., *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Torino, 2013, 10 ss., 58 ss.

con al proprio interno un altro reato che costituisca l'oggetto del dolo specifico, come accade nell'articolo 615-*quinquies* del codice penale dove il fatto di "procurarsi" un *software*, di base non pericolosa come condotta, viene punito nel momento in cui ciò avvenga ‹‹allo scopo di danneggiare illecitamente un sistema informatico o telematico››.

Chiaramente non sempre il fine che si vuole perseguire deve essere rappresentato da un reato, potrebbe benissimo sostanziarsi in un'azione assolutamente lecita come accade nell'articolo 615-*quater* c.p. dove, di base, il fine di ‹‹procurare a sé o ad altri un profitto›› non è ingiusto.

In altri casi, invece, in fine che muove la condotta pur non essendo illecito è comunque lesivo di qualche bene giuridico tutelato[272]. L'esempio può essere sempre preso dall'articolo 615-*quater* c.p. dove si sanziona la condotta di chi si procura dei codici di accesso ‹‹al fine di arrecare ad altri un danno››.

Chiaramente in tutte quelle norme dove il legislatore ha deciso di sottolineare il fine della commissione futura di un reato, la signoria sul programma informatico acquista un quanto mai palese carattere di natura preparatoria[273]. Si va a punire la condotta del soggetto agente solo perché con il suo comportamento prepara o, in ogni caso, rende più semplice la successiva commissione di un determinato reato lesivo di beni giuridici tutelati. Si trova un riscontro, per esempio, nella condotta di coloro che pensino e creino un programma informatico malevolo per commettere successivamente un accesso abusivo ad un sistema informatico o telematico: se non si producesse prima il *software*, sarebbe impossibile o molto più complesso realizzare il successivo piano criminoso.

Non è cosa comune, fuori dalla materia del *Cybercrime*, punire le condotte meramente prodromiche alla commissione di un reato, soprattutto se queste ultime non siano neanche sufficienti per rientrare nell'ambito del tentativo di reato[274]. La

---

[272] V. PICOTTI L., *"Dolo specifico"* und Absichtsdelikte. Der sog. Handlungszweck zwischen gesetzlicher Formulierungstechnik und dogmatischen Begriffen, in FS-Frisch, Berlin, 2013, 363 ss., 376 ss.; ID., Zwischen 'spezifischem' Vorsatz und subjektiven Unrechtselementen. Ein Beitrag zur typisierten Zielsetzung im gesetzlichen Tatbestand, Berlin, 2014, 37 ss.

[273] Cfr. SIEBER U., Legitimation und Grenzen, cit., 359, che partendo proprio da questo assunto ha coniato il termine "*Planungsdelikte*". Proprio su quest'ultima categoria di reati hanno scritto SIEBER U.-VOGEL B., Terrorismusfinanzierung. Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht, Berlin, 2015, 140 ss., 147 ss.

[274] V. MARINUCCI G., *Soggettivismo e oggettivismo nel diritto penale. Uno schizzo dogmatico e politico-criminale*, in *Riv. it. dir. proc. pen*., 2011, 1 ss., 9; SEMINARA S., *Il delitto tentato*, Milano,

decisione di dare comunque rilevanza penale a queste condotte rivela la pericolosità e l'offensività che il legislatore – italiano ma non solo – avverte in questi comportamenti prodromici che di per sé non potrebbero essere considerati neanche fatti "pretipici"[275], visto che il semplice atto di procurarsi un *malware* non è certamente un indice valido per considerare la propria condotta criminosa come iniziata (si potrebbero anche aspettare anni prima di utilizzarlo per commettere un reato, magari non lo si userà mai). Tale formulazione normativa è tipica di tutti quei reati che il legislatore, in via del tutto eccezionale, decide comunque di punire autonomamente sebbene rappresentati da meri atti preparatori nel momento in cui essi possano costituire le basi per la commissione di più gravi reati (normalmente in materia di terrorismo ecc.)[276].

Tornando ad analizzare la questione da un punto di vista meramente normativo, dunque, anche questa tipologia di reati "prodromici" rientra nella categoria dei reati di pericolo indiretto[277].

Nell'ordinamento italiano si è deciso di punire alcune condotte in cui l'agente entra in possesso di un *malware* ‹‹al fine di arrecare ad altri un danno›› (come si ritrova, ad esempio, nell'articolo 615-*quater* c.p.). È chiaro come tale comportamento non sia da solo in grado di ledere un bene giuridico tutelato, per farlo è necessario compiere l'ulteriore condotta di utilizzazione di questo programma informatico malevolo ma, ciononostante, si è ritenuto che il "pericolo di pericolo" di una lesione fosse, in questa materia, meritevole d'essere autonomamente incriminato.

6.2 La messa a disposizione di un *software* "pericoloso"

2012, 834 ss.; PICOTTI L., L'élargissement des formes de préparation et de participation, in *Rev. inter. dr. pén.*, vol. 78, 3/4 trim., 2007, 355 ss.; MANTOVANI F., *Dir. pen.*, PG, cit., 434; MARINUCCI G.-DOLCINI E., *Corso di diritto penale*, 1, 3ª ed., Milano, 2001, cit., 598 s.

[275] Cfr. MANTOVANI F., op. cit., 445.

[276] Reati di questo tipo non si ritrovano solo nell'ordinamento italiano. V. JESCHECKJ H.-H.-WEIGEND T., Lehrbuch des Strafrechts, AT, 5. voll. neubearb. u. erweit. Aufl., Berlin, 1996, 523; ESER A., Vorb. § 22 StGB, in SCHÖNKE A.-SCHRÖDER H. (Hrsg.), Strafgesetzbuch, cit., Rn. 13, 404-405; HILLENKAMP T., Vor. § 22 StGB, in LK, 12. neu. bearb. Aufl., I Band, Berlin, 2007, Rn. 7, 1381.

[277] Cfr. SALVADORI I., *I reati di possesso*, cit., 258 ss.

Simile ma differente è la condotta di coloro che, invece, mettono a disposizione questo programma informatico nei confronti di terzi. Ciò può avvenire in molti modi e spesso nelle varie fattispecie si leggono condotte come ‹‹procurare ad altri››, ‹‹comunicare››, ‹‹cedere›› o ‹‹rendere accessibile›› a un certo numero di soggetti un mezzo informatico idoneo a commettere un reato.

In questo specifico caso il creatore del *software* non ha più la signoria sul suo prodotto, lo mette semplicemente a disposizione di soggetti terzi che potranno utilizzarlo per qualsiasi scopo, tra cui quelli illegittimi. Sotto questo punto di vista il comportamento dell'agente è più grave poiché, oltre ad essere irresponsabile, permette ad un numero indefinito di soggetti di compiere ciò che più desiderano visto che, una volta inserito qualcosa sulla rete, difficilmente si riuscirà a ritirarlo dal mercato e la semplicità di duplicazione – anche per via anonima – permetterà a diverse persone di commettere reati spesso con serie ripercussioni per la collettività.

Nella grande maggioranza delle situazioni il creatore del programma informatico è cosciente della pericolosità dello stesso e lo carica in *Internet* sapendo che verrà quasi sicuramente usato per commettere un reato. Così facendo, il soggetto agisce con l'intento di aiutare un terzo per scopi illeciti, anche solo agevolando la sua condotta. In tutto e per tutto il suo comportamento si sostanzia in un contributo materiale che facilita la condotta illecita del terzo[278]. Il nostro legislatore nazionale ha accolto il principio dell'‹‹accessorietà minima›› nell'ambito del concorso di persone nel reato, permettendo di considerare come "concorrente atipico" l'originale possessore di questo programma che poi, ceduto a terzi, ha permesso la commissione del reato[279]. L'agente deve, però, essere consapevole di quello che sta facendo ed agire con il "dolo di partecipazione" ben sapendo non solo che qualcuno potrebbe utilizzare il suo *software* per fini illeciti, ma anche conscio del possibile ventaglio di reati che possono essere commessi[280]. Certo, non sarà richiesto che il "partecipe" sappia esattamente le modalità che verranno

[278] Cfr. STORTONI L., *Agevolazione e concorso di persone nel reato*, Padova, 1981, *passim*.
[279] V. PEDRAZZI C., *Il concorso di persone nel reato*, Palermo, 1952, 22 ss.; INSOLERA G., *Problemi di struttura del concorso di persone nel reato*, Milano, 1986, 8 ss.; SEMINARA S., *Tecniche normative e concorso di persone nel reato*, Milano, 1987, 279 ss.
[280] Cfr. MARINUCCI G.-DOLCINI E., *Manuale di diritto penale*, PG, cit., 461 ss.

utilizzate, basterà che durante l'esecuzione venga comunque seguita una modalità conforme al fatto tipico contenuto nella norma.

Ad ogni modo, non è sempre detto che la "messa a disposizione" di un programma informatico pericoloso debba necessariamente sostanziarsi in una condotta di contributo materiale "atipico" nella commissione del reato di terzi, come nell'esempio sopra fatto. Ci si potrebbe trovare di fronte, infatti, semplicemente ad un *hacker* cosciente della natura lesiva del programma informatico da lui codificato e che decide di ‹‹venderlo, cederlo o distribuirlo›› ad un altro individuo con il quale non ha un ‹‹nesso di collegamento››. Potrebbe accadere che il compratore decida alla fine di non utilizzare più quel *malware* per fini illeciti, cosa che non farebbe accedere il venditore al fatto illecito commetto da altri[281].

Come si è già detto nel corso del paragrafo precedente, quindi, il legislatore ha deciso di punire comportamenti che si ricollegano ad un'attività criminosa altrui, in questo specifico caso sanzionando addirittura una condotta solo perché vi è una possibilità che essa faciliti la commissione di un reato da parte di terzi.

Per quanto riguarda la condotta del "mettere a disposizione", però, tale previsione svolge la c.d. ‹‹funzione di incriminazione›› poiché stabilisce una disciplina che, in realtà, deroga a quella generale sul concorso di persone nel reato. Vengono perseguite condotte di concorso atipiche che, in altri casi, sarebbero restate impunite: si incrimina il comportamento di colui che lascia a disposizione un *malware* al pubblico, sebbene non sia detto che poi quello strumento verrà realmente utilizzato da un terzo per commettere un reato.

Anche in questo caso, quindi, la pericolosità della fattispecie nella nostra società ha spinto il legislatore a optare per la stessa soluzione che si è già riscontrata per quanto riguarda le condotte di signoria su un *software* pericoloso.

7.0 Presupposti per una corretta incriminazione dei "*dual use software*"

[281] In questi casi, infatti, si andrebbe ad integrare un'ipotesi di tentativo di concorso (o tentativo di partecipazione) che per sua natura, nel nostro ordinamento, non è punibile in quanto chiaramente escluso dall'articolo 115 c.p. V. PALAZZO F.C., *Corso di diritto penale*, PG, V ed. Torino, 2013, 494 ss.

La logica a cui si è assistito nel corso dei paragrafi precedenti è quella che vede il legislatore incriminare, generalmente, l'utilizzo dei *software* pericolosi per il loro carattere preparatorio alla commissione di più gravi reati. La previsione di simili fattispecie rende punibili comportamenti che non solo sono anteriori alla normale esecuzione del successivo reato ma che addirittura si pongono in un momento che non può essere fatto rientrare neanche nell'ambito del tentativo di reato. Questa struttura normativa è stata scelta principalmente per due motivi, entrambi connessi alla pericolosità normalmente ricollegata alla scorretta utilizzazione di questo programma informatico malevolo.

La prima ragione è legata alla motivazione politico-criminale che mira a creare una sorta di scudo protettivo intorno a beni giuridici tutelati e che potrebbero essere lesi dalla successiva condotta delle persone che utilizzerebbero i *malware* per scopi illeciti.

L'altra ragione è invece connessa a una più facile repressione di queste stesse condotte. Un crimine nel *cyberspace*, infatti, è difficilmente punibile poiché gli agenti solitamente sono protetti dallo schermo dell'anonimato o da una difficile perseguibilità trovandosi in paesi esteri, lontani, molto spesso paradisi per il *cybercrime*. Dal punto di vista probatorio e processuale[282], invece, tracciare la signoria o il semplice trasferimento di questi programmi informatici è più facile perché ci sono meno passaggi da seguire e meno indagini da portare avanti visto che la condotta si situa in un momento precedente alla commissione del reato più grave[283].

Così facendo, però, si vanno a comprimere non di poco i diritti fondamentali delle persone, anteponendo di molto nel tempo la normale tutela penale per incriminare condotte che solitamente non sarebbero state considerate illecite nella classica teoria penalistica. Per far ciò è necessario avere cause di giustificazione più che legittime. Certo, non è cosa nuova trovare nel nostro ordinamento così come in

[282] A teorizzare questa ipotesi per la prima volta è stato BENTHAM J., The Theory of Legislation, in Bentham's Theory of Legislation: being Principes de Législation and Traités de Législation, 1ª ed., *London*, 1864, rist. *London*, 1931, 425-427, che definisce queste fattispecie con il nome di "reati probatori"; SALVADORI I., *I reati di possesso*, cit., 374 ss.

[283] Cfr. KOSTORIS R.-MARCOLINI S.-DANIELE M. in RUGGIERI F.-PICOTTI L. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 179-182, 190-202, 203-215; DANIELE M., *Intercettazioni ed indagini informatiche*, in KOSTORIS R. (a cura di), *Manuale di procedura penale europea*, Milano, II ed. riv., 2015, 381 ss.

quelli esteri riferimenti a questa particolare categoria di reati che anticipano la tutela penale e che vengono definiti ‹‹reati di prevenzione›› (*Vorfeldsdelikte)* e si distanziano dalla tradizionale figura dei ‹‹reati repressivi››[284].

Punendo comportamenti che, quindi, solitamente non rientrerebbero neanche nel tentativo di altre condotte più gravi, alcuni autori parlano di ‹‹reati a consumazione anticipata››[285]. Vediamo l'utilizzo di questa nuova categoria di reati sempre più spesso nel corso degli ultimi anni, assistendo alla proliferazione di beni giuridici ‹‹intermedi›› (definiti ‹‹di sicurezza››)[286] che non fanno altro che anticipare di molto la tutela rispetto all'illecito compiuto nei confronti del bene giuridico finale[287] (esempi si possono riscontrare nell'ambito della lotta alla criminalità organizzata, dell'abuso sessuale nei confronti dei minori, nella materia della lotta al terrorismo ecc.).

In precedenza, si è cercato di esemplificare creando nell'ambito dei reati che hanno ad oggetto programmi informatici capaci di commettere o facilitare la commissione di reati (informatici) due categorie distinte a seconda che si abbia la "signoria" sul *software* o nel caso in cui ci si limiti a "metterlo a disposizione di terzi".

Nel primo caso il legislatore italiano – ma anche quello di altri ordinamenti europei – ha fatto riferimento ai ‹‹delitti di ostacolo›› con cui vengono punite le condotte che si sostanziano nella semplice signoria su un *malware* senza però

---

[284] In DONINI M., *Modelli di illecito penale minore. Un contributo alla riforma dei reati di pericolo contro la salute pubblica*, in DONINI M.-CASTRONUOVO D. (a cura di), *La riforma dei reati contro la salute pubblica. Sicurezza sul lavoro, sicurezza alimentare, sicurezza dei prodotti*, Padova, 2007, 201 ss., 254, 258-260. Nel corso di questa trattazione il concetto di ‹‹reati di prevenzione›› viene usato in un senso differente rispetto alla materia dell'inosservanza dei regolamenti preventivo-cautelari in cui fu coniato. Usandolo, infatti, si fa riferimento a tutti quei reati che non rientrano nella categoria dei ‹‹reati repressivi›› e quindi vi si ricomprendono quelle condotte che incriminano atti preparatori o prodromici alla commissione di più gravi reati. È in questo senso che la dottrina tedesca parla di ‹‹*Vorfeldsdelikte››. Cfr.* BECK W., Unrechtsbegründung und Vorfeldkriminalisierung. Zum Problem der Unrechtsbegründung im Bereich vorverlegter Strafbarkeit, - erörtert unter besonderer Berücksichtigung der Deliktstatbestände des politischen Strafrechts, Berlin, 1992; SIEBER U., Grenzen des Strafrechts. Grundlagen und Herausforderungen des neuen strafrechtlichen Forschungsprogramms am Max-Planck-Institut für ausländisches und internationales Strafrecht, in ZStW, Heft. 119, 2007, 11 ss., 27-28.

[285] Cfr. PARODI GIUSINO M., *La condotta nei reati a tutela anticipata*, in *Ind. pen*., 1999, 687 ss., 688.

[286] V. DONINI M., *Modelli di illecito penale minore*, cit., 254, 260, che afferma che tali reati producano e tutelino un bene giuridico allo stesso tempo.

[287] Cfr. DONINI M., op. cit., 254.

prevedere alcun collegamento rilevante con la figura di reato che potrebbe essere commesso in futuro mediante il suo utilizzo.

Nella seconda categoria, invece, si è fatta rientrare la materia nei ‹‹reati preparatori›› che solitamente puniscono la condotta di chi semplifica o permette la commissione di un reato successivo più grave da parte di terzi soggetti.

La problematica connessa all'anticipazione della tutela penale meriterebbe una trattazione a sé stante[288]. Nonostante questo, per poter offrire un quadro maggiormente completo all'analisi che si sta svolgendo, non ci si potrà esimere dal definire i criteri per i quali è possibile non solo stabilire la legittimità ma anche la logicità di tutte quelle norme che incriminano reati aventi ad oggetto *software* pericolosi e che si sono appena fatti generalmente rientrare nella categoria dei c.d. ‹‹reati di prevenzione››.

7.1 Il rango del bene giuridico tutelato

In praticamente ogni ordinamento di *civil law* è ancora oggi riscontrabile l'idea che il diritto penale sia posto a tutela di beni giuridici[289]. Ciò che può desumersi

---

[288] Nell'ambito della dottrina italiana si rimanda a GRASSO G., *L'anticipazione della tutela penale: i reati di pericolo e di attentato*, in *Riv. it. dir. proc. pen.*, 1986, 689 ss.; PARODI GIUSINO M., *La condotta*, cit., 687 ss., in specie 690; SALVADORI I., *I reati di possesso*, cit., 211, 234 ss., in specie 253 ss. Nella dottrina tedesca v. JAKOBS G., Kriminalisierung im Vorfeld einer Rechtsgutsverletzung, in *ZStW*, 1985, Bd. 97, H. 4, 751 ss.; WOHLERS W., Deliktstypen des Präventionsstrafrechts, cit., *passim*; PUSCHKE J., Grund und Grenzen des Gefährdungsstrafrechts am Beispiel der Vorbereitungsdelikte, in HEFENDEHL R. (Hrsg.), Grenzenlose Vorverlagerung des Strafrechts?, Berlin, 2010, 9 ss.; SINN A.-GROPP W.-NAGY F. (Hrsg.), Grenzen der Vorverlagerung in einem Tatstrafrecht. Eine rechtsvergleichende Analyse am Beispiel des deutschen und ungarischen Strafrechts, Göttingen, 2011, 13 ss., 99 ss.; nella dottrina inglese, invece, cfr. SIMISTER A.P.-VON HIRSCHS A., Remote Harms and Non-constitutive Crimes, in Crim. Just. Ethics, vol. 28, *Issue* 1, 2009, 89 ss.; ID., Crimes, Harms, and Wrongs. On the Principles of Criminalization, Oxford, 2011, in specie 53 ss., 70 ss.; ASHWORTH A.-ZEDNER L., Prevention and Criminalization: Justifications and Limits, in New Crim. L. Rev., vol. 15, *Issue* 4, 2012, 542 ss.

[289] È un punto fondamentale non solo dell'ordinamento italiano ma anche spagnolo, tedesco e latino-americano. Cfr. BRICOLA F., *Teoria generale del reato*, in *Noviss. dig. it.*, XIX, Torino, 1973, 5 ss., in specie 81 ss.; MARINUCCI G., *Fatto e scriminanti. Note dogmatiche e politico-criminali*, in *Riv. it. dir. proc. pen*., 1983, 1190 ss., 1207 ss.; MUSCO E., *Bene giuridico e tutela dell'onore*, Milano, 1974, 55 ss.; ANGIONI F., *Contenuto e funzioni*, cit., 108 ss.; MANES V., *Il principio di offensività. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza*, Torino, 2005, *passim*; DONINI M., *"Danno" e "offesa" nella c.d. tutela penale dei sentimenti. Note su morale e sicurezza come beni giuridici, a margine della categoria dell'"offense" di Joel Feinberg*, in CADOPPI A. (a cura di), *Laicità, valori e diritto penale*. The Moral Limits of the Criminal Law. *In ricordo di Joel Feinberg*, Milano, 2010, 41 ss., 49; ed in specie ID., *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Dir. pen. cont. - Riv. trim*., 2014, n. 4, 4 ss., nota 1, per leggere riferimenti bibliografici alla dottrina

da questa formulazione è che se il diritto penale deve intervenire può farlo solo a tutela di beni giuridicamente considerati rilevati e degni di tutela[290].

D'altronde è ormai un assunto certo in giurisprudenza[291] che nella Costituzione si possa desumere il principio di offensività e da ciò deriverebbe l'illegittimità di quelle fattispecie che anziché sanzionare l'offesa di un bene giuridico specifico, cercano di reprimere la semplice violazione di norme o provano a punire una determinata categoria di autori (nel nostro caso, ad esempio, l'*hacker*).

Tale principio, oltre a limitare l'ambito di selezione delle norme legittime in materia penale "in negativo", si spinge anche "in positivo", prevedendo che si possano sanzionare solo fatti materiali (‹‹*nullum crimen sine actione*››) e non i semplici pensieri o intenzioni personali (anche questa massima rappresentata da un brocardo: ‹‹*de internis non iudicat praetor*››).

Come tale il diritto penale sarebbe obbligato a reprimere unicamente le condotte umane che si manifestano con un'effettiva lesione di un interesse giuridico o che siano quantomeno in grado di metterlo oggettivamente in pericolo.

Dunque, secondo il principio che vede la necessaria proporzionalità tra la compressione di diritti fondamentali e la meritevole tutela di altri beni giuridici, la dottrina ha affermato che tanto più si ponga anticipata nel tempo la condotta che si intende incriminare dalla lesione del bene tanto più dovrà essere elevato l'interesse tutelato[292]. Da ciò discende che solo beni di rango praticamente primario potrebbero possedere una giustificazione valida per una tutela anticipata nei confronti di condotte che per essi non siano ancora neanche configurabili come un pericolo indiretto o astratto.

Se, a questo punto, si torna con la mente a quelle fattispecie di reato che si sono precedentemente illustrate, non si potrà non notare che molte di esse dovrebbero essere considerate illegittime perché non sono poste a tutela di beni giuridici che potrebbero essere considerati di rango "primario" (basti pensare a quelle norme

straniera; PULITANÒ D., *Offensività del reato (principio di)*, in *Enc. dir*., Annali VIII, Milano, 2015, 665 ss.

[290] Cfr. DONINI M., *"Danno" e "offesa"*, cit., 49-50; ID., *Il principio di offensività*, cit., 7; MARINUCCI G., *Fatto e scriminanti*, cit., p. 1207 ss.

[291] Si citano una serie di sentenze della Corte Costituzionale al riguardo. Corte cost. 24 luglio 1995, n. 360; Corte cost. 11 luglio 2000, n. 263; Corte cost. 21 novembre 2000, n. 519.

[292] V. ANGIONI F., *Contenuto e funzioni*, cit., 181 ss.; MARINUCCI G.-DOLCINI E., *Corso*, cit., 602 ss.

che puniscono condotte aventi ad oggetto programmi informatici in grado di garantire l'accesso a canali *Pay-TV* criptati).

Certo, nessuno potrebbe mai negare che il patrimonio non sia un bene fondamentale per garantire la vita di una persona[293]. Eppure, non si può forzare la mano a questa affermazione sostenendo che l'ipotetica perdita di future aspettative di profitto a causa della presenza di *software* malevoli in grado di decriptare canali a pagamento siano legati da un ‹‹nesso di strumentalità›› e che, quindi, future difficoltà economiche di quel determinato fornitore di servizi siano da ricondurre con certezza alla pericolosità di quella condotta prodromica che si intende reprimere.

Questi comportamenti non possono, alla luce di quanto detto, ricondursi ad un bene primario da proteggere non arrecando alcuna grave offesa diretta ad interessi di natura patrimoniale – sempre facendo riferimento al nostro esempio – ed il ricorso alla tutela penale in modo così anticipato a livello cronologico non appare giustificabile[294]. È anche per questo che, ad esempio, il legislatore tedesco ha preferito affidarsi in questo ambito a strumenti di tutela civilistica e amministrativa in modo da garantire più correttamente la prevalenza delle istanze di sussidiarietà (alcune volte adottando in questa materia anche misure extra-giuridiche come i TPMs).

Una disciplina molto simile è quella che si è già vista in punto di tutela del diritto d'autore e che vede la repressione di tutte quelle condotte aventi ad oggetto un *software* malevolo in grado di aggirare le misure di sicurezza tecnologica poste a tutela delle opere dell'ingegno. Anche in questo caso il bene giuridico tutelato è il patrimonio ma da un punto di vista del tutto ipotetico. I programmi informatici, infatti, non vanno a ledere direttamente l'opera coperta da *copyright*, che continua ad esistere e a poter generare guadagno, quanto, piuttosto, il "mancato" profitto che si teorizza potrebbe derivare dalla diffusione gratuita tra gli utenti della stessa opera su *Internet*.

---

[293] V. FIANDACA G., *Il "bene giuridico" come problema teorico e come criterio di politica criminale*, in STILE A. (a cura di), *Bene giuridico e riforma della parte speciale*, Napoli, 1985, 3 ss., 44.

[294] MOCCIA S., *Tutela penale del patrimonio e principi costituzionali*, Padova, 1988, 26 ss., 43 ss., *passim*, ha suggerito di ricorrere a strumenti di controllo sociale anziché affidarsi allo strumentario penale per dare tutela a questi specifici casi riguardanti il patrimonio.

Un simile comportamento si riscontra anche nei codici di Spagna e Germania che hanno adottato rispettivamente (art. 264.2 CP sp. e § 263 StGB) delle norme che puniscono la produzione, possesso o diffusione di programmi informatici utilizzati per commettere una frode informatica. Come fatto notare da parte della dottrina, infatti, anche in questo caso si sarebbe fatto un uso improprio della tutela di natura penale in quanto simili condotte costituiscono solo un ipotetico pericolo indiretto per un bene giuridico come il patrimonio[295].

Quanto sin qui affermato, però, non fa i conti con la complessità e la natura dei reati informatici. Se il legislatore ha deciso di far ricorso a questo mezzo tecnico è perché i delitti commessi nel *cyberspace* (dunque i reati informatici "in senso stretto") non possono essere equiparati ai reati tradizionali né da un punto di vista empirico né criminologico[296].

Prima di tutto la differenza principale è che un reato informatico è comunemente plurioffensivo, dal momento che con una sola azione si riescono a colpire un numero indefinibile di persone quando, invece, il diritto penale "tradizionale" è stato pensato per una criminalità in cui il rapporto agente/vittima è classicamente di uno ad uno.

Nel corso degli ultimi anni si è assistito al moltiplicarsi di questi reati che facilmente derogano a tale statistica, alcuni sono legati ai nuovi reati ambientali o ai c.d. "disastri tecnologici"[297] ma ancora di più questa situazione diventa palese se, per l'appunto, si guarda alla realtà del *cybercrime*.

Sempre più spesso i reati informatici in senso stretto non hanno bisogno neanche di un *hacker* che faccia partire l'attacco, basandosi totalmente su sistemi automatizzati che possono contare su di una "potenza di fuoco tecnologica" non indifferente (basti pensare al caso in cui si siano sottomessi diversi computer per il mondo con un *trojan horse* dando così vita ad una *botnet*) e che sono in grado di far partire un numero elevato di attacchi indipendentemente dal contatto con il

---

[295] Cfr. GALAN MUNOZ A., El nuevo delito del artículo *248.4 CP:* ¿Un adelantamiento de las barreras de protección penal del patrimonio?, in *LL*, 2004, 1859 ss.

[296] Cfr. PICOTTI L., Biens juridiques protégés et techniques de formulation des infractions dans le droit penal de l'informatique, in Revue Inter. Droit Pénal, vol. 3-4, 2006, 525 ss., 529 ss.; BRENNER S., Cybercrime Metrics: Old Wine, New Bottles?, in Virginia J. L. & Tech, vol. 9, n. 13, 2004, 1 ss.

[297] V. CENTONZE F., *La normalità dei disastri tecnologici. Il problema del congedo del diritto penale*, Milano, 2004.

proprio creatore che si è semplicemente limitato ad installare il programma o a creare la rete che ha dato il via al sistema[298]. Una volta che il sistema è operativo l'intervento dell'uomo non è più necessario ed il programma informatico malevolo farà tutto da solo. A quel punto sarà praticamente impossibile contrastarlo, trovandosi davanti ad una grande serie di danni che difficilmente potranno poi essere puniti poiché colpiscono in breve tempo e spesso con l'anonimato[299].

Si capisce facilmente perché la scelta politica-criminale del legislatore sia stata quella di colpire così duramente questo genere di condotte, mossa non solo da ragioni tecniche ma anche dalla necessità di contrastare l'installazione e la diffusione di *software* malevoli che, una volta in circolazione, possono compiere un numero praticamente indefinibile di reati[300]. L'utilizzazione scorretta di un solo programma informatico pericoloso può causare un insieme di attacchi a catena che vanno a ledere migliaia se non decine di migliaia di persone in una volta sola ed in tutto il mondo. Si aggiunga, quindi, che oltre ai danni difficilmente calcolabili si hanno difficoltà anche dal punto di vista della repressione processuale, poiché i dubbi si estendono in materia di giurisdizione e di autorità competenti in materia di reati informatici (in senso stretto)[301].

Oltretutto una volta che questi *malware* sono in circolazione è praticamente impossibile ritirarli dal mercato e non solo perché è irrealizzabile la volontà di controllare ogni singolo anfratto di *Internet*, ma anche perché se lo stesso cade nelle mani di una qualche organizzazione, quest'ultima sarà in grado di usarlo per commettere un grande numero di reati informatici più volte, a distanza di tempo e nei confronti di un'areale di persone praticamente impossibile da prevedere o calcolare.

Prendiamo, per esempio, un *trojan horse* usato da un c.d. "*bot herder*" per infettare centinaia se non migliaia di computer di persone totalmente ignare in

---

[298] Cfr. PICOTTI L., *Responsabilità penali in* Internet, in PASCUZZI G. (a cura di), *Diritto e informatica. L'avvocato di fronte alle tecnologie digitali*, Milano, 2002, 115 ss.; SALVADORI I., *I reati di possesso*, cit., 353 ss.

[299] Si è soffermato sulla questione PARKER D.B., Defining Automated Crime, in Information System Security, 2008, vol. 4, n.3, 16 ss.

[300] BRENNER S., Cybercrime Metrics, cit., 10, parla di ‹‹*one-to many crimes*››.

[301] Cfr. BRENNER S.W., Cybercrime Jurisdiction, in Crime, Law and Social Change, vol. 46, 2006, 189 ss.; CLOUGH J., Principles of Cybercrime, cit., 475 ss; GILLESPIE A.A., Cybercrime. Key and Issues and Debates, Abingdon, 2016, 21 ss.

tutto il mondo. Una volta inoculato, il *malware* devia parte delle capacità computazionali dell'elaboratore elettronico per permettere all'*hacker* di avere una *botnet* a disposizione. Anche se uno dei proprietari dei computer infettati dovesse accorgersene, il *bot herder* avrebbe comunque sempre a disposizione altre centinaia di *computer* ma, soprattutto, l'originale *trojan horse* che muovendosi autonomamente per la rete continua a procurargli seguaci senza che lui debba far nulla.

Come nel nostro esempio i reati informatici colpiscono, in realtà, beni giuridici di rango sicuramente non primario (solitamente la riservatezza, l'adeguatezza e l'integrità dei dati o il patrimonio) ma che si espandono non nell'ambito individuale quanto in quello della collettività. Il bene giuridico che si deve tutelare non è quello di una persona sola bensì di un numero indefinito di persone che si ritrovano collegate ad *Internet*. Si comprende bene, quindi, che è proprio il carattere di particolare diffusione del danno e dell'offesa derivanti da questa tipologia di reati aventi ad oggetto programmi informatici pericolosi e semplici da realizzare che giustificano eccezionalmente la tutela anticipata di bene giuridici di rango secondario.

Spiegata, però, la ragione che ha portato il legislatore – nazionale e sovranazionale – ad essere così rigido nel far affidamento alla tutela più efficace del diritto penale, bisognerà notare come tale normativa si applichi indipendentemente a tutti i *software* pericolosi, compresi quelli che hanno carattere "*dual use*". Sarà necessario, quindi, vedere anche l'altra faccia della medaglia e considerare se tali disposizioni siano adeguate a perseguire l'obiettivo per cui sono state pensate[302]. Se così fosse, infatti, dovrebbe essere possibile riuscire a distinguere i programmi informatici che sono stati creati o adattati per finalità illecite e che quindi, per la loro pericolosità, devono essere rimossi dalla rete da quell'insieme di *software* pensati, invece, proprio per rafforzare i sistemi e

[302] Sull'argomento v. PALAZZO F.C., *Offensività e ragionevolezza nel controllo di costituzionalità sul contenuto delle leggi penali*, in *Riv. it. dir. proc. pen*., 1998, 350 ss., 381 ss.; PULITANÒ D., *Politica criminale*, in *Enc. dir*., XXXIV, Milano, 1985, 73 ss., 90 ss. Anche nella dottrina tedesca v. VON HIRSCH A.-WOHLERS W., Rechtsgutstheorie und Deliktsstruktur - zu den Kriterien fairer Zurechnung, in HEFENDEHL R.-VON HIRSCH A.-WOHLERS W. (Hrsg.), Die Rechtsgutstheorie. Legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?, Baden-Baden, 2003, 196 ss., 197.

le misure di sicurezza informatiche e telematiche (privi di un carattere d'offensività).

7.2 La connotazione offensiva del "fatto" di reato

Si è visto come la previsione di una fattispecie incriminatrice debba trovare giustificazione in un danno o un pericolo nei confronti di un bene che si intende meritevole di tutela. Nel nostro caso ci troviamo innanzi a reati che sono caratterizzati da un'ampia anticipazione della tutela penale. Elemento necessario, quindi, è che il fatto che si vuole punire sia oggettivamente idoneo a cagionare un danno o un pericolo – anche se astratto o indiretto – per il bene giuridico[303] e che ciò possa essere accertato sul piano giudiziale[304].

Per vagliare se una determinata condotta preparatoria o prodromica sia realmente e oggettivamente in grado di aumentare il rischio di verificazione del successivo reato lesivo del bene giuridico che si intende garantire e che tale evento non presenti alcuna altra causa di giustificazione alternativa si devono presentare due condizioni indispensabili[305].

La prima è di carattere oggettivo e si riferisce al già più volte ripetuto principio che una condotta preparatoria (*Vorfeldhandlung*) ha una valenza veramente lesiva nel momento in cui la sua verificazione aumenta in maniera sensibile il rischio di un danno per il bene giuridico *(Risikoerhöhung)*[306]. Bisogna fare attenzione a considerare la condotta realmente lesiva solo quando il suo carattere offensivo non ha altra spiegazione possibile se non quella di permettere o rendere più

[303] V. MARINUCCI G., *Fatto e scriminanti*, cit., 1207 ss.; DELITALA G., *Il "fatto" nella teoria generale del reato*, Milano, 1930; PAGLIARO A., *Il fatto di reato*, Palermo, 1960; ID., *Fatto (Diritto penale)*, in *Enc. dir*., XVI, Milano, 1967, 951 ss.; VASSALLI G., *Il fatto negli elementi del reato*, in AA. VV., *Studi in memoria di Giacomo Delitala*, III, Milano, 1984, 1641 ss.; anche in *Riv. it. dir. proc. pen*., 1984, 529 ss.; FIANDACA G., *Fatto nel diritto penale*, in *Dig. disc. pen*., V, Torino, 1991, 152 ss.

[304] Cfr. MARINUCCI G., *Fatto e scriminanti*, cit., 1209 ss.; DONINI M., *Il principio di offensività*, cit., 9 ss., 13-14; sul principio di determinatezza si faccia riferimento a MARINUCCI G.-DOLCINI E., *Corso*, cit., 163 ss.

[305] Trattate e teorizzate soprattutto dalla dottrina tedesca a cui si farà, ove possibile, riferimento.

[306] Cfr. FRISCH W., Tatbestandsmäßiges Verhalten und Zurechnung des Erfolgs, Heidelberg, 1988, 293.

semplice la commissione del reato[307]. Questo criterio viene quindi meno nel momento stesso in cui, ad esempio, il programma informatico è stato invece pensato per intenti leciti.

Basandoci su questi assunti possiamo tornare alle norme che abbiamo prima esaminato, tutte sostenute da condotte neutre che non hanno un intrinseco disvalore sociale di per sé stesse. Il disvalore dei comportamenti da queste descritti, quindi, si dovrà ritrovare in altri elementi costitutivi del reato che vadano a mostrare l'illiceità di queste condotte.

A questo punto subentra l'altro criterio di natura oggettiva-soggettiva. Saranno incriminati quei comportamenti che hanno ad oggetto *software* che manifestano un'intrinseca pericolosità in quanto quel determinato *malware* può realmente essere utilizzato per commettere un successivo reato lesivo del bene giuridico tutelato (ed in quanto tale pensato o appositamente adattato dal suo creatore)[308].

Tuttavia, nella realtà fattuale tutte le scelte operate dal legislatore – nazionale e sovranazionale – non sono riuscite a perseguire realmente l'obiettivo politico-criminale di punire solo le condotte realmente offensive.

Da una parte, infatti, il riferimento all'esclusività con cui un *software* avrebbe dovuto essere creato o adattato per commettere un reato è fin troppo restrittivo poiché, come si è più volte sottolineato in precedenza, non esiste un simile programma informatico e seguire questa via non farebbe altro che rendere la norma meramente simbolica, senza una reale efficacia repressiva sul piano legale. Non solo sarebbe quasi impossibile in sede processuale dimostrare che un determinato *software* sia stato pensato esclusivamente per fini illeciti ma, in ogni caso, questa categorizzazione escluderebbe di principio tutti i programmi informatici "multifunzione" e "multiscopo" dato che, per definizione, questi possono svolgere varie attività anche diverse tra loro.

Un elemento che potrebbe essere risolutivo è quello del criterio "oggettivo" che si baserebbe sul concetto dell'idoneità di un determinato programma informatico a commettere un reato specifico. Sapendo quali siano le caratteristiche di un

---

[307] Ancora una volta FRISCH W., op. cit., 281, 289; a sostegno si veda anche WOHLERS W., Deliktstypen des Präventionsstrafrechts, cit., 335; DUGGTE G., Vorbereitung eines Computerbetruges, cit., 301.

[308] V. ALBRECHT A., op. cit., 277 ss., che spiega la questione anche con riferimento all'‹‹idoneità alla commissione di un delitto (*Eignung zur Deliktsbegehung*)››.

software di questo tipo e quali le sue quasi certe o possibili utilizzazioni sarebbe più facile punire la condotta di chi li crea, ne entra in possesso, li metta a disposizione o li diffonda (che siano essi "multiscopo" o "multifunzione". Una simile precisazione sarebbe anche bastevole a chiarire meglio e a soddisfare il principio di determinatezza-tassatività permettendo anche una più semplice perseguibilità sul piano processuale[309].

Si deve, però, operare una successiva distinzione interna. È vero, infatti, che alcuni programmi informatici sono intrinsecamente pericolosi e, come tali, possono essere bollati e differenziati dagli altri, ma è anche vero che la loro offensività si basa altresì sulla volontà del soggetto che poi dovrà utilizzarli per commettere il reato (informatico).

Chiaramente non potranno porsi sullo stesso piatto della bilancia le condotte di colui che diffonde il *malware* tramite TOR, mettendolo virtualmente a disposizione di un numero indefinito ed indefinibile di persone che poi potranno usarlo per gli scopi più vari – anche illeciti – e la condotta di chi, invece, ha la signoria sul programma informatico che decide di utilizzare o di mettere a disposizione di un numero limitato di persone, potendo non solo porre in essere meno condotte criminose ma venendo anche più facilmente perseguito in caso si riuscisse a risalire alla sua persona[310]: il disvalore sociale di questi due comportamenti è innegabilmente differente ed il giudice dovrà tenerne conto. Sarà quindi necessario dare al giudice la possibilità discrezionale di poter considerare e valutare queste due situazioni in modo distinto, ritenendo l'una o l'altra più o meno gravi.

Considerare come pericolose, però, solo un insieme di condotte di per sé stesse "neutre" (produzione, messa a disposizione, distribuzione ecc.) solo perché hanno ad oggetto *software* intrinsecamente capaci di facilitare o rendere possibile la commissione di un reato potrà anche soddisfare il requisito di determinatezza-tassatività ma non, sicuramente, la corretta repressione di quei comportamenti illeciti.

---

[309] Cfr. PALIERO C.E., *Il principio di effettività nel diritto penale*, in *Riv. it. proc. pen*., 1990, 430 ss.; ID, *Il principio di effettività nel diritto penale*, Napoli, 2011.

[310] V. FRISCH W., Tatbestandsmäßiges Verhalten, cit., 265.

La natura di un "*dual use software*" – come si è più volte ripetuto – è insita nel fatto che questi strumenti, proprio come un'arma, potrebbero essere utilizzati per scopi leciti come illeciti a seconda della volontà del loro possessore. Un DPO che si procura un *malware* e ne abbia la signoria con l'intento di utilizzarlo per cercare di accedere al sistema informatico aziendale certamente non commette un fatto lesivo se lo fa per rafforzare le stesse misure di sicurezza della società con un *penetration test* e certamente non si potrà dire oggetto di biasimo sociale l'attività di una *software house* che produce questi programmi informatici.

Se si vuole evitare un'eccessiva e scorretta criminalizzazione bisognerà fare un passo in più, studiare le fattispecie criminose e riuscire a scegliere tra i fatti quelli che sono più marcatamente indicativi di una preparazione o agevolazione rispetto alla commissione di un reato. Quelli che per loro natura sono più oggettivamente in grado di poter ledere il bene giuridico che si vuole tutelare. In alcuni ordinamenti si è già assistito, infatti, alla creazione di un elemento in più di natura soggettiva che fa riferimento al "fine" di commettere un reato o di aiutare nella sua commissione da parte del soggetto che esegue la condotta avente ad oggetto il *software* malevolo[311].

La dottrina tedesca si concentra in modo assoluto su questa tipizzazione dell'elemento soggettivo partendo dall'assunto che l'oggetto del reato, per quanto pericoloso, sia in realtà privo di disvalore: siamo noi che vogliamo utilizzare in maniera illecita questi oggetti (armi da fuoco, programmi informatici, esplosivi ecc.) a configurarli in maniera negativa. Se non fosse per la nostra volontà questi beni non sarebbero diversi da molti altri ed è proprio il movente della nostra condotta ad avere un valore "tipizzante" che concede a questi oggetti di reato una sfumatura di significato delittuosa[312]. Nonostante l'ipotesi sia interessante, però, non sembra condivisibile.

Il fine illecito, lo scopo su cui si costruisce l'interezza del fatto-base, prima d'avere un valore principe nell'elemento soggettivo incide ancora di più

---

[311] ALBRECHT A., op. cit., 278, definisce questo elemento in più con il termine "*Verwendungsabsicht*" ma gli fornisce una connotazione quasi esclusivamente soggettiva a differenza della sfumatura di tipizzazione "oggettiva-soggettiva" del fatto base qui suggerita.

[312] Cfr. FRISCH W., Tatbestandsmäßiges Verhalten, cit., 319; *idem* SIEBER U., Legitimation und Grenzen von Gefährdungsdelikten, cit., 361.

sull'elemento oggettivo che viene da esso tipizzato[313]. Attraverso il riferimento a questo dolo specifico, infatti, prima ancora dell'inizio della condotta che porterà poi alla commissione del reato informatico successivo, troviamo già una volontà chiara da parte del soggetto agente che conduce il suo comportamento ad essere interamente basato su quegli strumenti effettivamente utili per la persecuzione del suo obiettivo illecito.

Non si può nascondere il ‹‹nesso teleologico›› che lega indissolubilmente queste azioni aventi tutte ad oggetto un programma informatico intrinsecamente pericoloso e capace di rendere possibile il proprio fine illecito. ‹‹Il "fine" specifico di commettere quel determinato reato (o risultato o evento lesivo) che deve sorreggere la condotta oggettivamente descritta non solo ne implica la previa rappresentazione da parte dell'agente, ma anche che questa abbia una efficacia "causale" sul suo agire esterno››[314].

Se non si avverasse quella originaria condotta di entrare in possesso o mettere a disposizione d'altri un *software* in grado di rendere possibile la commissione del reato successivo, non ci sarebbe alcun reato successivo. La condotta di procurarsi uno strumento in grado di accedere abusivamente ad un sistema informatico o telematico è già di per sé stesso metà dell'azione che poi porterà a compiere il fatto illecito in quanto strumento necessario alla realizzazione dello scopo perseguito[315].

Si può dire, quindi, che il dolo specifico dell'agente nel procurarsi un determinato *malware* riempie di significato preparatorio la stessa condotta. Non è solo la volontà dell'agente a rendere illecito l'utilizzo di quel programma informatico ma è la volontà di procurarsi quel *software* pericoloso per usarlo poi al fine di commettere un reato: sono due aspetti della stessa medaglia legati tra di loro da una connessione teleologica, legame che rende la fattispecie tipica e dunque rilevante dal punto di vista penale.

Quello esposto è un concetto facile e allo stesso tempo non così semplice ma è anche l'unico che, una volta seguito, potrebbe impedire il "*chilling effect*"

---

[313] V. PICOTTI L., *Il dolo specifico*, cit., 501 ss.

[314] Frase tratta da SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Rivista italiana di diritto e procedura penale*, ISSN 0557-1391, Vol. 60, N. 2, 2017, pag. 747-788.

[315] Cfr. PICOTTI L., *Il dolo specifico*, cit., 502.

immancabilmente cagionato dall'incriminazione di tutti i *"dual use software*", senza considerare l'importanza che lo sviluppo di questi strumenti ha nel settore ICT per risolvere eventuali vulnerabilità e scoprire modi per combattere il pericolo – tutt'altro che astratto – costituito dai programmi informatici creati dalla criminalità informatica.

Non si potrebbe in alcun modo incriminare la condotta del programmatore informatico di una grande azienda che produce da sé un *malware* con l'unica intenzione di fornirlo al proprio *system administrator* al fine di mettere alla prova i propri sistemi di sicurezza. Mancherebbe del tutto, infatti, qualsiasi legame tra il possedere il *dual use software* ed il fine di commettere un reato o di perseguire un qualsivoglia fatto illecito.

Anche questa formulazione, però, ha i suoi aspetti problematici. Spesso, infatti, il riferimento al dolo specifico legato alla commissione di un determinato reato o al semplice cagionare un danno risulterebbe in un'eccessiva specificazione di ciò che rientrerebbe nel penalmente rilevante. Il primo esempio possibile che viene in mente è connesso all'ipotesi in cui il programmatore prima citato, pur avendo creato il programma informatico nell'alveo della propria azienda per permettere un *penetration test*, decisa successivamente di renderlo disponibile sul mercato nero così da ottenere un maggior profitto[316].

Se si seguisse pedissequamente quanto sopra detto, questa condotta, come già affermato, non potrebbe essere fatta rientrare nella fattispecie di reato poiché mancherebbe il dolo specifico, visto che il *software* non sarebbe stato creato all'origine per perseguire un fine illecito. Allo stesso tempo il cederlo sul mercato non comporterebbe l'integrazione del dolo specifico poiché se anche si ipotizzasse che il programmatore fosse consapevole della possibilità che un terzo lo utilizzi per commettere un reato, in realtà, lui non starebbe agendo per il fine di facilitare o rendere possibile questo fatto illecito quanto per un proprio interesse rappresentato dal profitto personale[317]. Sebbene, quindi, la condotta crei una situazione di pericolo non potrebbe essere sanzionata.

---

[316] Tale possibilità è tutt'altro che astratta tanto che il nostro legislatore ha deciso di inserirla in un apposito articolo, il 615-*quater* c.p.

[317] Cfr. GALLO M., *Dolo (dir. pen.)*, in *Enc. dir*., XIII, Milano, 1964, 750 ss., 794; PICOTTI L., *Il dolo specifico*, cit., 595 ss., 598 ss., 610.

Per risolvere questa situazione sarebbe sufficiente prevedere l'abusività della condotta di colui che diffonde programmi informatici idonei a commettere o a facilitare la commissione di un reato (informatico)[318]. In poche parole, si dovrebbe incriminare la "volontà consapevole" di mettere a disposizione di terzi – senza autorizzazione – *malware* che sono intrinsecamente offensivi nei confronti di beni giuridici tutelati dal nostro ordinamento. In questo modo si eviterebbe la lacuna normativa e si potrebbero incriminare anche le condotte di quei soggetti che, pur non essendo pensate per essere strumentali alla realizzazione di un delitto, rappresentano certamente un rischio non indifferente per i beni giuridici che si vogliono tutelare non rientrando nelle comuni e lecite attività socialmente accettate ed utili nell'alveo di coloro che lavorano nell'ambito ICT al fine di aumentare il livello di sicurezza informatica.

7.3 Proporzionalità della sanzione penale

Delineate le modalità che potrebbero essere incriminate sulla base della fattispecie di reato e delle condotte, bisogna domandarsi se vi sia l'effettiva necessità di punire questi atti meramente preparatori o prodromici alla commissione di reati più gravi facendo ricorso allo strumentario offerto dal diritto penale[319]. Ci si dovrà chiedere, in particolare, se sia rispettato il principio di sussidiarietà ancor prima di quello di proporzionalità-adeguatezza. In breve, è necessario capire se la tutela di questi beni giuridici non potrebbe essere perseguita in modo altrettanto efficace facendo ricorso a forme di controllo e punizione che comprimano in maniera minore i diritti dei singoli (facendo ricorso a sanzioni amministrative o civili, responsabilizzazione del settore ICT, potenziamento delle misure di sicurezza ecc.).

Se si pensa ai beni giuridici che si intendono tutelare, però, sembrerebbe che il ricordo allo strumento penale sia quantomai necessario se si vuole evitare che interessi particolarmente importanti come quelli connessi al corretto funzionamento delle infrastrutture critiche (centrali elettriche, mercati finanziari,

[318] V. ALBRECHT A., *op. cit*., 270, 278.
[319] Cfr. ROMANO M., *‹‹Meritevolezza di pena››, ‹‹bisogno di pena›› e teoria del reato*, in *Riv. it. dir. proc. pen*., 1992, 39 ss., 50.

trasporto pubblico, aziende sanitarie ecc.) non vengano lesi da un'eccessiva espansione di questo settore della criminalità già di per sé stesso in crescita. Come, oltretutto, dimenticare che questi *software* malevoli sono in grado di attaccare un numero indeterminato e indeterminabile di soggetti che operano semplicemente sulla rete senza distinzione alcuna.

Allo stesso tempo non si deve compiere l'errore di sovrastimare l'offensività di questi atti illeciti che, sia tenuto a mente, puniscono condotte – aventi ad oggetto programmi informatici – prodromiche alla commissione di reati (informatici) futuri e che quindi sono connesse alla realizzazione del risultato finale senza essere esse stesse la causa della lesione diretta al bene giuridico tutelato. Il trattamento sanzionatorio adottato da altri legislatori europei è stato, quindi, correttamente giudicato illegittimo dagli stessi commentatori per la sua presa di posizione eccessiva (in particolar modo quello spagnolo)[320].

Per trovare, però, trattamenti in contrasto con il principio di proporzionalità-adeguatezza si può ben guardare anche nel nostro Paese che, per esempio, punisce con la stessa pena il delitto di ‹‹fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata›› (articolo 461 c.p.) ed il delitto a cui questo risulta essere preparatorio, cioè l'‹‹alterazione di monete›› (articolo 454 c.p.). Se si rispettasse il principio di adeguatezza, infatti, si dovrebbe calcolare una pena più lieve ed in ogni caso proporzionata al tentativo del reato a cui è prodromica (delitti preparatori come quelli contenuti negli articoli 435, 455 e 462 del Codice penale vengono sanzionati più gravemente rispetto al mero tentativo *ex* articolo 56 c.p. del reato a cui attendono).

Un altro esempio di sperequazione si ritrova nella legge complementare, precisamente agli articoli 171-*ter*, comma 1, lettera f) e 171-*ter*, comma 1, lettera f-*bis*) della legge sul diritto d'autore che, come abbiamo già visto, puniscono condotte di produzione, diffusione, adattamento, messa a disposizione ecc. di programmi informatici in grado di aggirare le misure di protezione informatiche

[320] V. CORCOY BIDASOLO M., Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos, in Eguzkilore. Cuaderno del Instituto Vasco de Criminología, 2007, n. 21, 7 ss., 16; ALVAREZ GARCIA F.J., Estafa (I), in ID. (dir.), Derecho penal español, Parte especial (II), Valencia, 2011, 354.

poste a tutela di beni coperti dal diritto d'autore e che, quindi, sono prodromiche rispetto alla commissione di più gravi reati successivi (articoli ai quali sono equiparati dal punto di vista meramente sanzionatorio).

In questo senso, forse, il nostro legislatore avrebbe fatto meglio a ricorrere allo strumento penalistico solo per sanzionare le condotte aventi ad oggetto *malware* utilizzabili per commettere reati lesivi della tutela del *copyright* su scala commerciale (come d'altronde era anche stato suggerito a livello sovranazionale all'articolo 10 della Convenzione di Budapest del 2001).

Questa eccessiva reazione viene anche più sottolineata se si mettono a confronto questi reati lesivi della componente "economico-patrimoniale" rispetto a reati che vanno a colpire beni di rango più elevato come quelli che attentano alla salute o alla vita delle altre persone (paradigmatico è il fatto che non si punisca la mera detenzione di un veleno o il possedere un'arma con cui poi si andrà a commettere un omicidio)[321].

Si arriva, dunque, alla conclusione che pur essendo corretta la tutela in via anticipata di questi bene giuridici che si intendono tutelare, non è altrettanto giusto applicare in maniera sproporzionata il diritto penale a situazioni in cui sarebbe più che sufficiente una forma di tutela meno comprimente dei diritti fondamentali e della libertà delle persone.

Per evitare l'applicazione di norme punitive che andrebbero contro al ‹‹divieto di eccesso›› (*Übermaßverbot*), il legislatore tedesco ha preferito far riferimento a sanzioni di natura amministrativa per punire tutte quelle condotte aventi ad oggetto *malware* idonei a violare misure di sicurezza e che successivamente potrebbero essere utilizzati per commettere reati contro la proprietà intellettuale (offesa non particolarmente grave ad un bene giuridico di non primaria importanza)[322].

[321] Cfr. SALVADORI I., *I reati di possesso*, cit., 260 ss., che fa notare come in questi casi il legislatore tende ad applicare la tecnica d'incriminazione dei "reati di ostacolo" e non quella dei "reati preparatori" in senso stretto.

[322] Cfr. §§ 95a, Abs. 3, 111a Abs. 1, b), UrhG.

CONCLUSIONI

Alla luce dell'analisi sin qui compiuta, si è visto come la complessità della materia continui a causare non poche difficoltà di criminalizzazione delle fattispecie penali aventi ad oggetto *software* idonei a commettere un reato; inoltre, le ripercussioni negativa degli attacchi informatici– sia in ambito economico che politico – hanno fatto sì che la normativa sovranazionale si indirizzasse verso scelte particolarmente restrittive. Si, pensi, ad esempio al Regolamento UE 1382/2014[323] che ha inserito tra i "*dual use goods*" di cui all'allegato 1 (sottoposti ad un controllo più rigido) anche i c. d. "software d'intrusione"[324] senza distinguere tra fini leciti o illeciti del loro utilizzo. La successiva modifica all'Accordo di Wassenaar[325], a cui il Regolamento si ispira, ha comportato l'allentamento di queste misure di protezione e controllo all'esportazione causando un grande trasferimento di risorse informatiche potenzialmente pericoloso verso Paesi spesso con regimi non democratici. È chiaro come ciò abbia causato una reazione di ritorno quando il 23 novembre 2017 l'*International trademark Association* (*Inta*) si è espressa a favore di un nuovo irrigidimento dei controlli in materia di esportazione dei "*dual use goods*". Questa breve disamina mette dunque in luce tutte le difficoltà che, ancora oggi, si riscontrano in questa materia ben rappresentata da un pendolo che continuamente oscilla tra la necessità di incriminare condotte illecite e l'altrettanto importante obiettivo di non causare un "*chilling effect*" nei confronti delle società dell'ICT che operano con fini leciti.

---

[323] Che ha modificato il precedente Regolamento UE 428/2009 in materia di ‹‹controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso››.

[324] Con ciò si intende far riferimento a tutti i software ‹‹appositamente progettato o modificato per evitare l'individuazione da parte degli "strumenti di monitoraggio", o per sconfiggere le "contromisure di protezione", di un computer o un dispositivo collegabile in rete, che esegue una delle seguenti funzioni: a. l'estrazione di dati o informazioni da un computer o un dispositivo collegabile in rete, o la modifica dei dati del sistema o dell'utente; o b. la modifica del percorso standard di esecuzione di un programma o di un processo al fine di consentire l'esecuzione di istruzioni fornite dall'esterno››.

[325] Siglato nel 1995 e successivamente modificato, l'accordo è uno dei quattro regimi internazionali di controllo delle esportazioni. Il suo fine ultimo è quello di impedire l'accumulo, con effetti destabilizzanti, di armi convenzionali e di beni che possono essere utilizzati a fini sia civili sia militari ("*dual use goods*"), contribuendo così a promuovere la sicurezza e la stabilità regionale e internazionale.

Un corretto inquadramento della materia, però, è a nostro avviso assolutamente possibile. Nel corso della trattazione di questo elaborato si sono sottolineate sia le criticità che i punti di forza della disciplina riguardante i *dual use software* ed ora sembra opportuno cercare di raggiungere una degna conclusione che provi anche a suggerire tecniche legislative capaci di risolvere le problematicità legate in gran parte alla difficoltà di incriminare un oggetto di reato così ampio, variegato e allo stesso tempo non necessariamente legato a intenti illeciti.

In realtà, il nostro ordinamento e la nostra società già hanno incontrato spesso oggetti a "duplice utilizzo". Si considerino, ad esempio, i grimaldelli, sostanze chimiche, informazioni e pistole o altre armi capaci di offendere ecc. Anche in questi casi si è dovuto trovare un compromesso e non si vede la ragione per cui queste conclusioni non possano e non debbano essere estese anche ai programmi informatici. In particolare, la corretta incriminazione dei *dual use software* sembra passare per il rispetto di tre requisiti.

Per prima cosa sarebbe necessario delineare in modo specifico l'oggetto materiale del reato. Con ciò non si intende suggerire di adottare una completa e fin troppo esaustiva casistica che incrimini unicamente i programmi informatici esclusivamente creati o adattati per commettere un qualche reato. Se così si facesse, infatti, si rischierebbe di relegare questa disciplina a un ruolo meramente simbolico poiché inapplicabili nella realtà materiale.

Prendiamo ad esempio l'articolo 461 c.p. che, al comma 1, fa espresso riferimento a un oggetto materiale del reato specificatamente destinato a commettere un reato[326]. Si nota subito come in giurisprudenza sia rimasto praticamente inapplicato nel corso degli anni e questo destino è condiviso con tutte le altre fattispecie che adottato questa eccessiva restrizione a livello di tutela penale.

Una strada maggiormente praticabile parrebbe quella che opta, invece, per la sanzione di tutti quei comportamenti aventi ad oggetto materiale *software* che per loro natura risultino intrinsecamente idonei a essere utilizzati per fini illeciti.

[326] ‹‹Chiunque fabbrica, acquista, detiene o aliena filigrane, programmi e dati informatici o strumenti destinati alla contraffazione o alterazione di monete, di valori di bollo o di carta filigranata è punito, se il fatto non costituisce un più grave reato, con la reclusione da uno a cinque anni e con la multa da euro 103 a euro 516››.

Questa formulazione è la stessa dell'articolo 615-*quater* del Codice penale[327] che restringe l'incriminazione a quelle condotte che si caratterizzano per far riferimento a un programma informatico idoneo ad accedere a un sistema informatico o telematico protetto da misure di sicurezza. Anche il legislatore tedesco ha scelto di seguire questa strada inserendo nel proprio ordinamento riferimenti ai programmi informatici ‹‹che per loro natura sono idonei a commettere una falsificazione di monete o valori bollati››[328].

Questo primo criterio di "idoneità" non è però sufficiente da solo a risolvere le problematiche sopra rilevate. Se, infatti, ci si fermasse qui si otterrebbe l'effetto esattamente opposto e cioè una norma eccessivamente ampia che si applica anche a quella categoria di soggetti che producono, entrano in possesso, scambiano o utilizzano *malware* ma con fini leciti e virtuosi. Ci si riferisce, ovviamente, a tutti quei programmatori che operano nell'ambito dell'ICT così come i *system administrators* delle imprese che hanno il compito di curare lo *standard* di sicurezza informatica dei sistemi a loro affidati, cosa che normalmente viene svolta proprio attraverso *penetration test* che mettono alla prova le misure di protezione installate tramite l'utilizzo di *software* malevoli, gli stessi che potrebbero essere utilizzati anche per commettere un reato essendo intrinsecamente idonei ad offendere un sistema informatico o telematico.

Per distinguere queste pratiche pericolose e veramente lesive da quelle che non lo sono si suggerisce il rispetto di un secondo criterio basato sulla contemplazione di un "dolo specifico": la condotta avente ad oggetto quel programma informatico intrinsecamente pericoloso deve essere rivolta a commettere un reato, utilizzando dunque quel *software* per fini illeciti (che sia per cagionare un danno o per perseguire un profitto).

La dottrina maggioritaria italiana sostiene ancora, in realtà, che il dolo specifico vada a sorreggere e qualificare unicamente l'elemento soggettivo del reato ma bisogna ammettere che questo, prima ancora di sortire effetti sulla colpevolezza,

---

[327] ‹‹Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a euro 5.164››.

[328] Cfr. § 149, Abs. 1, Nr. 1 StGB.

qualifica anche l'elemento oggettivo del reato. Sottolineando che la condotta debba essere posta in essere "al fine di" si presuppone che il soggetto attivo si sia procurato un programma informatico malevolo con lo scopo specifico di perseguire quel determinato obbiettivo: senza questo "interesse causale" ad agire l'agente non si procurerebbe il *malware* idoneo e, quindi, si denota che questi due aspetti siano due facce della stessa medaglia.

Alla base di tutte le fattispecie aventi ad oggetto *dual use software* vi deve essere un rapporto conflittuale tra coloro che vorrebbero penetrare, ad esempio, in un sistema informatico e chi, invece, vorrebbe impedirglielo[329]. Con il procurarsi o con l'entrare in possesso di programmi informatici capaci di ledere la sicurezza informatica di un altro soggetto o di un gruppo indeterminato di soggetti, il soggetto agente pone in essere una condotta che di per sé costituisce l'oggetto per commettere il fine chiaramente richiamato nella fattispecie.

Così facendo, però, ancora una volta si rischierebbe di restringere eccessivamente l'ambito di applicazione penale di questa tipologia di norme, legandolo esclusivamente alla condotta di quegli agenti che si procurino, producano, adattino un *software* pericoloso per il fine specifico di commettere un reato. Ne resterebbero esclusi, ad esempio, i programmatori che pur sviluppando *malware* con l'intento di venderli a persone che poi commetteranno un reato, non agiscono in prima persona nell'utilizzazione illecita dei loro stessi *software*. Infatti, non si potrebbe punire il comportamento di chi mette il proprio programma informatico malevolo a disposizione di soggetti indeterminati, immaginando che possa essere utilizzato per fini illeciti senza che ciò, però, acquisti senza alcun dubbio la valenza di un dolo specifico.

Si potrebbe risolvere la questione prevedendo reati che puniscano autonomamente le condotte di questo tipo, richiedendo in questi casi unicamente un "dolo generico" e cioè la "volontà consapevole" che tra queste persone indeterminate alle quali si mette a disposizione il *malware* intrinsecamente idoneo a commettere

[329] Sostengono questa tesi in dottrina, ad esempio, autori come PALAZZO F.C., *I confini della tutela penale: selezione dei beni e criteri di criminalizzazione*, in *Riv. it. dir. proc. pen*., 1992, 453 ss., 463; PICOTTI L., *Il dolo specifico*, cit., 547 ss.; successivamente ID., *La nozione di ‹‹criminalità informatica››*, cit., 838 ss.

un reato (informatico) potrebbe essercene anche qualcuna che voglia utilizzarlo per fini illeciti.

Per completare il quadro si potrebbe e dovrebbe far riferimento a un terzo criterio già incontrato in materia di reati informatici. Si sta parlando dell'"abusività" o della "mancanza di autorizzazione" quando si utilizzano i *dual use software* in situazioni che potrebbero integrare un fatto di reato avente ad oggetto tali programmi informatici[330]. L'introduzione di questa semplice clausola di antigiuridicità speciale – insieme al rispetto dei due criteri sopra indicati – assicurerebbe alle persone che lavorano in ambito ICT l'impunità e gli permetterebbe di operare in sicurezza e nella legalità al fine di migliorare la sicurezza informatica e perseguire altri scopi leciti a sostegno della comunità e della collettività in una società che è sempre più dipendente dall'utilizzo di apparecchiature elettroniche ed informatiche interconnesse tramite la rete Internet.

[330] Da notare come ciò sia già stato pensato e fatto in Francia dove il legislatore, riguardo alle condotte aventi ad oggetto dati o programmi informatici destinati a commettere un reato lesivo della riservatezza informatica, incrimina la disponibilità o l'utilizzo di questi strumenti quando ciò avvenga ‹‹senza un motivo legittimo, ragioni di ricerca o di sicurezza informatica›› (articolo 323-3-1 CP).

BIBLIOGRAFIA

ALMA M.M.-PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. proc.*, 1997, 4, 504 ss.

AMATO G., DESTITO V. S., DEZZANI G., SANTORIELLO C., *I reati informatici*, Padova, 2010.

AMATO G., *Commento agli articoli 617*-quater, *617*-quinquies, in PADOVANI T. (a cura di), *Codice Penale*, Milano, 2007, 3815.

ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983.

ANTOLISEI F., *Manuale di diritto penale. Parte generale*, Milano, 2017.

ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, vol. I, Milano, 2016.

BARTOLI R. *L'accesso abusivo a un sistema informatico (art. 615* ter *c.p.) a un bivio ermeneutico teleologicamente orientato*, in *Dir. pen. cont. – Riv. Trim.*, 1/2012, 123 ss.

BERGHELLA F.-BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, 2329 ss.

BONDI A., *I reati aggravati dall'evento tra ieri e domani*, Napoli, 1999.

BORRUSO R., *La tutela del documento e dei dati*, in BORRUSO R.-CORASANITI G.-D'AIETTI G. (a cura di), *Profili penali dell'informatica*, Milano, 1994, 1 ss.

CANNATA S.-COSTALUNGHI D., *Detenzione e diffusione di codici d'accesso a sistemi informatici o telematici (art. 615*-quater*)*, in CADOPPI A.-CANESTRARI S.-MANNA A.-PAPA M. (diretto da), *Trattato di diritto penale. Parte speciale*, vol. IX, *I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti*, Torino, 2011, 553 ss.

CORASANITI G., *La tutela della comunicazione informatica e telematica*, in BORRUSO G.-CORASANITI G.-D'AIETTI G. (a cura di), *Profili penali dell'informatica*, Milano, 1994, 101 ss.

CUOMO L., *La tutela penale del sistema informatico*, in *Cass. pen.*, 2000, 2998 ss.

D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, in BORRUSO R.-BUONOMO G.-CORASANITI G.-D'AIETTI G. (a cura di), *Profili penali dell'informatica*, Milano, 1994, 39 ss.

D'ARCANGELO F., *L'accesso abusivo ad un sistema informatico nell'era di Internet*, in *Giur. merito*, 2008, 1066 ss.

DE FLAMMINEIS S., *Art. 615* -ter *c.p.: accesso legittimo ma per finalità estranee ad un sistema informatico*, in *Cass. pen.*, 2011, n. 6, 2209 ss.

DELITALA G., *Il "fatto" nella teoria generale del reato*, Milano, 1930.

FASANI F., *Accesso abusivo a un sistema informatico: le Sezioni Unite cambiano di nuovo rotta*, in *Soc.*, n. 12/2017, 1397 ss.

FIANDACA G., MUSCO M., *Diritto Penale. Parte generale*. Bologna, 2019.

FIANDACA G., MUSCO M., *Diritto penale. Parte speciale*, Volume I, Bologna, 2012.

FIANDACA G., MUSCO M., *Diritto penale. Parte speciale*, Volume II tomo II, Bologna, 2013.

FLOR R., *Natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. pen. proc.*, 2008, 1, 106 ss.

FLOR R., *Verso una rivalutazione dell'art. 315* ter *c.p.?*, in *Dir. pen. cont. – Riv. Trim.*, 2/2012, 126 ss.

FLOR R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo* jus excludendi alios, in *Dir. pen. proc.*, 2015, 1, 81 ss.

FLOR R., voce *Riservatezza informatica*, in *Enc. Giur. online*, 2017, 1 ss.

FUMAGALLI G., *La tutela del* software *nell'Unione Europea. Brevetto e diritto d'autore*, Milano, 2005.

FUMO M., *La condotta nei reati informatici*, in *Arch. pen*., 2013, 771 ss.

GALDIERI P., *La tutela penale del domicilio informatico*, in ID. (a cura di), *Problemi giuridici dell'informatica nel MEC*, Milano, 1996.

GALDIERI P. *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997.

LACSON W.-JONES B., *The 21st Century DarkNet Market: Les-sons from the Fall of Silk Road*, in *IJCC*, vol. 10, Issue 1, 2016, 40 ss.

LESSIG L., *Code and Other Laws of Cyberspace*, New York, 2000.

LUPÀRIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Dir. pen. proc*., 2008, 6, 696 ss.

MARINUCCI G.-DOLCINI E., *Manuale di diritto penale. Parte generale*, Milano, 2019.

PALAZZO F., *Considerazioni in tema di tutela della riservatezza (a proposito del "nuovo" art. 615*-bis *c.p.)*, in *Riv. it. dir. e proc. pen*., 1975, 126 ss.

PARODI C., *Accesso abusivo, frode informatica, rivelazione di documenti informatici segreti: rapporti da interpretare*, in *Dir. pen. proc.o*, 1998, 1038 ss.

PARODI C.-CALICE A., *Responsabilità penale e Internet: le ipotesi di responsabilità penale nell'uso dell'informatica e della telematica*, Milano, 2001.

PATRONO P, *Privacy e vita privata*, in *Enc. Dir*., XXXV, Milano, 1986, 557 ss.

PAZIENZA F., *In tema di criminalità informatica: l'art. 4 della legge 23.12.1993, n. 547*, in *Riv. it. dir. e proc. pen*., 1995, 750 ss., 755.

PECORELLA C., *Il diritto penale dell'informatica*, rist. agg., Padova, 2006.

PECORELLA C., *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. pen.*, 2012, 3692 ss.

PERRI P., *Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore del sistema*, in *Giur. merito*, 2008, 1651 ss.

PICA G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. trim. dir. e proc. pen.*, 1995, 412 ss.

PICOTTI L., *La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione*, in *Dir. inf.*, 1986.

PICOTTI L., *Sulla riforma dell'abuso d'ufficio*, in *Riv. trim. dir. pen. econ.*, 1997, n. 1-2, 283 ss.

PICOTTI L., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, 5, 2008.

PICOTTI L., *La ratifica della Convenzione di Budapest sul Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, 6, 700 ss.

PICOTTI L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 29 ss.

PLANTAMURA V., *Domicilio e diritto penale nella società post-industriale*, Pisa, 2017.

PULITANO' D., *Diritto penale. Parte generale*, Torino, 2019.

PULITANO' D., *Diritto penale. Parte speciale*, vol. I, Torino, 2019.

SALVADORI I., *Il microsistema normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante,* in *Riv. it. dir. e proc. pen.*, 2012, 204 ss.

SALVADORI I., *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, Napoli, 2016.

SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "*dual-use software*"* in *Riv. it. dir. e proc. pen.*, 2017, 2, 747 ss.

SALVADORI I., *I reati contro la riservatezza informatica,* in CADOPPI A.-CANESTRARI S.-MANNA A.-PAPA M. (a cura di), *Cybercrime,* Milano, 2019, 656 ss.

SIEBER U., *Organised crime in Europe: the threat of cybercrime. Situation Report 2004*, in *Council of Europe Publishing*, Strasburgo, 2005.

TRENTACAPILLI D., *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione,* in *Dir. pen. proc*., 2002, 1280 ss.

TIGANO S., *Delitti contro l'inviolabilità del domicilio*, in ALEO S. (a cura di), *Istituzioni di diritto penale,* PS, Milano, 2017, 237 ss.

RIFERIMENTI GIURISPRUDENZIALI

Cass. pen., sez. V, 7.11.2000, Zaia, n. 1675.

Cass. pen., sez. V, 6.7.2007, n. 31135.

Cass. pen., sez. V, 29.5.2008, n. 26797.

Cass. pen., sez. V, sent. 8.7.2008, n. 37322.

Cass. pen., sez. V, 30.9.2008, n.1727.

Cass. pen., sez. VI, sent. 8.10.2008, Peparaio, n. 39290.

Cass. pen., sez. V, 3.2.2009, n. 18006.

Cass. pen., sez. V, 10.12.2009, n. 2987.

Cass. pen., sez. V, 12.2.2010, n. 19463.

Cass. pen., sez. V, 22.9.2010, n. 39620.

Cass. pen., sez. V, 18.1.2011, n. 24583.

Cass. pen., SS. UU., sent. 27.10.2011, n. 4694.

Cass. pen., sez. V, 18.11.2011, n. 8555.

Cass. pen., sez. V. 5.4.2012 n. 8555.

Cass. pen., sez. V, 8.5.2012, n. 42021.

Cass. pen., sez. II, 14.12.2012, n. 9870.

Cass. pen., sez. II, 6.3.2013, n. 13475.

Cass. pen., sez. V, 24.4.2013, n. 22024.

Cass. pen., sez. I, 27.5.2013, n. 1921.

Cass. pen., sez. I, 27.9.2013, n. 40303.

Cass. Pen., sez. II, 19.12.2014, n. 52680.

Cass. pen., sez. V, 30.1.2015, n. 29091.

Cass. pen., SS. UU., 26.3.2015, n. 17325, 2015, 1296 ss.

Cass. pen., sez VI, 5.5.2016, n. 18713.

Cass. pen., sez. V, 28.7.2016, n. 33311.

Cass. pen., sez. V, 29.11.2017, n. 1021.

SITOGRAFIA

www.affariitaliani.it

www.altalex.com

www.camera.it

www.curia.europa.eu

www.diritto.net

www.europa.eu

www.europarl.europa.eu

www.europol.europa.eu

www.garanteprivacy.it

www.gazzettaufficiale.it

www.giurisprudenzapenale.com

www.osservatoriopenale.it

www.penale.it

www.penalecontemporaneo.it

www.*privacy*.it

RINGRAZIAMENTI

Questa tesi rappresenta il compimento del mio percorso universitario e lo spartiacque tra la vita da studente e, forse, l'età adulta in cui sto per entrare. Non sarei mai arrivato qui senza i sacrifici dei miei genitori ed il loro sostegno. Quando ero piccolo mi sarei immaginato ovunque tranne che a frequentare la stessa università e la stessa facoltà che fece mio padre Enrico, soprattutto quando lo guardavo lavorare di notte sul terrazzo su fogli contenenti frasi in una lingua (giuridica) a me incomprensibile. Ad oggi sento di riuscire a comprendere meglio quell'uomo che al tempo, per me, risultava un mistero. La vita non è sempre prevedibile e spero che grazie alle ali che mi sono state donate io possa presto spiccare il volo, ma portando con me l'affetto che mi lega a coloro a cui devo ogni cosa. Ringrazio mia madre Antonella che mi ha sempre spinto a dare il massimo e a non arrendermi anche quando la vita sembrava difficile. Spero, un giorno, di poterti ripagare di tutti i sacrifici che hai deciso di sopportare, spesso in silenzio e di nascosto, per la mia felicità. Ringrazio i miei nonni, quelli scomparsi troppo presto per potermi vedere in questo giorno e nonno Antonio che, invece, sta quest'oggi sfidando il caldo per essere qui presente. Mi hai insegnato a provare tutto nella vita, che una mente acuta è più importante della forza e da sempre mi hai spinto a superare i miei limiti: se oggi trovo facilmente il coraggio di parlare davanti a molte persone è solo grazie a te. Ringrazio le mie zie, Patrizia e Loredana, su cui ho potuto sempre contare e che, nonostante il mio carattere chiuso e non particolarmente amabile, mi hanno sopportato e supportato per quello che sono e che oggi sono qui, immancabili nonostante il contingentamento. Ringrazio mia zia Laura la cui passione per la conoscenza mi ha sempre spinto a migliorare me stesso, anche se adesso non è qui presente la sento vicina. Ringrazio mio zio Riccardo sia per non avermi mai appeso al pennone dello stabilimento balneare che frequentavamo quando ero piccolo sia per avermi trasmesso l'interesse per l'informatica e l'elettronica. Per quanto non potrò mai aiutarti con il "diritto d'antenna", spero quantomeno di poterti essere utile a montarla un giorno. Ringrazio mia cugina Chiara con cui sono cresciuto e che per

me rappresenta una sorella. Sono felice di poter condividere questo giorno con lei, raramente nella mia vita ricordo un evento significativo della mia vita senza la sua presenza e spero che questo legame non vada mai a perdersi. Ringrazio la mia famiglia senza la quale non potrei immaginare la mia esistenza, nonostante tutto. Ringrazio i qui presenti membri della commissione così come tutti i professori che mi hanno guidato nella strada da me intrapresa ormai cinque anni fa. Ringrazio la dottoressa Elisabetta Pietrocarlo che mi ha pazientemente seguito nella stesura di questo elaborato e alla quale non sarò mai grato abbastanza. Ringrazio il Professor Bellacosa la cui passione e buonumore sono sempre stati per me un faro da seguire e ringrazio il Professor Gullo senza il quale non avrei mai scritto questo elaborato: mi ha fornito gli strumenti per iniziare questa tesi e ha trasmesso ad un me più giovane e distratto l'amore per la materia del diritto penale, senza di lei non sarei qui quest'oggi. Ringrazio i miei amici, sia quelli storici con cui sono cresciuto che quelli con cui ho condiviso gioie e disgrazie qui alla LUISS. Ringrazio tutte le persone che hanno avuto importanza nella mia vita così come quelle appena sfiorate, ringrazio tutti per gli insegnamenti che hanno fatto si di portarmi qui quest'oggi.